THESIS PRESENTED TO OBTAIN THE DEGREE OF

DOCTOR OF PHILOSOPHY

UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE DROIT
SPÉCIALITÉ DROIT PRIVE ET SCIENCES CRIMINELLES
Centre de droit comparé du travail et de la sécurité sociale, UMR 5114
16, Avenue Léon Duguit CS 50057, Bâtiment Enseignement, Entrée C4, 1er étage
33608 Pessac Cedex – France

UNIVERSITAT DE VALÈNCIA

ESCUELA DE DOCTORADO
PROGRAMA DE DOCTORADO EN DERECHOS HUMANOS, DEMOCRACIA Y JUSTICIA INTERNACIONAL
Instituto Universitario de Derechos Humanos
Calle Serpis, nº29. Edificio de Institutos de Investigación,
46022, Valencia - España

Salomé LANNIER

NEW TECHNOLOGIES AND HUMAN TRAFFICKING
An analysis based on the theory of sovereignty

Directed by
Bénédicte LAVAUD-LEGENDRE
COMPTRASEC, CNRS/Université de Bordeaux
&
María Teresa ALEMANY JORDÁN
Departamento de Derecho Internacional “Miaja de la Muela,” Universitat de València

Deposit request presented the 12/09/2023
Thesis presented the 18/12/2023

Members of the jury:

- Carmen AZCÁRRAGA MONZONÍS, Profesora Titular de Derecho Internacional Privado, Universitat de Valéncia
- Olivier DECIMA, Professeur de droit privé et de sciences criminelles, Université de Bordeaux
- Víctor Luis GUTIÉRREZ CASTILLO, Profesor Titular de Derecho Internacional Público y Relaciones Internacionales, Universidad de Jaén
- Joanne VAN DER LEUN, Full Professor of Criminology, Leiden University
- Valère NDIOR, Professeur de droit public, Université de Bretagne occidentale
- Anne WEYEMBERGH, Professeure ordinaire, Université Libre de Bruxelles

CAVEATS

The University of Bordeaux and the University of Valencia do not intend to provide any approval or disapproval of the opinions expressed in this thesis; these opinions are considered to belong solely to their author.

L'Université de Bordeaux et l'Université de Valencia n'entendent donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur.

La Universidad de Burdeos y la Universidad de Valencia no pretenden aprobar ni desaprobar las opiniones expresadas en esta tesis; dichas opiniones deben considerarse como propias del autor.

ACKNOWLEDGMENTS

To the ones who have known me before I was even born, Mom and Dad, thank you for opening the doors of reading, culture, and education; for nourishing my curiosity; for listening to me talk about my thesis for years. I love you.

To the ones I have known before they were born, little sis' and little bro', thank you for the deep connection of sisterhood and brotherhood, for all the laughs and arguments we had, for challenging my thoughts. I love you, and I couldn't be prouder of the people you are both becoming.

To the ones I have met long before starting this research adventure, especially my "witch sis'," thank you for being crazy with me, for your constant support and listening, for nourishing my creativity. I love you, and I can't wait to live out our next adventures together.

To the ones I have met since my research adventure was on track and to the ones who shared a few moments of my life and were interested in hearing me talk (maybe too much) about my research, thank you for making me discover the diversity of life.

To the ones who share my life, in real time or summarized during the time capsule in which we meet, in real life or through the intermediaries of phones or computers, thank you for always being here to listen or help, for sharing knowledge and stories, for bringing joy and fun. I love you, and I can't wait to enjoy much more time together.

To the ones who share my life closely, in so many different ways, thank you for accepting me for who I am, for caring deeply for me, for making me smile every day. I love you, and I couldn't express how much I feel lucky to have met you.

To the ones who directed this work, Bénédicte and Maite, thank you for trusting me and this research project.

Also, a huge thank to Elisabeth and María Angeles who helped me in all the administrative challenges I faced during my adventure as a young researcher.

Likewise, a big thank to Debbie, for her high-quality proofreading and bringing my English to the next level.

Finally, this work would not have been the same without all the scholars and practitioners who offered a bit of their time to talk about my research and to exchange knowledge, ideas, and references. Thank you so much for your help.

SUMMARY

LIST OF MAIN ABBREVIATIONS

¶/§	paragraph
AI	Artificial intelligence
CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CNIL	Commission nationale de l'informatique et des libertés (France)
CPHR	Convention for the Protection of Human Rights and Fundamental Freedoms
CSR	Corporate social responsibility
DIICOT	Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism
e.g.	*Exempli gratia*
ECHR	European Court of Human Rights
ECJ	European Court of Justice
E-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market
E-evidence regulation	Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings
Ed.	Editor/Edition
Et al.	et alia
Etc.	Et cetera
EU	European Union
FOSTA (or FOSTA-SESTA)	Allow States and Victims to Fight Online Sex Trafficking Act
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
GRETA	Group of Experts on Action against Trafficking in Human Beings
Ibid.	*Ibidem* (in the same source)

i.e.	*Id est*
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICTs	Information and communication technologies
ILO	International Labour Organisation
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOM	International Organization for Migration
IP	Internet Protocol
Law Enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
NGO	Non governmental organization
No.	Number
OCLTI	Office central de lutte contre le travail illégal
OCRTEH	Office central pour la répression de la traite des êtres humains
OECD	Organisation for Economic Co-operation and Development
Op. cit.	*Opus citatum*
OSCE	Organization for Security and Co-operation in Europe
p.	page
Palermo Convention	Convention against Transnational Organized Crime
Palermo Protocol	Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children
SAVE Act	Stop Advertising Victims of Exploitation Act
UCRIF	Unidad Central de Redes de Inmigración Ilegal y Falsedades Documentales
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States of America
USC	US Code

v.	Versus
Vol.	Volume
Warsaw Convention	Convention on Action against Trafficking in Human Beings

ABSTRACT [ENGLISH VERSION]

Title: New technologies and human trafficking: an analysis based on the theory of sovereignty

Keywords: human trafficking, new technologies, sovereignty, digital actors, duty to protect, legitimate coercion, partnerships, jurisdiction, digital investigative techniques, right to privacy, due process, electronic evidence, data retention, encryption, corporate criminal liability, online intermediaries' liability, criminal policy, sex work, content moderation, personal data protection, artificial intelligence, corporate social liability, digital social liability, victims' protection, trafficking prevention, interdependence

Human trafficking, a criminal offense resulting in the exploitation of people, is increasingly facilitated by new technologies. Similarly, the anti-trafficking framework and its actors are evolving to modernize their strategies and policies. In particular, states and digital actors appear at the crossroads of the repression of trafficking and the regulation of cyberspace. As both seek to participate in this fight, the theory of sovereignty is challenged. Indeed, the repression of cyber human trafficking requires research into who exercises coercion, particularly to establish the obligations of states as sovereigns, and the existence of new sovereigns, specifically to question the role of digital actors. Consequently, when various sovereigns emerge, this study focuses on the order of coercion between them, particularly the strategies they develop and their impact on the repression of cyber human trafficking. Instead of a demonstration in favor of its demise, this study aims to rethink the basis of the theory of sovereignty to offer a new perspective on its application, using the repression of cyber human trafficking as a case study.

This study reveals that sovereignty can be applied outside the framework of the state and that relationships of coercion and collaboration are being developed between sovereign entities, challenging the notion of independence as the basis for sovereignty. If sovereignty is linked to the exercise of coercion, it can then be disconnected from the state. This disconnection clearly appears as a result of the limitations of the state in implementing it when digital actors exercise coercion over data. Indeed, various sources of coercion appear in the repression of cyber trafficking and are needed to protect the victims and convict the perpetrators. Consequently, various types of relationships can be drawn between sovereigns. First, imposing coercion between sovereigns hinders the independent exercise of coercion and the effective repression of trafficking. Second, collaboration between sovereigns arises as a strategy to protect each other's sovereignty and to head toward a comprehensive repression of cyber trafficking. This mindset is particularly developed outside of criminal law. As a result, digital actors are intermediaries in the implementation of human rights, and states are intermediaries for digital actors by lending them guidance and tools to legitimize their actions. However, partly due to a traditional understanding of sovereignty and a mainly neoliberal approach to the business sector, this interconnectedness is negated under the current theory of sovereignty. Its traditional basis, independence, challenges the implementation and legitimization of norms, particularly human rights and anti-trafficking frameworks. Accordingly, a complementary criterion could legitimize

sovereignty: interdependence. Thus, this study offers a new perspective on sovereignty and adapts it to the current societal environment. The role of the law is also questioned. This study on the legal tools to repress cyber trafficking highlights a downgrade in the quality of the law, specifically criminal law, which is seen as a tool to solve social problems. The law is magnified as a solution, in particular, to challenges derived from technologies, leading to legal solutionism.

RESUME [FRENCH VERSION]

Titre : Nouvelles technologies et traite des êtres humains - Approche à partir de la théorie de la souveraineté

Mots clés : Traite des êtres humains ; nouvelles technologies ; souveraineté ; acteurs numériques ; devoir de protection ; contrainte légitime ; partenariats ; compétence juridictionnelle ; techniques d'enquête numérique ; droit à la vie privée ; *due process* ; preuves électroniques ; conservation des données ; chiffrement ; responsabilité pénale des entreprises ; responsabilité des intermédiaires en ligne ; politique pénale ; travail du sexe ; modération de contenu ; protection des données personnelles ; intelligence artificielle ; responsabilité sociale des entreprises ; responsabilité sociale numérique ; protection des victimes ; prévention de la traite des êtres humains ; interdépendance

Introduction

L'évolution des technologies offre de nouvelles opportunités pour les auteurs d'infraction et contribue notamment à faciliter les processes de traite des êtres humains. L'utilisation des technologies par les auteurs de traite a été qualifiée de cybertraite[1] ou de e-traite, définie comme « *la traite des êtres humains facilitée, rendue possible ou réglementée par l'utilisation de* » nouvelles technologies[2]. L'infraction est définie par le Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants (2000). Premièrement, des actes matériels spécifiques doivent être prouvés, tel que le recrutement des victimes ; deuxièmement, ces actes doivent être commis à l'aide de moyens spécifiques, qui annulent le consentement de la victime[3], comme la contrainte ou la fraude ; enfin, la traite a une finalité spécifique, l'exploitation de la victime.

Les opportunités offertes aux trafiquants sont décuplées par la digitalisation. Dans cette étude, les nouvelles technologies désignent au sens large « *les technologies de l'information et de la communication, en particulier celles qui constituent des environnements numériques et en réseau* »[4], dont « *l'ensemble des techniques utilisées dans le traitement et la transmission des informations* »[5], notamment Internet. La digitalisation facilite l'accès à tous les acteurs, le caractère abordable des outils et

---

[1] V. Greiman, C. Bain, « The Emergence of Cyber Activity as a Gateway to Human Trafficking », *International Journal of Cyber Warfare and Terrorism*, 2012, vol. 12, nº 2, p. 29; A. Sykiotou, « Cyber trafficking: recruiting victims of human trafficking through the net », *in* N.E. Kourakēs, C.D. Spinellis (dir.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017, p. 1549

[2] S. Milivojević, « Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus », *in* M. Segrave, L. Vitis (dir.), *Gender, Technology and Violence*, Routledge, 2017, p. 28-44

[3] Par conséquent, le consentement n'est pas un élément de l'infraction.

[4] H. Watson, A. Donovan, « Role of technology in human trafficking », *TRACE*, octobre 2015, p. 3

[5] M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 15

des services utilisés et l'anonymat[6] pour la commission des faits de traite. En général, à tous les stades du processus, les trafiquants tirent parti des opportunités numériques.

Ces pratiques infractionnelles, facilitées ou non par les technologies, portent atteinte à des valeurs protégées aux niveaux national comme supranational, notamment la dignité et l'intégrité des personnes et les droits fondamentaux de manière générale. Par conséquent, les Etats mettent en œuvre des pouvoirs coercitifs, nécessaires à la lutte contre la traite, et qui évoluent en réponse à la digitalisation de ce phénomène. Ces pouvoirs étatiques renvoient et sont légitimés par la théorie de la souveraineté. Il s'agit, selon Bodin, de la « *puissance absolue et perpétuelle d'une République* »[7]. Pourtant, cette vieille théorie fait face à des défis, notamment la digitalisation. Un nouveau concept a été développé : la souveraineté numérique. Selon une approche positive, « *la souveraineté numérique est l'expression [du] contrôle sur le miroir virtuel de l'économie et de la population* »[8]. Selon une approche négative, la souveraineté numérique souligne les difficultés des États à réguler ces espaces, car concurrencés par des entités privées[9]. Celles-ci seront largement désignées comme des acteurs numériques, afin de souligner leur rôle actif dans le façonnement des nouvelles technologies, des expériences numériques et dans la répression de la traite des êtres humains.

Cette étude de recherche en droit s'appuie sur différents choix méthodologiques.

Tout d'abord, comme la souveraineté et la traite des êtres humains font l'objet de développements nationaux et internationaux, cette étude est basée sur une méthodologie comparative. Celle-ci permet d'étudier les interactions entre les différents niveaux de souverainetés et de souligner les différences, les points communs[10], les lacunes et les bonnes pratiques[11]. Cette recherche est principalement basée sur l'étude de quatre systèmes juridiques nationaux. La France et l'Espagne constituent le noyau de cette étude, comme systèmes de droit civil d'Europe occidentale. Le choix de deux systèmes géographiquement proches met en évidence les différences qui subsistent dans leurs cadres juridiques. La Roumanie offre la perspective d'un pays d'Europe de l'Est. Les trois pays légifèrent de manière harmonisée en raison de leur participation au sein de l'UE, mais des différences subsistent aux niveaux juridiques et institutionnels. En outre, les États-Unis exercent une forte influence sur la répression mondiale de la traite et apportent une perspective de common law.

Deuxièmement, cette étude s'appuie sur une méthodologie interdisciplinaire, à travers une « *articulation des savoirs entre des disciplines qui développe des*

---

[6] A. Cooper, « Sexuality and the Internet: Surfing into the New Millennium », *CyberPsychology & Behavior*, janvier 1998, vol. 1, nº 2, p. 187

[7] J. Bodin, *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie nº 4619, 1993, p. 111

[8] S. Guillou, *La souveraineté numérique française passera par l'investissement dans les technologies numériques*, Sciences Po Paris, Chaire Digital, Gouvernance, et Souveraineté, 2020, p. 3

[9] F. G'Sell, « Remarques sur les aspects juridiques de la « souveraineté numérique » », *La revue des juristes de Sciences Po*, 2020, nº 19, p. 52

[10] M. Durán Bernardino, « El método comparado en los trabajos de investigación », *in* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (dir.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 49

[11] V. Robert, L. Usunier, « Conclusion. Du bon usage du droit comparé », *in* M. Delmas-Marty, Université de Paris I: Panthéon-Sorbonne (dir.), *Critique de l'intégration normative: l'apport du droit comparé à l'harmonisation des droits*, Presses Universitaires de France, Les voies du droit, 1re éd., 2004, p. 231

problématiques se recoupant partiellement »[12]. Elle ne se limite pas au droit pénal : tant la théorie de la souveraineté que la répression de la traite des êtres humains requièrent diverses disciplines juridiques pour une approche globale[13]. De plus, dans cette recherche, la science juridique est fortement liée à la science politique, car de nombreuses lois étudiées ont été et sont encore en cours de négociation et d'amendement. Ainsi, « *entre droit et politique, la détermination est réciproque, et l'implication mutuelle constante* »[14]. De même, l'étude des textes juridiques ne peut être séparée de leur mise en œuvre.

Troisièmement, cette étude ne repose pas sur une conception du droit limitée au droit étatique. La réglementation des nouvelles technologies et de la lutte contre la traite nécessite de prendre en compte les normes supranationales et locales, ainsi que des normes privées ou des règles incorporées dans certaines techniques. Cette recherche est guidée par l'hypothèse du pluralisme juridique : « *le droit n'est pas seul ; il coexiste avec d'autres systèmes de normes* »[15].

Quatrièmement, cette étude fait appel à d'autres sciences sociales, afin de comprendre totalement le phénomène de la traite. Aussi, l'étude des nouvelles technologies requiert des notions d'informatique. D'autres disciplines sont donc nécessaires pour établir un « *contexte factuel* » et élargir le « *contexte théorique* »[16].

Pour résumer, cette méthodologie « *peut être brièvement décrite comme l'association de références hétérogènes. Il s'agit d'organiser un dialogue avec les textes non-juridiques […] Une telle méthode autorise à utiliser les glissements et les rapprochements, au lieu de recourir exclusivement aux opérations de la logique juridique [… Ce] bricolage rend possible un retour au droit en même temps qu'il affranchit des contraintes de méthodes exercées par la science juridique. Il libère le cheminement vers des phénomènes juridiques inaperçus* »[17]. A première vue, la répression de la traite des êtres humains et la régulation des nouvelles technologies ne se connectent guère dans le champ juridique. Pourtant, leur interconnexion est nécessaire pour réprimer globalement la cyber-traite. Cette interconnexion offre une nouvelle perspective sur la théorie de la souveraineté. Ainsi, cette étude applique la méthodologie du *feminist practical reasoning* : « *le point de départ féministe est l'expérience humaine réelle et ses implications* »[18]. La méthode est pragmatique et inductive, puisqu'il consiste en un questionnement particulier, ici, une étude de cas, pour interroger une théorie juridique[19].

---

[12] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, Dalloz, Méthodes du droit, 2e édition, 2016, p. 346-348

[13] B. Lavaud-Legendre, *Approche globale et traite des êtres humains - De l'« injonction à la coopération » au travail ensemble*, CNRS, 1 juillet 2018, en ligne https://halshs.archives-ouvertes.fr/halshs-02177213 (consulté le 29 octobre 2021)

[14] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit nº 25, 2016, p. 376

[15] J. Carbonnier, *Flexible droit: pour une sociologie du droit sans rigueur*, Librairie Générale de Droit et de Jurisprudence, 7e éd., 1992, p. 25

[16] L. Lalonde, « L'interdisciplinarité comme « contextes », quels usages de l'Autre ? », *in* Journée d'étude sur la méthodologie et l'épistémologie juridiques, G. Azzaria (dir.), *Les cadres théoriques et le droit: actes de la 2e Journée d'étude sur la méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2013, p. 394, 404

[17] V. Forray, S. Pimont, *Décrire le droit... et le transformer: essai sur la décriture du droit*, Dalloz, 2017, § 91

[18] G. Binion, « Human Rights: A Feminist Perspective », *Human Rights Quarterly*, Johns Hopkins University Press, 1995, vol. 17, nº 3, p. 513

[19] *Ibid.* p. 516

La traite des êtres humains étant facilitée par les nouvelles technologies, sa répression doit s'adapter. Or, dès lors que les États et les acteurs numériques sont amenés à participer à cette lutte, la théorie de la souveraineté est remise en cause. Plutôt qu'une démonstration en faveur de sa disparition, cette étude vise à repenser les fondements de la théorie de la souveraineté pour offrir une nouvelle perspective quant à son application, en prenant comme cas d'étude la répression de la cyber-traite.

Pour développer cette problématique principale, l'étude est divisée en deux parties. Premièrement, la répression de la cyber-traite suppose de rechercher qui exerce des pouvoirs de contrainte, notamment pour établir les obligations des États en tant que souverains et l'existence de nouveaux souverains, plus précisément pour interroger le rôle des acteurs numériques (partie 1). Dans un second temps, alors que différents souverains émergent, cette étude s'intéresse à l'ordonnancement de la contrainte entre ces derniers, notamment aux stratégies qu'ils développent et à leur impact sur la répression de la cybertraite (partie 2).

Partie 1 : Cybertraite et souveraineté : l'exercice de la contrainte

Au croisement de la cyber-traite et de la souveraineté se pose la question des acteurs appelés à réprimer ce délit. Pour les théoriciens du droit, cette question n'a pas de sens : la souveraineté est détenue par les États. L'État est considéré comme un système fermé, une pyramide de normes se légitimant elle-même. En premier lieu, pour réprimer la cyber-traite, les États mettent en oeuvre des pouvoirs souverains traditionnels (titre 1). Cependant, les caractéristiques des nouvelles technologies soulignent la nécessité de coopérer avec d'autres entités. En particulier, pour réprimer la cyber-traite, l'État ne peut agir en vase clos et les acteurs numériques apparaissent comme des partenaires essentiels. Ainsi, une théorie plus large de la contrainte peut étendre la souveraineté hors de l'État. En appliquant leurs propres formes de contrainte, les acteurs numériques s'érigent en détenteurs complémentaires de souveraineté (titre 2).

Titre 1 : États : appliquer la souveraineté pour réprimer la cybertraite

Les juristes considèrent l'État comme l'institution centrale et souveraine des systèmes juridiques, en particulier pour enquêter, poursuivre et condamner les infractions pénales. En tant que tel, il est l'acteur principal de la répression de la cyber-traite, qui constitue une menace spécifique pour sa souveraineté (chapitre 1). Pièce maîtresse de la contrainte légitime de l'État, le droit pénal fournit des concepts juridiques permettant d'adapter la répression pénale à la cybertraite (chapitre 2).

Chapitre 1 : La nécessité de la souveraineté étatique pour faire face à la cyber-traite

Ce premier chapitre détaille les liens entre la souveraineté des États et la traite des êtres humains, y compris lorsqu'elle est facilitée par les nouvelles technologies. La souveraineté, assimilée à celle des États, est généralement définie par trois éléments : une population, un territoire et un gouvernement. Toutefois, ces composantes sont variables. Leur définition dépend des États et non de la souveraineté. Néanmoins, la traite des êtres humains apparaît comme une menace à ces composantes. La traite, en particulier lorsqu'elle est facilitée par les nouvelles technologies, viole chaque droit fondamental des victimes. Les conséquences de ces violations pourraient être amplifiées par les nouvelles technologies, bien que des études approfondies fassent

encore défaut sur ce sujet. Lorsque la traite est transnationale, elle entrave le contrôle de l'État sur son territoire. Ce défi est d'autant plus important lorsque l'infraction est facilitée par des services du cyberespace, qui n'est pas circonscrit aux frontières nationales. Liée à la corruption, au blanchiment d'argent et aux organisations criminelles, la traite a un impact négatif sur les gouvernements.

Afin de distinguer ce qui est propre à la souveraineté, l'analyse s'appuie ensuite sur le concept de monopole de la contrainte légitime, théorisé par Weber. En questionnant les détenteurs de la souveraineté, il convient non pas de savoir si un détenteur monopolise la contrainte, mais de comprendre qui peut exercer cette contrainte[20] et qui est légitime à la mettre en œuvre. Selon Weber, il existe trois légitimités à l'exercice de la contrainte[21] : la légitimité traditionnelle, la légitimité charismatique et la légitimité légale. Cette dernière a retenu l'attention des juristes, notamment de Kelsen, qui la traduit à travers le principe de légalité. L'ordre juridique étatique monopolise la contrainte en ce sens qu'il crée un cadre permettant de légitimer juridiquement les normes[22]. De cette définition naît le concept d' « État de droit »[23]. Avec l'expansion du monde numérique, l'État peut développer de nouveaux modes de contrainte : une contrainte légitime numérique. Premièrement, une interprétation restrictive inclut la contrainte numérique dans un environnement digital : l'action (la contrainte) et ses conséquences ont lieu dans l'espace numérique. D'une part, une contrainte non numérique peut répondre à un comportement numérique et *vice versa*. D'autre part, la contrainte numérique peut déclencher un comportement dans le monde réel (comportement non numérique) et *vice versa*. En théorisant la contrainte numérique légitime, les États peuvent réaffirmer leur souveraineté, grâce à de nouveaux moyens dédiés à la poursuite des auteurs d'infractions, à la protection des victimes et à la prévention de la traite[24]. Ce rôle de l'État souverain dans la répression de la cybertraite est reconnu au niveau international. Les traités sont principalement neutres sur le plan technologique, mais la jurisprudence de la CEDH crée de nouvelles obligations positives pour l'État pour les adapter aux modes opératoires des auteurs de traite.

Chapitre 2 : L'extension de la souveraineté étatique face à la cyber-traite

Face à la cybercriminalité, de nombreuses modifications pénales visent à renforcer la contrainte numérique et la souveraineté étatique. Ainsi, lorsque la traite comprend des éléments numériques, le rattachement à un seul territoire s'estompe. Par conséquent, les États étendent leur compétence juridictionnelle pour poursuivre les auteurs d'infractions, en modifiant la définition traditionnelle de la territorialité. Cette compétence est en effet une matérialisation de leur souveraineté, en définissant le champ d'application de l'exercice de la contrainte. Pourtant, en raison de la difficulté à élever la traite comme priorité politique, la compétence territoriale ne semble pas être remise en question.

---

[20] M. Eabrasu, « Les états de la définition wébérienne de l'État », *Raisons politiques*, Presses de Sciences Po, 4 mai 2012, vol. 45, nº 1, p. 200

[21] M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, trad. R. Livingstone, p. 34

[22] M. Troper, « Le monopole de la contrainte légitime », *Lignes*, Éditions Hazan, 1995, vol. n° 25, nº 2, p. 36

[23] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit nº 1, 2004, p. 32

[24] Assemblée Générale, « Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons », Organisation des Nations Unies, 30 juillet 2010, A/RES/64/293

Les forces de l'ordre ont besoin de preuves pour parvenir à des condamnations. Étant donné l'évolution de la traite, les moyens de contrainte évoluent en parallèle, ce qui donne lieu à diverses techniques d'enquête numériques (perquisitions numériques, interceptions de communications, cyberinfiltration, géolocalisation, sonorisation, utilisation de drones, accès à la correspondance électronique et piratage informatique légal). Toutes ces techniques sont applicables aux enquêtes contre des faits de traite. Le droit pénal et la procédure pénale, apanages de la souveraineté, sont avant tout nationaux et emploient les formes de contrainte les plus lourdes. Pourtant, malgré l'absence de cadre harmonisé, et bien que les codes espagnol et roumain semblent dépourvus de certaines techniques, les codes réglementent les mêmes techniques. Les États prennent généralement en compte les techniques disponibles, en supposant que le droit évolue constamment pour s'adapter aux nouvelles technologies.

Titre 2 : Acteurs numériques : compléter la souveraineté pour réprimer la cybertraite

Bien que la loi offre de nombreux nouveaux outils, la régulation étatique ne peut être étudiée comme un système fermé. La contrainte numérique légitime de l'État fait face à des défis : la coopération est nécessaire (chapitre 1). Alors que les acteurs numériques apparaissent centraux dans la répression de la traite, les cadres de coopération reconnaissent progressivement leur autonomie et leurs pouvoirs souverains (chapitre 2).

Chapitre 1 : La nécessité de compléter la souveraineté de l'État pour faire face à la cybertraite

La souveraineté étatique repose sur la protection de sa population et de son territoire. Cependant, d'une part, des voix se sont élevées pour attirer l'attention sur la violation des droits fondamentaux dans la régulation des techniques d'enquête numériques, alors que le respect de ces standards est primordial pour l'État de droit. À la lumière de la jurisprudence de la CEDH relative au droit à la vie privée, les régimes de ces techniques semblent instables. Les lois nationales ne se conforment pas à tous les critères de conformité pour toutes les techniques. Cela rend les forces de l'ordre peu aventureuses. Cette instabilité résulte également de l'absence de conformité totale avec les normes relatives au procès équitable, soulignant la mince distinction entre l'agent cyber-infiltré et l'agent provocateur. D'autre part, de nombreuses difficultés pratiques subsistent pour mettre en œuvre ces techniques. Les moyens humains et matériels restent limités, notamment dans le cadre de la lutte contre la traite, en raison de l'absence de spécialisation dans les cyber-enquêtes. Ainsi, la contrainte numérique étatique est limitée et les États doivent compléter leurs pouvoirs par ceux d'autres entités.

La stratégie globale de répression de la traite est complétée par un élément transversal : les partenariats[25]. Un premier niveau a été originellement développé entre États, par le biais de l'assistance mutuelle, ce qui questionne la souveraineté étatique face au droit international et à l'Union européenne. La deuxième strate comprend la société civile, en particulier les organisations non gouvernementales. Cela questionne

[25] Secrétaire général adjoint, « Add 'partnership' to 'three P' agenda of United Nations anti-trafficking protocol, deputy secretary-general urges General Assembly thematic debate », Organisation des Nations Unies, 3 juin 2008, DSG/SM/397-GA/10713-HR/4956

également l'impact de cette répartition des compétences sur la souveraineté étatique. Enfin, les partenariats se tournent vers le secteur des affaires. Ce cadre de coopération est encore limité bien que la participation des acteurs numériques soit incontournable en matière de répression de la cyber-traite.

Chapitre 2 : L'extension de la souveraineté pour réprimer la cyber-traite

Pour mener à bien les enquêtes sur la traite, les États s'appuient sur des cadres nationaux et internationaux pour collaborer avec les acteurs numériques. Les processus de coopération nationaux manquent de « *fiabilité, de transparence, de responsabilité et de sécurité juridique* »[26], y compris lorsqu'il s'agit de poursuivre des faits de traite[27]. Les textes relatifs à l'entraide internationale sont plus fiables, mais il n'existe pas de cadre géographique unifié, et les dispositions relatives au champ d'application matériel et aux procédures sont à peine adaptées à la sécurisation efficace des données dans le cadre des enquêtes sur la traite. Par la suite, d'autres instruments ont pris en compte les besoins en matière de poursuites contre la cybercriminalité, en particulier la convention du Conseil de l'Europe sur la cybercriminalité (2001). Toutefois, cette convention ne permet pas de demander efficacement des données, bien qu'elle soit applicable à la traite des êtres humains. Par conséquent, certains États (les États-Unis et la Belgique) ont proposé de nouveaux mécanismes afin de contourner l'entraide judiciaire, en redéfinissant le principe de territorialité. Cependant, ces solutions non harmonisées remettent en cause la protection des droits fondamentaux et de la souveraineté[28], et les acteurs numériques doivent alors se conformer à des réglementations potentiellement contradictoires [29].

Pour contourner ces difficultés, les réformes ultérieures ont reconnu une autonomie accrue aux acteurs numériques, offrant une approche pragmatique de leur propre souveraineté, interne et externe. La première repose sur des pouvoirs de contrainte sur les sujets tandis que la seconde réside dans l'autonomie au niveau international par l'exclusion négative d'une « *puissance supérieure à l'État* »[30]. Les cadres européens relatifs aux preuves électroniques établissent une souveraineté externe embryonnaire pour les acteurs numériques. Traditionnellement, les sujets des obligations internationales sont les États. Or, ces nouveaux textes formulent de nouvelles obligations pour les acteurs numériques, en reconnaissant leur pouvoir de contrainte. De plus, les acteurs numériques ont un rôle majeur dans la structuration du cyberespace, une forme de souveraineté interne, qui impacte directement sur les enquêtes portant sur des faits de traite. Ainsi, la contrainte des acteurs numériques se manifeste par la mise en œuvre de code (informatique) plutôt que de loi. Les acteurs numériques agissent de manière autonome, face à l'incapacité de l'État à réguler la

[26] Commission européenne, « Security Union facilitating Access to Electronic Evidence », UE, avril 2018, p. 1.
[27] GRETA, « Online and technology-facilitated trafficking in human beings. Full report », Conseil de l'Europe, mars 2022, p. 57
[28] P. Jacob, « La compétence des États à l'égard des données numériques - Du nuage au brouillard… en attendant l'éclaircie ? », *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, n° 3, p. 668
[29] V. Franssen, « The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level Reports: Practitioner's Corner », *European Data Protection Law Review*, 2017, vol. 3, n° 4, p. 540
[30] T. Christakis, *« European Digital Sovereignty »: Successfully Navigating Between the « Brussels Effect » and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, 7 décembre 2020, p. 5; J. Combacau, S. Sur, *Droit international public*, LGDJ, 2014, p. 236

conservation des données et à l'absence de régulation du chiffrement, alors que ces deux sujets sont au cœur des enjeux de la répression de la cyber-traite. En résumé, certaines questions ne reposent plus sur les capacités normatives étatiques, mais sur la manière dont les acteurs numériques codent le cyberespace. Les États veulent contrôler ces derniers, mais leur autorité juridique est limitée par les droits fondamentaux.

Reconnus progressivement comme des partenaires de l'État dans la répression de la traite, les acteurs numériques détiennent des pouvoirs souverains de contrainte. Qualifier les acteurs numériques d'acteurs souverains est disruptif pour les théoriciens classiques du droit, qui conçoivent leurs études sur la base de l'unité étatique. Pourtant, la doctrine élargie appelle depuis un certain temps déjà à la reconnaissance des pouvoirs des entités privées. Au lieu de soutenir une « *post-souveraineté* »[31], la souveraineté pourrait être déconnectée de la théorie de l'État pour souligner les principales entités dotées de pouvoirs d'encadrement et d'application de la contrainte. Les enquêtes des faits de cyber-traite soulignent l'urgence de reconnaître les pouvoirs matériels des acteurs numériques afin d'améliorer leur coopération avec les États. Or, cette cohabitation entre différents détenteurs de souveraineté est inhabituelle dans le cadre juridique classique. Alors, des tensions apparaissent dans l'ordonnancement des pouvoirs entre les souverains, alors qu'il demeure central pour assurer une répression efficace de la cyber-traite.

Partie 2 : Cyber-traite et souveraineté : ordonner la contrainte

Entre les États souverains traditionnels, l'ordonnancement de leur indépendance et de leur contrainte est fixé par le droit international, public et privé. Les acteurs numériques n'étant pas reconnus pleinement comme souverains, leur exercice de la contrainte interroge leur ordonnancement avec les États. Il en résulte un « *rapport de force mais aussi [… une] recherche d'une complémentarité entre intérêts et entre approches* »[32]. Plusieurs États entendent réaffirmer leur souveraineté en appliquant la contrainte, notamment pénale (titre 1). Cependant, pour parvenir à une répression globale de la traite, il convient de favoriser la coordination entre les différentes sources de contrainte et d'inscrire la protection des victimes et l'État de droit dans les interactions entre les souverains (titre 2).

Titre 1 : Exercer la contrainte sur les souverains pour réprimer la cyber-traite

La lutte contre la cyber-traite offre des exemples de la volonté des États d'exercer une contrainte sur les autres souverains, en rechercheant la responsabilité pénale des acteurs numériques (chapitre 1). Toutefois, cette contrainte des acteurs numériques sur la base de politiques étatiques a pour effet d'imposer des orientations nationales à l'échelle mondiale. Ainsi, l'indépendance normative des États est menacée par l'expansion de politiques étrangères à travers les acteurs numériques et les technologies (chapitre 2).

[31] B. Badie, « D'une souveraineté fictive à une post-souveraineté incertaine », *Studia Diplomatica*, Egmont Institute, 2000, vol. 53, nº 5, p. 5-13

[32] C. Husson-Rochcongar, « La gouvernance d'Internet et les droits de l'homme », *in* Q. Van Enis, C. de Terwangne (dir.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 50

Chapitre 1 : Imposer la contrainte étatique par la souveraineté originelle

Criminaliser les entreprises pour leur implication dans un processus de traite fait partie de la stratégie mondiale en la matière. Lorsque les États-Unis et la France ont poursuivi des acteurs numériques dans un objectif de répression de la traite, leur responsabilité pénale a été critiquée. Contrairement aux critiques, cette responsabilité a été constamment élargie. Cependant, la définition de la traite s'accorde difficilement avec le rôle des acteurs numériques dans la facilitation du processus. De plus, ils sont en partie protégés grâce à leur immunité en tant qu'intermédiaires numériques, qui, lorsqu'elle est interprétée de manière large, les soustrait à l'emprise des États. En raison de l'inadéquation de cette souveraineté originelle pour contraindre les nouveaux souverains, les États se sont appuyés sur d'autres stratégies.

A la suite de ces affaires, les États-Unis ont modifié à la fois l'infraction de traite et l'immunité des acteurs numériques. Toutefois, ces modifications ne semblent pas améliorer la répression du phénomène. Néanmoins, les fermetures de sites ont été fructueuses. Ces conséquences résultent de politiques pénales élargies, utilisant un nouveau type de contrôle social qui remet en cause leur légitimité. En effet, dans les sociétés modernes, la loi tend à être considérée comme le noyau de l'État de droit, conduisant « *à la juridicisation intégrale de l'ordre social* »[33]. Pourtant, le droit pourrait ne pas être adapté pour insuffler un contrôle étatique dans la mise en œuvre de la contrainte des acteurs numériques. Cependant, cette moralisation les a indirectement conduits à intérioriser la répression de l'infraction, en dehors de tout cadre légal. Cette intériorisation repose principalement sur la suppression des contenus potentiellement liés à des faits de traite, au détriment de la poursuite des auteurs et de la protection des victimes. En tentant de réaffirmer leur souveraineté, les Etats sont sortis du champ du droit, conduisant à partager davantage les pouvoirs de contrainte avec les acteurs numériques.

Chapitre 2 : Ordonner les souverainetés étatiques à travers les acteurs numériques

Les souverains devraient être indépendants. Cependant, la théorie juridique ne tient pas compte des différences de pouvoirs entre les États[34]. En matière de lutte contre la traite des êtres humains et de régulation d'Internet, les États-Unis peuvent être désignés comme le leader mondial. Au carrefour de ces deux secteurs, ce chapitre souligne un « impérialisme américain désordonné »[35]. Des conséquences directes découlent de l'application de la souveraineté originelle. En imposant leur cadre pénal aux acteurs du numérique, les États-Unis étendent leur approche de la traite des êtres humains, confondue avec le travail du sexe. Or, le travail sexuel fait l'objet de diverses régulations à l'échelle mondiale. Ainsi, cela entrave l'indépendance des États étrangers, soulignant un impérialisme pénal américain. D'autres conséquences, indirectes, sont mises en œuvre par les acteurs numériques. Cela met en évidence

[33] J. Chevallier, *L'État de droit*, LGDJ, Clefs, 6e éd., 2017, p. 59

[34] J. Charpentier, « Le phénomène étatique à travers les grandes mutations politiques contemporaines », *in* Société française pour le droit international (dir.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 25

[35] Delmas-Marty utilise la notion d'impéralisme comme opposé du pluralisme, M. Delmas-Marty, « Les processus de mondialisation du droit », *in* C.-A. Morand (dir.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no 46, 2001, p. 78

l'« impérialisme de plateforme » des États-Unis[36] : les politiques américaines façonnent le contenu en ligne lié à la traite et au travail du sexe par l'intermédiaire d'acteurs numériques. Cependant, les actions judiciaires américaines et la modération des acteurs numériques sont à peine questionnées par les normes européennes relatives aux droits fondamentaux. Bien que la proportionnalité de la saisie d'un site puisse être remise en question au regard des standards de la CEDH, les internautes sont à peine protégés. L'importante marge d'appréciation laissée aux souverains en matière de protection de la morale, ainsi que l'imprécision et la variabilité des critères, ne permettent pas de considérer l'évolution de la modération des contenus comme incompatible avec la liberté d'expression.

Les conséquences des politiques américaines élargies en matière de traite sont également incorporées dans les systèmes d'intelligence artificielle, dédiés au soutien des forces de l'ordre ou à la modération. Cela souligne l'impérialisme américain sur le code, à la fois potentiel et réel. Ces systèmes véhiculent des valeurs et des politiques spécifiques[37]. Leur extension par l'application globale de solutions techniques « *revient à normaliser les systèmes juridiques nationaux en les dépouillant de leurs particularités* »[38]. En ce qui concerne la traite des êtres humains, ils reposent sur une définition nationale spécifique et une représentation de réalités criminologiques nationales particulières, sur des priorités propres en matière de politique criminelle et sur une conception de la traite qui est assimilée au travail du sexe. Ce cadre américain entrave en outre la souveraineté numérique européenne en raison de l'absence de prise en compte de la protection des données dès la conception des systèmes. De plus, les normes de protection des données personnelles ne prennent pas en compte les spécificités de l'intelligence artificielle. L'UE tente de renforcer les normes applicables à l'intelligence artificielle pour protéger sa souveraineté technique, mais elles restent pour l'instant limitées.

Titre 2 : Renforcer la collaboration entre souverains pour réprimer la cyber-traite

L'application de la contrainte entre les acteurs souverains pour réprimer la cyber-traite est critiquée. En conséquence, d'autres relations se sont développées pour coordonner la collaboration entre les souverains. D'un contrôle descendant mandaté par les Etats par le biais du droit pénal, d'autres cadres juridiques mettent en œuvre une collaboration ascendante qui se fondent sur les principes de l'État de droit, notamment la protection des droits fondamentaux. Premièrement, la responsabilité sociale des entreprises et la compliance offrent de nouvelles modalités de coordonnation pour lutter contre la traite (chapitre 1). Deuxièmement, la jonction des souverains aux individus et aux collectifs est nécessaire pour assurer une protection des victimes et la prévention du phénomène, et ainsi légitimer pleinement les nouveaux souverains (chapitre 2).

[36] D.Y. Jin, « Facebook's Platform Imperialism: The Economics and Geopolitics of Social Media », *in* O. Boyd-Barrett, T. Mirrlees (dir.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, p. 189-190

[37] K. Crawford, *Atlas of Ai: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, p. 8

[38] G. Kettani, « Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique », *Dalloz IP/IT*, Dalloz, 2022, p. 556

Chapitre 1 : Coordonner la contrainte par une souveraineté souple

Quand les États visent à appliquer leur souveraineté originelle aux acteurs numériques qui facilitent la cybertraite, ces derniers intégrent sa répression dans leurs politiques. Ces initiatives privées font face à des critiques que le droit pénal ne peut résoudre. La responsabilité sociale des entreprises, qui découle d'une version souple de la souveraineté, permet d'instiller les principes de l'État de droit dans ces initiatives. La traite des êtres humains est visée, explicitement ou comme une violation des droits fondamentaux, par les principales normes de compliance. Pourtant, celles-ci ne prennent guère en compte l'impact de la digitalisation sur les droits fondamentaux ni le rôle des acteurs numériques. En outre, elles sont principalement limitées aux grands acteurs privés et ont des difficultés à s'étendre aux acteurs étrangers. Aussi, les normes nationales et européennes sont affaiblies par les limites de la transparence et des moyens d'exécution, et leur imprécision. L'État n'apparaît qu'en tant qu'intermédiaire qui établit une orientation juridique sur la contrainte numérique des acteurs numériques pour réprimer la traite. Bien que l'on puisse y voir le début d'une corégulation et d'une collaboration entre souverains, l'équilibre demeure en faveur des acteurs privés. Les systèmes de compliance actuels soutiennent leur indépendance et leurs pouvoirs souverains, mais ils limitent l'exportation des valeurs pour protéger les souverainetés européennes.

Dès lors, l'UE a développé de nouvelles formes de compliance dédiées aux acteurs numériques pour protéger les valeurs européennes. Les normes régulant les activités numériques envisagent à peine la répression de la traite, tandis que les normes de lutte contre la traite envisagent à peine l'utilisation de normes appliquées aux activités et acteurs numériques. Pourtant, le Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et la Proposition de la Commission européenne du 21 avril 2021 de règlement du Parlement Européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) offrent des champs d'application larges, appropriés pour inclure les activités liées ou appliquées à la répression de la cyber-traite, telles que l'utilisation de systèmes d'intelligence artificielle et la modération de contenu. Leur potentiel effet Bruxelles[39] contribue à protéger l'indépendance des souverainetés de l'UE. En effet, les deux textes s'appliquent en fonction de critères liés au marché, en lieu et place de l'exigence juridique artificielle d'établissement. Pourtant, la protection des souverainetés européennes est toujours limitée par le recours aux définitions nationales du « contenu illégal ». La définition de la traite, bien qu'harmonisée, ne bénéficie pas d'une définition similaire dans tous les États membres. En dépit de certaines critiques, la compliance développe d'autres relations juridiques entre les acteurs numériques et les États afin d'améliorer leur coordination dans la répression de la cyber-traite.

Chapitre 2 : Connecter les souverainetés par la légitimité

La responsabilité sociale des entreprises et des acteurs numériques vise une coordination entre États et acteurs privés. Pour élaborer des politiques de lutte contre la cyber-traite respectueuses des droits fondamentaux, il convient de prendre en compte les relations entre les acteurs numériques et les personnes, en particulier les victimes de la traite. La souveraineté pragmatique des acteurs numériques repose sur

[39] A. Bradford, *The Brussels effect: how the European Union rules the world*, Oxford University Press, 2020

une reconnaissance empirique de leur pouvoir. Cependant, elle n'est guère soutenue par une légitimité. Alors que le rôle actuel des acteurs numériques repose principalement sur une approche sécuritaire de la traite, la protection et la prévention sont nécessaires pour légitimer pleinement leurs actions. Une approche fondée sur les droits fondamentaux n'est pas suffisante pour aborder les opportunités que les acteurs numériques peuvent offrir aux victimes. Alors que leur rôle est limité dans le cadre d'une procédure pénale et du statut de victime, le statut d'utilisateur ou utilisatrice de leurs services ouvre de nouvelles perspectives. Grâce à la protection des données personnelles (par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) et aux droits liés à leur environnement en ligne (par le règlement sur les services numériques), le droit offre de nouvelles relations entre les acteurs numériques et les victimes potentielles ou réelles, sur trois niveaux. Premièrement, les droits fondamentaux fournissent une orientation générale. Deuxièmement, la loi définit des droits spécifiques sur cette base. Enfin, le code informatique met en œuvre ces droits. La légitimité pragmatique de la souveraineté d'un État dépend désormais de sa relation avec les acteurs numériques pour obtenir ou appliquer des moyens de contrainte. La légitimité pragmatique de la souveraineté des acteurs numériques dépend également de l'intermédiation par le droit étatique des droits et des objectifs d'intérêt général pour les transcrire ensuite en moyens numériques.

La souveraineté pragmatique manque encore de bases solides pour être pleinement légitime et les connections nécessaires à sa mise en œuvre remettent en question l'indépendance en tant que composante de la souveraineté. L’origine de cette notion, en particulier la division public/privé, est très critiquée. Cette division semble fluide, presque disparue, en particulier dans le cyberespace. Pourtant, la traite requiert l’intervention de la sphère publique. La sphère privée est alors effacée pour légitimer le plein exercice de la contrainte des souverains. Cependant, cette opposition binaire complique une répression globale de la traite, en effaçant la notion d'agentivité des individus. De plus, la notion d'indépendance occulte les possibilités d'action collective, notamment en matière de prévention. Par conséquent, la légitimation de la souveraineté semble nécessiter des liens d'interdépendance forts. Cette étude offre une proposition méthodologique pour légitimer les actions des souverains interdépendants. Tout d'abord, il convient de définir des valeurs fondamentales interdépendantes. Cela implique d’admettre que la neutralité n’exclut pas l'implication des acteurs privés dans la définition des valeurs. Deuxièmement, la mise en œuvre de ces valeurs pourrait s'appuyer sur de nouvelles passerelles entre les souverains et les individus. Dans ce cadre, des réseaux interconnectés sont nécessaires pour inclure tous les acteurs concernés par la répression de la traite.

Conclusion générale

La répression de la cyber-traite constitue une étude de cas dans l'application de la théorie de la souveraineté. Si celle-ci est liée à l'exercice de la contrainte, elle peut alors être déconnectée de l'Etat. Cette déconnexion apparaît clairement en raison des limites de l’action de l’Etat dans la mise en œuvre de la contrainte. Alors que le droit reconnaît de manière croissante et pragmatique le pouvoir des acteurs numériques d'exercer une contrainte par leur contrôle sur les données, et leur indépendance grandissante pour ce faire, ces acteurs semblent s'inscrire dans une définition de la souveraineté, déconnectée des États. Pourtant, les États sont toujours souverains. Dès lors, plusieurs sources de contrainte apparaissent et plusieurs types de relations

se développent entre elles. Premièrement, l'imposition de la contrainte entre souverains entrave à la fois l'exercice indépendant de la contrainte, et donc leur souveraineté, mais aussi la répression efficace de la traite des êtres humains. Deuxièmement, la collaboration entre souverains se révèle être une stratégie permettant de protéger la souveraineté de chacun et de s'orienter vers une répression globale de la cyber-traite. Toutefois, dans un contexte juridique axé sur la responsabilité sociale des entreprises, la collaboration n'a encore qu'un impact limité sur les victimes de la traite. Pour étendre le rôle des acteurs numériques, il convient de dépasser une approche sécuritaire et de mettre en œuvre les droits fondamentaux par le biais d'une approche pragmatique. En dehors du droit pénal, les acteurs numériques peuvent avoir des obligations utiles à l'assistance des victimes de traite, grâce au contrôle de leurs données. Ici, l'État apparaît comme un intermédiaire dans la mise en œuvre des droits fondamentaux, tandis que les acteurs numériques sont les véritables responsables de leur application. Ce cadre de collaboration reconnaît différents pouvoirs de contrainte tout en protégeant les normes de l'État de droit. En outre, ce cadre remet en question les fondements de la théorie de la souveraineté.

La théorie de la souveraineté repose sur l'indépendance des souverains. Cependant, ce critère entrave une réponse globale à la traite, ainsi que les pouvoirs de contrainte des souverains. L'indépendance reste nécessaire pour délimiter négativement la souveraineté : elle en fixe les limites. Pourtant, l'indépendance ne suffit pas à mettre en œuvre et à légitimer les normes, en particulier en matière de droits fondamentaux et de lutte contre la traite. Un nouveau critère pourrait alors fonder la légitimité des acteurs souverains : l'interdépendance. Ce concept pourrait être développé à travers une théorie générale, notamment basée sur des valeurs fondamentales partagées, et une mise en oeuvre concrète, par exemple en établissant des processus de connexion entre les différents acteurs de la société. Cette approche de la souveraineté en tant qu'interdépendance conduit à trois commentaires.

La répression de la cyber-traite nécessite de faire appel à des cadres juridiques divers. Tout d'abord, cela questionne la stratégie visant à adopter une loi globale pour réprimer la traite[40]. Cette stratégie reconnaît la nécessaire interdisciplinarité de la lutte contre la traite, notamment en allant au-delà du droit pénal. Il s'agit en particulier de rassembler les droits des victimes dans un cadre unique, afin d'obtenir une vision plus claire au lieu de droits éparpillés. Cependant, cette étude souligne que l'assistance et la protection des victimes de la traite ne devraient pas se limiter à leur statut de victime dans le cadre d'une procédure pénale. En particulier, la répression de la cyber-traite souligne l'importance de renforcer la protection de leurs données personnelles et le contrôle de leur environnement en ligne. Il pourrait donc sembler superficiel de limiter le cadre de la lutte contre la traite à une loi globale. De plus, la plupart des défis à la répression de la traite ne sont pas propres à cette infraction : une amélioration du cadre juridique uniquement pour réprimer la traite pourrait ne pas être adaptée. Deuxièmement, cette étude questionne la nécessité de focaliser les actions de prévention à l’existence de ce phénomène. L’infraction fut créée pour faciliter la coopération entre Etats et le contrôle des migrations : à l’origine, les actions préventives étaient fortement limitées, notamment aux contrôles aux frontières. Au-delà de cette approche restrictive, le phénomène met en lumière des vulnérabilités structurelles de la société. Si la définition de la traite est nécessaire à sa répression,

[40] Par exemple, en Espagne, P. Lloria García, « El delito de trata de seres humanos y la necesidad de creación de una ley integral », *Estudios Penales y Criminológicos*, 22 juin 2019, vol. 39, p. 353; C. Villacampa Estiarte, « ¿Es necesaria una ley integral contra la trata de seres humanos? », *Revista General de Derecho Penal*, Iustel, 2020, nº 33, p. 16

cette perspective pénale semble insuffisante pour une prévention intégrale du phénomène. Le renforcement des capacités individuelles comme collectives et des actions de prévention visant des inégalités et des violations des droits fondamentaux structurelles pourraient contribuer à la prévention de la traite. L'alphabétisation numérique, l'éducation sexuelle et affective, une culture du respect et du consentement, le développement d'opportunités de vie, pourraient contribuer à la prévention de la traite. Cela interroge à la fois le rôle des droits fondamentaux et du droit, et sa relation avec l'alphabétisation juridique et d'autres types de normes et d'actions.

La multiplication des entités souveraines interroge leur collaboration pour la répression de la traite, mais aussi, de manière générale, pour la régulation et la mise en œuvre des droits fondamentaux. Elle conduit aujourd'hui à « *l'absence d'un pouvoir clairement assignable au titre de débiteur de ces droits* »[41]. Pourtant, dans le cadre du cyberespace, un changement de mentalité semble s'opérer. Les acteurs numériques sont généralement considérés comme des intermédiaires qui permettent la mise en relation des personnes. La reconnaissance de souverains interdépendants offre une nouvelle compréhension de l'intermédiation. D'une part, les acteurs numériques apparaissent comme des intermédiaires dans la mise en œuvre des droits fondamentaux, protégés à l'origine par les États et en faveur des personnes/internautes. D'autre part, les États sont des intermédiaires pour les acteurs numériques face aux personnes/internautes en leur fournissant un cadre et des outils pour légitimer leurs actions. Cependant, en partie à cause d'une compréhension traditionnelle de la souveraineté et d'une approche principalement capitaliste et néolibérale du secteur des affaires, cette interconnexion manque d'une théorie générale. Pour l'instant, elle n'est adoptée qu'au cas par cas, en particulier pour la régulation de la vie en ligne. Pourtant, une protection complète des droits fondamentaux exige d'aller au-delà des dispositions abstraites et d'en déduire des mesures concrètes pour assurer leur protection. Étant donné que le processus démocratique traditionnel n'est pas appliqué, voire pas applicable, aux acteurs numériques, cette théorie générale et ses processus de mise en œuvre devraient chercher de nouvelles bases de légitimité. Un tel processus soutiendrait, en premier lieu, une discussion autour des valeurs, à la fois en tant qu'orientation générale et au niveau de l'application individuelle et collective. Pour l'instant, les droits fondamentaux « *exprime[nt] un système de croyances proprement occidentales* », complété par d'autres structures d'oppression[42]. Cette nécessaire et constante rétroaction de l'universel sur les applications concrètes souligne que « *l'idée de Droit ne saurait prétendre à l'universalité* » pour bénéficier d'une légitimité intégrale[43]. Pour définir ces valeurs, de nouveaux ponts pourraient être et sont construits entre les acteurs, dans l'espoir d'améliorer la communication et la compréhension commune.

Alors que les droits fondamentaux constituent un cadre général qui manque d'orientations pour une mise en œuvre quotidienne, le concept de droit est censé parvenir à la généralité. Cependant, cette étude sur les outils juridiques pour réprimer la cyber-traite a mis en évidence une dégradation de la qualité du droit en tant qu'outil général. Il est de plus en plus technique et sectoriel. Les réglementations ne sont pas modifiées en profondeur, ce qui entraîne des problèmes d'interprétation, un manque de garanties et, de manière générale, une diminution de la force légitime du droit

[41] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.* note 14, p. 494
[42] A. Supiot, *Homo juridicus essai sur la fonction anthropologique du droit*, Éditions du Seuil, 2005, p. 283
[43] *Ibid.* p. 284

étatique. Comme l'a théorisé Emeric sous la notion de « droit fluide », le droit « *est d'abord le produit d'un discours politique, un idéal de réformateurs, une présentation marketing du droit* »[44]. Le droit, et plus particulièrement le droit pénal, est perçu comme un outil permettant de résoudre des problèmes sociaux. Le droit est magnifié comme une solution, notamment aux défis posés par les nouvelles technologies. Or, ce solutionnisme juridique poussé à l'extrême oublie d'autres systèmes et espaces de régulation des comportements, comme l'éducation ou la structuration du cyberespace. Comme le souligne la question suivante : « *confondons-nous un outil technique avec la culture qui l'utilise pour nuire ?* »[45]. Si d'autres sources de normes, y compris privées, ont un impact et une contrainte potentielle sur les personnes, les juristes pourraient vouloir étendre leur regard en dehors du droit étatique. Si le droit est un outil destiné à promouvoir des valeurs, à ordonner la société et à résoudre des problèmes sociaux, son étude approfondie ne devrait pas faire l'impasse sur la prise en compte de la réalité de sa mise en œuvre, de l'impact des structures sociales et économiques préexistantes et de la flexibilité nécessaire pour évoluer au rythme de la société.

[44] N. Emeric, « Droit souple + droit fluide = droit liquide. Réflexion sur les mutations de la normativité juridique à l'ère des flux », *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, nº 2, p. 33

[45] K. Maltzahn, *Digital dangers Information & communication technologies and trafficking in women*, APC-200608-WNSP-I-EN-P-0024, Association for progressive communications, Issue Papers, août 2006, p. 2

RESUMEN [SPANISH VERSION]

Título: Nuevas tecnologías y trata de seres humanos - Una perspectiva desde la teoría de la soberanía

Palabras claves: trata de seres humanos; nuevas tecnologías; soberanía; actores digitales; deber de protección; coerción legítima; alianzas; competencia jurisdiccional; diligencias de investigación tecnológicas; derecho a la vida privada; garantías procesales; pruebas electrónicas; conservación de datos; cifrado; responsabilidad penal de las empresas; responsabilidad de los intermediarios en línea; política criminal; trabajo sexual; moderación de contenidos; protección de datos personales; inteligencia artificial; responsabilidad social de las empresas; responsabilidad social digital; protección de las víctimas; prevención de la trata; interdependencia.

Introducción

Los avances tecnológicos abren nuevas oportunidades a los criminales y, en particular, contribuyen a facilitar los procesos de trata de seres humanos. El uso de las tecnologías por autores de trata se ha acuñado como cibertrata[1] o e-trata, definida en sentido amplio como «*la trata de seres humanos facilitada o permitida o regulada mediante el uso de [nuevas tecnologías]*»[2]. El delito se define en el Protocolo adicional a la Convención de las Naciones Unidas contra la delincuencia organizada para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños (2000). Los elementos para constituir el delito de trata son los siguientes: deben probarse actos materiales específicos del proceso de trata, como la captación de víctimas; esos actos deben cometerse a través de medios específicos que anulen el consentimiento de la víctima[3], como la fuerza o el engaño; la trata tiene una intención específica, la explotación de la víctima.

Las oportunidades de comisión del delito se multiplican para los tratantes con la digitalización. En este estudio, las nuevas tecnologías, en sentido amplio, «*se refieren a las tecnologías de la información y la comunicación, en particular las que constituyen entornos digitales y en red*»[4] e incluye «*todas las técnicas utilizadas en el tratamiento y transmisión de la información*»[5], con especial atención a Internet. La digitalización facilita el acceso a todos los actores, la asequibilidad de las herramientas y servicios

---

[1] V. Greiman, C. Bain, «The Emergence of Cyber Activity as a Gateway to Human Trafficking», *International Journal of Cyber Warfare and Terrorism*, 2012, vol. 12, n.º 2, p. 29; A. Sykiotou, «Cyber trafficking: recruiting victims of human trafficking through the net», *en* N.E. Kourakēs, C.D. Spinellis (eds.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017, p. 1549

[2] S. Milivojević, «Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus», *en* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, pp. 28-44

[3] Por lo que el consentimiento no es un elemento del delito.

[4] H. Watson, A. Donovan, «Role of technology in human trafficking», *TRACE*, octubre de 2015, p. 3

[5] M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 15

utilizados, y el anonimato[6] para la comisión de la trata. En general, los tratantes aprovechan las oportunidades que ofrece Internet para cada fase del proceso de trata.

Estas prácticas delictivas, facilitadas o no por la tecnología, atentan contra valores protegidos tanto en el ámbito nacional como supranacional: los derechos fundamentales, en particular, la dignidad y la integridad de las personas. Por consiguiente, los Estados ejercen poderes coercitivos, necesarios para luchar contra la trata, y que evolucionan en respuesta a la digitalización de este fenómeno. Estos poderes estatales remiten a la teoría de la soberanía y están legitimados por ella. Es, según Bodin, el «*poder absoluto y perpetuo de una República*»[7]. Sin embargo, esta teoría tradicional se enfrenta a desafíos como la digitalización. En consecuencia, se ha desarrollado un nuevo concepto: la soberanía digital. Desde una perspectiva positiva, «*es la expresión [del] control sobre el espejo virtual de la economía y la población*»[8]. Desde una perspectiva negativa, se subraya las dificultades de los Estados para regular dichos espacios, compitiendo con entidades privadas[9]. Para nombrar a entitades privadas del sector digital se utiliza el concepto amplio de actores digitales, para destacar su papel activo en la configuración de las nuevas tecnologías, la experiencia en línea y, últimamente, la represión de la trata.

En relación a la metodología, cabe mencionar las diferentes pautas de este estudio, centrado en una perspectiva jurídica.

En primer lugar, dado que tanto la soberanía como la trata tienen varias vertientes nacionales como internacionales, este estudio aplica una metodología comparativa. El derecho comparado permite estudiar cómo interactúan las soberanías nacionales, y pone de relieve diferencias, puntos comunes[10], deficiencias y buenas prácticas[11]. Esta investigación desarrolla principalmente el estudio de cuatro ordenamientos jurídicos nacionales. Francia y España constituyen el núcleo de este estudio, y representan sistemas de Europa occidental de derecho civil. La selección de dos sistemas similares pone de relieve las diferencias que subsisten entre sus marcos jurídicos a pesar de su proximidad geográfica. Rumanía aporta la perspectiva de un país de Europa del Este. Los tres países han adoptado marcos jurídicos armonizados por su pertenencia a la UE, pero persisten diferencias en algunos elementos jurídicos e institucionales. Además, los Estados Unidos tienen una fuerte influencia en la represión global de la trata, y aporta una perspectiva de derecho anglosajón.

En segundo lugar, este estudio desarrolla una metodología interdisciplinar, a través de una «*articulación de conocimientos entre disciplinas que desarrollan temas que se solapan parcialmente*»[12]. La investigación no se limita al derecho penal: tanto la teoría de la soberanía como la represión de la trata requieren de diversas disciplinas jurídicas

---

[6] A. Cooper, «Sexuality and the Internet: Surfing into the New Millennium», *CyberPsychology & Behavior*, enero de 1998, vol. 1, n.º 2, p. 187

[7] J. Bodin, *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie n.º 4619, 1993, p. 111

[8] S. Guillou, *La souveraineté numérique française passera par l'investissement dans les technologies numériques*, Sciences Po Paris, Chaire Digital, Gouvernance, et Souveraineté, 2020, p. 3

[9] F. G'Sell, «Remarques sur les aspects juridiques de la " souveraineté numérique "», *La revue des juristes de Sciences Po*, 2020, n.º 19, p. 52

[10] M. Durán Bernardino, «El método comparado en los trabajos de investigación», *en* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 49

[11] V. Robert, L. Usunier, «Conclusion. Du bon usage du droit comparé», *en* M. Delmas-Marty, Université de Paris I: Panthéon-Sorbonne (eds.), *Critique de l'intégration normative: l'apport du droit comparé à l'harmonisation des droits*, Presses Universitaires de France, Les voies du droit, 1.ª ed., 2004, p. 231

[12] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, Dalloz, Méthodes du droit, 2e édition, 2016, pp. 346-348

para su estudio exhaustivo[13]. Además, las ciencias jurídicas se encuentran muy unidas a las ciencias políticas: varias normas analizadas han sido y siguen siendo negociadas y reformadas. Así, «*entre el derecho y la política, la determinación es recíproca, y la implicación mutua es constante*»[14]. En consecuencia, el estudio de los textos jurídicos no puede separarse de su aplicación.

En tercer lugar, este estudio no se fundamenta en una comprensión del derecho limitada al derecho estatal. La regulación de las nuevas tecnologías como la lucha contra la trata exigen tener en cuenta normas supranacionales y locales, así como normas privadas o reglas incorporadas a las nuevas tecnologías. Esta investigación se enmarca en la hipótesis del pluralismo jurídico: «*el derecho no está solo; coexiste con otros sistemas de normas*»[15].

Por último, este estudio integra otras ciencias sociales, para entender plenamente la trata. De esta forma, el estudio de las nuevas tecnologías requiere de la conceptualización de la ciencia informática. Por consecuencia, otras disciplinas son necesarias tanto para establecer un «*contexto fáctico*» como para ampliar el «*contexto teórico*»[16].

En resumen, esta metodología «*puede describirse brevemente como la asociación de referencias heterogéneas. Se trata de organizar un diálogo con textos no jurídicos [...] Tal método permite recurrir a desplazamientos y conciliaciones, en lugar de recurrir exclusivamente a las operaciones de la lógica jurídica [...] Este «bricolaje» permite volver al derecho al mismo tiempo que nos libera de las limitaciones de los métodos ejercidos por la ciencia jurídica. Libera el camino hacia fenómenos jurídicos inadvertidos*»[17]. A primera vista, la represión de la trata y la regulación de las nuevas tecnologías apenas conectan dentro del ámbito jurídico. Sin embargo, su interconexión es necesaria para una represión integral de la cibertrata. Esta interconexión conlleva una nueva perspectiva sobre la teoría de la soberanía. Asimismo, se aplica una metodología que ya venía dada por el razonamiento práctico feminista desarrollado por las teorías feministas: «*el punto de partida feminista es a partir de la experiencia humana real y sus implicaciones*»[18]. El método es pragmático e inductivo. Mediante la formulación de preguntas particulares y, en este estudio, el establecimiento de un caso práctico se cuestiona la teoría jurídica[19].

Mientras la trata está facilitada por las nuevas tecnologías, su represión debe adaptarse. Sin embargo, en la medida en que los Estados y actores digitales participan en esta lucha, se cuestiona la teoría de la soberanía. En lugar de una demostración a favor de su desaparición, este estudio pretende analizar las bases de la teoría de la

[13] B. Lavaud-Legendre, *Approche globale et traite des êtres humains - De l'« injonction à la coopération » au travail ensemble*, CNRS, 1 de julio de 2018, en línea https://halshs.archives-ouvertes.fr/halshs-02177213 (recuperado 29 de octubre de 2021)

[14] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit n.º 25, 2016, p. 376

[15] J. Carbonnier, *Flexible droit: pour une sociologie du droit sans rigueur*, Librairie Générale de Droit et de Jurisprudence, 7.ª ed., 1992, p. 25

[16] L. Lalonde, «L'interdisciplinarité comme " contextes ", quels usages de l'Autre ?», *en* Journée d'étude sur la méthodologie et l'épistémologie juridiques, G. Azzaria (eds.), *Les cadres théoriques et le droit: actes de la 2e Journée d'étude sur la méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2013, pp. 394, 404

[17] V. Forray, S. Pimont, *Décrire le droit... et le transformer: essai sur la décriture du droit*, Dalloz, 2017, § 91

[18] G. Binion, «Human Rights: A Feminist Perspective», *Human Rights Quarterly*, Johns Hopkins University Press, 1995, vol. 17, n.º 3, p. 513

[19] *Ibid.* p. 516

soberanía para aportar una nueva perspectiva sobre su aplicación, utilizando la represión de la cibertrata como caso práctico.

Para desarrollar esta cuestión central, este estudio se divide en dos partes. En primer lugar, la represión de la cibertrata requiere investigar quién ejerce la coerción con el fin de establecer las obligaciones de los Estados soberanos y la existencia de nuevos actores soberanos, los actores digitales (Parte 1). En segundo lugar, cuando surgen varios actores soberanos, este estudio se centra en el ordenamiento de la coerción entre éstos, en particular las estrategias que desarrollan y su impacto en la represión de la cibertrata (Parte 2).

Parte 1. Cibertrata y soberanía: el ejercicio de la coerción

El estudio de la represión de la cibertrata a través de la soberanía cuestiona cuales son los actores encargados de dicha represión. La respuesta de los teóricos del derecho es simple: los Estados son soberanos. El Estado es un sistema cerrado, organizado por una pirámide de normas, legitimándose a sí mismo. La represión de la cibertrata pone de relieve la relevancia de los actores soberanos tradicionales: los Estados (Título 1). Sin embargo, las características de las nuevas tecnologías subrayan la necesidad de cooperación con otras entidades. En particular, para reprimir la trata, el Estado no puede actuar en un sistema cerrado; su marco jurídico y sus acciones deben complementarse, en particular, con la coerción de los actores digitales. Una teoría más amplia de la coerción puede desvincular el concepto de la soberanía del sistema estatal. Al aplicar sus propias formas de coerción, los actores digitales se erigen en titulares complementarios de la coerción y, por tanto, de la soberanía (Título 2).

Título 1. Aplicar la soberanía de los Estados para reprimir la cibertrata

Los juristas consideran que el Estado es la institución central y soberana de los sistemas jurídicos, en particular para investigar delitos penales. Como tal, es el actor central para reprimir la cibertrata, que amenaza su soberanía (Capítulo 1). El derecho penal, como acervo de la coerción legítima del Estado, proporciona conceptos jurídicos necesarios para adaptar la represión penal a la evolución de la trata (Capítulo 2).

Capítulo 1. La necesidad de la soberanía estatal para afrontar la cibertrata

Este primer capítulo detalla los vínculos entre la soberanía estatal y la trata, incluso cuando está facilitada por nuevas tecnologías. La soberanía, equiparada a los Estados, suele definirse a través de tres componentes: la población, el territorio y el gobierno. Sin embargo, estos conceptos son variables. Por consecuencia, esta definición depende de los Estados, no de la soberanía. No obstante, la trata sobrepasa estos componentes clásicos del Estado. Este delito viola los derechos fundamentales de las víctimas, integrantes de la población del Estado. Las consecuencias podrían verse amplificadas debido a las nuevas tecnologías, aunque todavía faltan estudios exhaustivos. Cuando la trata es transnacional, dificulta el control del Estado sobre su territorio; este reto aumenta cuando los procesos se desarrollan por el ciberespacio. Cuando la trata está vinculada a la corrupción, el blanqueo de dinero, y las organizaciones criminales, también repercute negativamente en los gobiernos.

A continuación, para distinguir lo que es propio a la soberanía, el análisis se apoya en el concepto del monopolio de la coerción legítima, teorizado por Weber. No se trata

de averiguar si alguien monopoliza la coerción, sino de entender quién puede ejercerla de manera legítima[20]. Según Weber, existen tres fundamentos para legitimar la coerción[21]: la legitimidad tradicional, la carismática y la legal. Esta última retiene el interés de los pensadores jurídicos, sobre todo de Kelsen, quien la traduce a través del principio de legalidad. El orden jurídico estatal monopoliza la coerción porque crea un marco para legitimar las normas jurídicamente[22]. A partir de esta definición se creó el concepto de «Estado de derecho»[23]. Con la expansión del mundo digital, el Estado puede desarrollar nuevas formas de coerción: una coerción digital legítima. En primer lugar, una interpretación restrictiva incluye la coerción digital en un entorno digital: la acción (la coerción) y sus consecuencias tienen lugar en el espacio digital. En segundo lugar, un concepto más amplio implica una interacción con la coerción no digital. Por un lado, la coerción no digital puede responder a un comportamiento digital y viceversa. Por otro lado, la coerción digital puede resultar de un comportamiento en el mundo real (no digital) y viceversa. Al teorizar la coerción digital legítima, los Estados pueden reafirmar su soberanía con nuevas formas de perseguir a los autores, de proteger a las víctimas y de prevenir el fenómeno[24]. Dicho papel del Estado soberano en la represión de la cibertrata está reconocido en el marco internacional. Los tratados son mayoritariamente neutrales desde el punto de vista tecnológico, pero la jurisprudencia del TEDH crea nuevas obligaciones positivas para que el Estado tenga en cuenta la evolución de la trata.

Capítulo 2. La extensión de la soberanía del Estado frente a la cibertrata

Frente a los ciberdelitos, numerosas reformas penales pretenden reforzar la coerción digital y la soberanía estatal. En particular, la conexión con un territorio se difumina cuando la trata incluye elementos cibernéticos. En consecuencia, los Estados amplian su competencia jurisdiccional para perseguir a los autores, modificando la definición tradicional de territorialidad. Dicho principio es una materialización de la soberanía, al definir el alcance del ejercicio de la coerción. Sin embargo, debido a la dificultad de plantear la trata como una prioridad política, este tema no parece cuestionarse y estas reformas no parecen aplicarse en materia de cibertrata.

Las autoridades represivas necesitan pruebas para garantizar las condenas. Los medios de coerción evolucionan de manera paralela a la trata, en particular con la adopción de diversas diligencias de investigación tecnológicas (registros −incluso remotos−, interceptación de comunicaciones, agente encubierto informático, captación de la imagen, de seguimiento y de localización, grabación y captación de comunicaciones orales, uso de drones, acceso a la correspondencia electrónica). Todas ellas son aplicables a investigaciones contra la trata. El derecho penal substantivo y procesal, como pináculo de la soberanía, es principalmente nacional. Sin embargo, a pesar de la falta de un marco armonizado, y aunque los códigos español y rumano parecen carecer de ciertas diligencias, las normas de procedimiento

[20] M. Eabrasu, «Les états de la définition wébérienne de l'État», *Raisons politiques*, Presses de Sciences Po, 4 de mayo de 2012, vol. 45, n.º 1, p. 200

[21] M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, trad. R. Livingstone, p. 34

[22] M. Troper, «Le monopole de la contrainte légitime», *Lignes*, Éditions Hazan, 1995, vol. n° 25, n.º 2, p. 36

[23] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit n.º 1, 2004, p. 32

[24] Asamblea General, «Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons», Naciones Unidas, 30 de julio de 2010, A/RES/64/293

penal de los tres países europeos estudiados regulan las mismas diligencias. Los Estados suelen tener en cuenta las técnicas disponibles, asumiendo la constante evolución del derecho para adaptarse a las nuevas tecnologías.

Título 2. Complementar la soberanía con actores digitales para reprimir la cibertrata

Aunque la ley aporta numerosas herramientas nuevas, la regulación estatal no puede estudiarse como un sistema cerrado. Cuando la coerción digital legítima del Estado se enfrenta a retos, es necesaria la cooperación: los actores digitales tienen un rol central en la represión de la trata (Capítulo 1). Por consecuencia, los marcos de cooperación reconocen cada vez más su autonomía y sus poderes soberanos (Capítulo 2).

Capítulo 1. La necesidad de complementar la soberanía estatal para afrontar la cibertrata

La soberanía estatal se fundamenta en la protección de su población y su territorio. Sin embargo, los derechos humanos, vitales para el Estado de Derecho, deben de tenerse en cuenta a la hora de regular las diligencias de investigación tecnológicas. A la luz de la jurisprudencia del TEDH sobre el derecho a la vida privada, los regímenes de estas diligencias no se ajustan a los estándares de protección de los derechos humanos. Eso crea inestabilidad, lo que conlleva que las autoridades represivas sean poco atrevidas en su utilización. Dicha inestabilidad también deriva de una falta de plena conformidad con los estándares del debido proceso, dada la escasa diferencia entre el agente encubierto informático y el agente provocador. Además, existen numerosas dificultades prácticas en la implementación de estas diligencias. Los recursos humanos y materiales siguen siendo limitados, en particular para luchar contra la trata, debido a la ausencia de especialización en las investigaciones digitales. Por tanto, la coerción digital estatal es limitada y los Estados necesitan complementar sus poderes con los de otras entidades.

La estrategia global para reprimir la trata incluye un elemento transversal: las alianzas[25]. En primer lugar, dichas alianzas fueron desarrolladas entre estados soberanos, mediante la asistencia mutua, cuestionando la soberanía estatal frente al derecho internacional y a la UE. En segundo lugar, las alianzas englobaron la sociedad civil, en particular las organizaciones no gubernamentales. Esta extensión cuestiona su impacto en la soberanía con una división de competencias con actores no estatales. En tercer lugar, las alianzas incluyeron el sector empresarial. Este marco de cooperación aún está limitado, aunque la participación de los actores digitales es esencial en la lucha contra la cibertrata.

Capítulo 2. La ampliación de la soberanía frente a la cibertrata

A la hora de llevar a cabo investigaciones contra la trata, los Estados utilizan marcos nacionales e internacionales para colaborar con actores digitales. Los procesos de cooperación nacional carecen de «*fiabilidad, transparencia, responsabilidad y*

[25] Secretario General Adjunto, «Add ‘partnership’ to ‘three P’ agenda of United Nations anti-trafficking protocol, deputy secretary-general urges General Assembly thematic debate», Naciones Unidas, 3 de junio de 2008, DSG/SM/397-GA/10713-HR/4956

seguridad jurídica»[26], incluso a la hora de investigar fenómenos de trata[27]. Tampoco son plenamente eficaces los textos internacionales de asistencia mutua: sus marcos geográficos no son unificados, y sus ámbitos de aplicación y sus procedimientos apenas permiten obtener datos de manera eficaz para la investigación de la trata. Por otra parte, existen otros instrumentos que se dedican a la persecución de la ciberdelincuencia, en particular el Convenio del Consejo de Europa sobre la ciberdelincuencia (2001). Sin embargo, tampoco permite solicitar datos de forma eficaz, a pesar de ser aplicable a la trata. En consecuencia, algunos Estados, como los Estados Unidos y Bélgica, aplicaron nuevas soluciones para eludir la asistencia mutua, con una nueva definición del principio de territorialidad. Sin embargo, estas soluciones no están coordinadas con los demás Estados, por lo que cuestionan la protección de los derechos humanos y la soberanía[28].

Para eludir estos desafíos, las reformas posteriores reconocen una mayor autonomía a los actores digitales, adoptando un enfoque pragmático sobre su soberanía interna y externa. La soberanía interna descansa en poderes de coerción sobre los sujetos; la soberanía externa reside en la autonomía del actor soberano en el contexto internacional mediante la exclusión negativa de «*un poder superior*»[29]. Los marcos europeos sobre pruebas electrónicas construyen un embrión de soberanía externa para los actores digitales. Tradicionalmente, los sujetos de las obligaciones internacionales son los Estados. Sin embargo, los nuevos textos crean nuevas obligaciones para los actores digitales, reconociéndoles sus poderes de coerción. Además, los actores digitales desempeñan un papel fundamental en la estructuración del ciberespacio, una forma de soberanía interna, lo que repercute directamente en las investigaciones contra la trata. La coerción digital de los actores digitales queda demostrada por su control del código informático. Estos actores gobiernan de forma autónoma, en ausencia de regulación estatal sobre la retención de datos y el cifrado, siendo ambos temas, retos centrales para la represión de la cibertrata. En resumen, algunas cuestiones ya no dependen de la capacidad reguladora del Estado, sino de cómo los actores digitales codifican el ciberespacio. Los Estados quieren gobernar a los codificadores, pero su autoridad legal se ve limitada por los derechos fundamentales.

Cada vez más reconocidos como socios del Estado en la represión de la trata, los actores digitales ostentan poderes soberanos de coerción. Calificar a los actores digitales de soberanos es muy disruptivo para los teóricos clásicos del derecho, que se limitan a la unidad estatal. Sin embargo, la doctrina general lleva tiempo reclamando el reconocimiento de los poderes de las entidades privadas. En lugar de apoyar una perspectiva de «*post-soberanía*»[30], la soberanía podría desconectarse de

[26] Comisión europea, «Security Union facilitating Access to Electronic Evidence», UE, abril de 2018, p. 1.
[27] GRETA, «Online and technology-facilitated trafficking in human beings. Full report», Consejo de Europa, marzo de 2022, p. 57
[28] P. Jacob, «La compétence des États à l'égard des données numériques - Du nuage au brouillard… en attendant l'éclaircie ?», *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, n.º 3, p. 668
[29] T. Christakis, *«European Digital Sovereignty»: Successfully Navigating Between the «Brussels Effect» and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, 7 de diciembre de 2020, p. 5; J. Combacau, S. Sur, *Droit international public*, LGDJ, 2014, p. 236
[30] B. Badie, «D'une souveraineté fictive à une post-souveraineté incertaine», *Studia Diplomatica*, Egmont Institute, 2000, vol. 53, n.º 5, pp. 5-13

la teoría del Estado para destacar la coerción ejercida por otras entidades. La investigación de la cibertrata subraya la urgencia de reconocer los poderes materiales de los actores digitales para mejorar su cooperación con los Estados. Sin embargo, esta cohabitación de varios titulares de soberanía es inusual dentro de la ciencia jurídica. Por consecuencia, surgen tensiones en el ordenamiento de poderes entre actores soberanos. Este ordenamiento es fundamental para garantizar una represión eficaz de la cibertrata.

Parte 2. Cibertrata y soberanía: ordenar la coerción

Entre los estados soberanos independentes, el ordenamiento de su coerción lo establece el Derecho internacional público y privado. Dado que los actores digitales no son reconocidos plenamente como soberanos, su ejercicio de la coerción cuestiona su ordenación con la coerción de los Estados. Surge una «*relación de fuerza pero también [...] una búsqueda de complementariedad entre intereses y enfoques*»[31]. Varios Estados pretenden reafirmar su soberanía, ejerciendo coerción, en particular, penal. (Título 1). Sin embargo, para lograr una represión integral de la trata, se favorece la coordinación entre acciones de lucha contra la trata. Dicha coordinación permite integrar la protección de las víctimas y los principios del Estado de derecho dentro de las interacciones entre los actores soberanos (Título 2).

Título 1. Ejercer coerción sobre actores soberanos para reprimir la cibertrata

A través de la lucha contra la cibertrata, se analizan ejemplos de los intentos de los Estados por imponer coerción, en particular la responsabilidad penal, sobre actores digitales (Capítulo 1). Sin embargo, la coerción de dichos actores sobre la base de las políticas de Estados Unidos dio lugar a una expansión de dichas políticas a escala mundial. De este modo, la independencia de los actores soberanos está amenazada a medida que algunas políticas estatales quedan integradas en las políticas de los actores digitales o en las tecnologías que están desarrolladas (Capítulo 2).

Capítulo 1. Imponer la coerción estatal mediante la soberanía primaria

Requerir la responsabilidad de las empresas por estar implicadas en un proceso de trata forma parte de la estrategia global de represión de dicho delito. Cuando los Estados Unidos y Francia procesaron a actores digitales por trata, se cuestionó su responsabilidad penal corporativa. En contra de las críticas, este marco se amplía de manera constante. Sin embargo, la definición de la trata apenas encaja con el papel de los actores digitales en la facilitación del proceso. Además, dichos actores están protegidos parcialmente por su inmunidad como intermediarios digitales, que, interpretada en sentido amplio, los excluye del control estatal. Frente a la insuficiencia de dicha soberanía primaria, los Estados recurrieron a otras estrategias.

Posteriormente, los Estados Unidos modificaron tanto la definición de la trata (con fines de explotación sexual) como la inmunidad de los actores digitales. Sin embargo, dichas reformas no parecen haber mejorado la represión del fenómeno. No obstante, los cierres de sitios web tuvieron éxito. Estas consecuencias son el resultado de políticas criminales extendidas, que utilizan un nuevo tipo de control social, cuya legitimidad se puede cuestionar, dado que queda fuera del marco jurídico. En efecto, en las sociedades modernas, la ley tiende a ser considerada como el núcleo del

[31] C. Husson-Rochcongar, «La gouvernance d'Internet et les droits de l'homme», *en* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 50

Estado de derecho, lo que conduce «*a la juridización completa del orden social*»[32]. Sin embargo, es posible que la ley no sea suficiente para implementar un control estatal sobre los actores digitales o para hacerles tomar conciencia de su papel en la represión de la trata. Por el contrario, las políticas criminales extendidas les llevaron indirectamente a interiorizar la represión del delito, al margen de cualquier marco jurídico. Esta interiorización resulta principalmente en la supresión de contenidos en lugar de la persecución de los tratantes y de la protección de las víctimas. En su intento de resolver el fenómeno a través de la soberanía primaria, los actores soberanos salieron del ámbito de la ley, lo que les llevó a compartir todavía más sus poderes de coerción con los actores digitales.

Capítulo 2. Ordenar las soberanías estatales a través de los actores digitales

Dado que los actores soberanos deberían ser independientes, la teoría jurídica se olvida de las diferencias de poderes entre los Estados[33]. En lo que respecta a la lucha contra la trata y la regulación de Internet, puede decirse que Estados Unidos es el líder mundial en su regulación. En la intersección de ambos sectores, este capítulo subraya un «imperialismo americano desordenado»[34]. Las primeras consecuencias estudiadas en este capítulo son directas y derivan de la aplicación de la soberanía penal estadounidense. Al imponer su marco penal a los actores digitales, Estados Unidos extiende cierto entendimiento de la trata, que se confunde con el trabajo sexual, aunque éste último reciba múltiples regulaciones por el mundo. En consecuencia, obstaculiza la independencia de los demás Estados, subrayando un imperialismo penal estadounidense. Los actores digitales implementan otras consecuencias indirectas. Esto subraya un «*imperialismo de plataforma*»[35] estadounidense: las políticas de dicho país moldean la regulación del contenido en línea relacionado con la trata y con el trabajo sexual, a través de las reglas fijadas por los actores digitales. Sin embargo, las acciones estadounidenses y la moderación de los actores digitales apenas son cuestionadas desde las normas europeas sobre derechos humanos. Aunque la proporcionalidad de la confiscación de la empresa investigada en los Estados Unidos puede cuestionarse en relación con las normas del Convenio europeo sobre derechos humanos, los internautas casi no están protegidos frente a las órdenes de bloqueo. El amplio margen de apreciación concedido a los actores soberanos para la protección de la moral, y la vaguedad y variabilidad de sus criterios no permiten considerar lisa y llanamente la evolución de la moderación de contenidos como incompatible con la libertad de expresión.

Las consecuencias de la ampliación de las políticas estadounidenses sobre la trata también están integradas en sistemas de inteligencia artificial, tanto para respaldar la labor de las autoridades represivas como de moderación de los actores digitales. Esto pone de relieve un imperialismo de código estadounidense, tanto potencial como real.

---

[32] J. Chevallier, *L'État de droit*, LGDJ, Clefs, 6.ª ed., 2017, p. 59

[33] J. Charpentier, «Le phénomène étatique à travers les grandes mutations politiques contemporaines», *en* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 25

[34] Delmas-Marty utiliza la noción de imperialismo frente a la de pluralismo, M. Delmas-Marty, «Les processus de mondialisation du droit», *en* C.-A. Morand (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international n.º 46, 2001, p. 78

[35] D.Y. Jin, «Facebook's Platform Imperialism: The Economics and Geopolitics of Social Media», *en* O. Boyd-Barrett, T. Mirrlees (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, pp. 189-190

Estos sistemas incorporan valores y políticas específicas[36]. Su extensión mediante una aplicación global de soluciones técnicas «*equivale a uniformizar los sistemas jurídicos nacionales despojándolos de sus particularidades*»[37]. En cuanto a la trata, estas soluciones aplican una definición nacional específica, la estadounidense, la representación de realidades criminológicas americanas, priorizando una política criminal enfocada en la trata con fines de explotación sexual y una concepción de la trata que se confunde con el trabajo sexual. Este marco estadounidense obstaculiza aún más la soberanía digital debido a la falta de consideración de la protección de datos en su propio diseño. Además, las normas actuales de protección de datos personales no tienen en cuenta las especificidades de la inteligencia artificial. Finalmente, la UE está intentando reforzar sus normas aplicables a la inteligencia artificial para proteger su soberanía técnica, pero siguen siendo limitadas.

Título 2: Refuerzo de la cooperación entre actores soberanos para combatir la cibertrata

Dado que se critican las estrategias de coerción entre actores soberanos para reprimir la cibertrata, se han desarrollado otras formas de relaciones para coordinar la coerción entre actores soberanos. De manera diferente al control descendente ordenado por los Estados a través del derecho penal, otros marcos jurídicos implementan una colaboración ascendente a través los principios del Estado de Derecho, incluidos los derechos fundamentales. En primer lugar, la responsabilidad social de las empresas y la compliance ofrecen nuevas herramientas para coordinar la lucha contra la trata (Capítulo 1). En segundo lugar, el vínculo entre actores soberanos e individuos y colectivos es necesario para garantizar la protección de las víctimas y la prevención de la trata, y legitimar plenamente a los nuevos actores soberanos (Capítulo 2).

Capítulo 1: Coordinar la coerción mediante una soberanía flexible

Cuando los Estados aplican su competencia penal sobre actores digitales cuando facilitan la cibertrata, estos últimos, en reacción, desarrollan iniciativas privadas para luchar contra el fenómeno. Dichas iniciativas reciben críticas que el derecho penal no puede resolver. La responsabilidad social de las empresas, derivada de una versión flexible de la soberanía, permite inculcar los principios del Estado de Derecho en estas iniciativas. La trata está contemplada, explícitamente o como violación de los derechos fundamentales, por las normas principales de compliance. Sin embargo, dichas normas apenas tienen en cuenta el impacto de la digitalización en los derechos fundamentales ni el papel de los actores digitales. Además, se limitan principalmente a grandes actores privados y tienen dificultades para extenderse a los actores extranjeros. Las normas nacionales y europeas también se ven debilitadas por las limitaciones de las normas de transparencia, por sus medios de ejecución, y por su imprecisión. El Estado sólo aparece como un intermediario que establece orientaciones jurídicas a los poderes de coerción de los actores digitales dedicados a la represión de la trata. Aunque estos marcos se pueden considerar como el inicio de una co-regulación y de una colaboración entre los actores soberanos, la balanza sigue

[36] K. Crawford, *Atlas of Ai: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, p. 8

[37] G. Kettani, «Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique», *Dalloz IP/IT*, Dalloz, 2022, p. 556

inclinándose a favor de los actores privados. Los sistemas actuales de compliance respaldan su independencia y sus poderes soberanos, pero limitan la exportación de valores necesarios para proteger las soberanías europeas.

En consecuencia, la UE ha desarrollado nuevas formas de compliance dedicadas a los actores digitales. Las normas que regulan las actividades digitales apenas contemplan la represión de la trata, mientras que las normas de lucha contra la trata apenas contemplan el uso de normas aplicadas a las actividades y actores digitales. Sin embargo, el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y la Propuesta de la Comisión Europea del 21 de abril de 2021 del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) ofrecen amplios ámbitos de aplicación, apropiados para incluir actividades vinculadas o aplicadas a la represión de la cibertrata, como el uso de sistemas de inteligencia artificial y la moderación de contenidos. Su posible efecto Bruselas[38] contribuye a proteger la independencia de las soberanías dentro de la UE. En efecto, ambos textos se aplican sobre la base de criterios relacionados con el mercado, en lugar del criterio artificioso del lugar de establecimiento. Sin embargo, la protección de la soberanía europea sigue estando limitada por la utilización de las definiciones nacionales de «contenido ilícito». La definición de la trata, aunque armonizada, no se beneficia para integrar una definición igual en todos los Estados miembros. A pesar de ciertas críticas, la compliance desarrolla otras relaciones jurídicas entre los actores digitales y los Estados para mejorar su coordinación en la represión de la cibertrata.

Capítulo 2: Conectar soberanías a través de la legitimidad

La responsabilidad social de las empresas y de los actores digitales favorece la coordinación entre los Estados y los actores privados. Pero para desarrollar políticas de lucha contra la cibertrata que respeten los derechos fundamentales, es necesario tener en cuenta también las relaciones entre los actores digitales y los individuos, en particular las víctimas de la trata. La soberanía pragmática de los actores digitales se fundamenta en un reconocimiento empírico de su poder. Sin embargo, apenas está respaldada por la legitimidad. Si bien el papel actual de los actores digitales desarrolla principalmente un enfoque securitario de la trata, la protección y la prevención son necesarias para legitimar plenamente sus acciones. Un enfoque desde los derechos fundamentales no es suficiente para estudiar las oportunidades que los actores digitales pueden ofrecer a las víctimas de la trata. Si bien su papel es limitado en el contexto de los procedimientos penales y la condición de víctima, la condición de usuario o usuaria de sus servicios abre nuevas perspectivas. Gracias a la protección de los datos personales (a través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) y los derechos relacionados al entorno en línea (a través del reglamento de servicios digitales), el derecho ofrece nuevas relaciones entre los actores digitales y las víctimas potenciales o reales, en tres ámbitos. En primer lugar, los derechos fundamentales proporcionan una orientación general. En segundo lugar, las normas definen derechos específicos para desarrollar dichos conceptos abstractos. Por último, el código informático aplica estos derechos. La legitimidad pragmática de la

[38] A. Bradford, *The Brussels effect: how the European Union rules the world*, Oxford University Press, 2020

soberanía de un Estado depende ahora de su relación con los actores digitales para obtener o aplicar medios de coacción. La legitimidad pragmática de la soberanía de los actores digitales depende también de la intermediación del derecho estatal en los derechos y objetivos del interés general, que luego se transcriben en medios digitales.

La soberanía pragmática sigue careciendo de una legitimidad plena, y las conexiones necesarias para ponerla en práctica cuestionan la independencia como componente de la soberanía. Los orígenes de esta noción, en particular la división entre lo público y lo privado, son muy criticados. Esta división parece fluida, casi desaparecida, sobre todo en el ciberespacio. Sin embargo, la trata requiere la intervención de la esfera pública. La esfera privada se borra para legitimar el pleno ejercicio de la coerción soberana. Sin embargo, esta oposición binaria complica una represión global de la trata, al borrar la noción de agentividad de los individuos. Además, la noción de independencia oscurece las posibilidades de acción colectiva, en particular en materia de prevención. En consecuencia, la legitimación de la soberanía parece requerir fuertes vínculos de interdependencia. Este estudio ofrece una propuesta metodológica para legitimar las acciones de los actores soberanos interdependientes. En primer lugar, es necesario definir los valores fundamentales interdependientes. Eso significa admitir que la neutralidad no excluye la participación de actores privados en la definición de los valores. En segundo lugar, la aplicación de estos valores podría basarse en nuevos puentes entre los actores soberanos y los individuos. En este contexto, se necesitan redes interconectadas que incluyan a todos los actores implicados en la represión de la cibertrata.

Conclusión general

La represión de la cibertrata se ha estudiado como un caso práctico para analizar la aplicación de la teoría de la soberanía. Cuando dicha teoría se vincula al ejercicio de la coerción, puede ser desconectada del sistema estatal. Esta desconexión se desprende claramente de los límites de la acción del Estado en la aplicación de la coerción. Dado que la ley reconoce cada vez más y de forma pragmática el poder de los actores digitales para ejercer coerción de manera independiente a través de su control sobre los datos, dichos actores parecen inscribirse en una definición de la soberanía, desconectada de los Estados. Sin embargo, los Estados siguen siendo soberanos. Entonces, aparecen varias fuentes de coerción, que hay que ordenar. En primer lugar, la imposición de la coerción entre actores soberanos obstaculiza tanto el ejercicio independiente de la soberanía, como una represión eficaz de la trata. Como segunda opción, la colaboración entre actores soberanos surge como estrategia para proteger mutuamente la soberanía y encaminarse hacia una represión integral de la cibertrata. Sin embargo, por la aplicación de una perspectiva legalista centrada en la responsabilidad social corporativa, la colaboración tiene todavía un impacto limitado sobre las víctimas de trata. Ampliar el papel de los actores digitales exige superar una perspectiva securitaria e implementar los derechos humanos a través de asequibilidades pragmáticas. Fuera del ámbito del derecho penal, los actores digitales pueden tener obligaciones que contribuyan a ayudar a las víctimas mediante el control de sus datos. En este caso, el Estado aparece como intermediario en la aplicación de los derechos humanos, mientras que los actores digitales son los verdaderos ejecutores. Este escenario de colaboración reconoce un poder coercitivo diferente mientras protege los principios del Estado de Derecho. Además, este escenario cuestiona la base de la teoría de la soberanía.

La teoría de la soberanía se fundamenta en la independencia de los Estados. Sin embargo, este criterio obstaculiza una respuesta global a la trata, así como los

poderes de coerción de los actores soberanos. La independencia sigue siendo necesaria para delimitar negativamente la soberanía al establecer sus límites. No obstante, la independencia por sí sola no es suficiente para aplicar y legitimar las normas, en particular los derechos humanos y la lucha contra la trata. Entonces, un nuevo criterio podría fundamentar la legitimidad de los actores soberanos: la interdependencia. Este concepto podría elaborarse mediante una teoría general, fundada en valores fundamentales compartidos, y una aplicación concreta, por ejemplo, estableciendo procesos de conexión entre los distintos actores de la sociedad. Este planteamiento de la soberanía como interdependencia conduce a tres conclusiones.

La represión de la cibertrata requiere abarcar muchos ámbitos jurídicos. Eso cuestiona la estrategia de adoptar una ley integral[39]. Dicha estrategia reconoce la necesaria interdisciplinariedad de la lucha contra la trata, especialmente, yendo más allá del derecho penal. Dicha ley permitiría agrupar todos los derechos de las víctimas bajo un mismo marco, para obtener una imagen más clara de su protección jurídica, en lugar de derechos dispersos entre varias normas. Sin embargo, este estudio pone de relieve que la asistencia a las víctimas de la trata no debe limitarse a su condición de víctima en un proceso penal. En particular, la represión de la cibertrata subraya la importancia de reforzar la protección de sus datos personales y el control sobre su entorno digital. Entonces, podría parecer superficial limitar el marco de lucha contra la trata a una ley integral. Además, la mayoría de los retos que plantea la represión de la trata no son exclusivos de este delito: una mejora del marco jurídico sólo para reprimir la trata no está adaptada a la represión global de la delincuencia. Asimismo, este estudio cuestiona la necesidad de centrar las medidas preventivas en la existencia de este fenómeno. El delito se creó para facilitar la cooperación entre los Estados y controlar la migración: originalmente, las medidas preventivas quedaron muy limitadas, en particular a los controles fronterizos. Más allá de este enfoque restrictivo, el fenómeno pone de manifiesto las vulnerabilidades estructurales de la sociedad. Si bien la definición de la trata es necesaria para su represión, esta perspectiva penal parece insuficiente para una prevención global del fenómeno. El refuerzo de las capacidades individuales y colectivas y la adopción de medidas preventivas contra las desigualdades estructurales y las violaciones de los derechos fundamentales podrían contribuir a prevenir la trata. La alfabetización digital, la educación sexual y afectiva, la cultura del respeto y el consentimiento y el desarrollo de oportunidades vitales podrían contribuir a la prevención de la trata. Esto llega a cuestionar tanto el papel de los derechos humanos y el derecho, como su relación con la alfabetización jurídica y otros tipos de normas y acciones.

La multiplicación de entidades soberanas cuestiona su colaboración para la represión de la trata, pero también, en general, para la regulación y aplicación de los derechos humanos. Conduce hoy en día a «*la ausencia de una autoridad claramente asignable como deudora de estos derechos*»[40]. Sin embargo, en el marco del ciberespacio, parece que se está produciendo un cambio de perspectiva. Los actores digitales suelen ser calificados como intermediarios, porque permiten conexiones entre personas. El reconocimiento de actores soberanos interdependientes resulta en una nueva interpretación de la intermediación. Por un lado, los actores digitales

[39] Por ejemplo, en España, P. Lloria García, «El delito de trata de seres humanos y la necesidad de creación de una ley integral», *Estudios Penales y Criminológicos*, 22 de junio de 2019, vol. 39, p. 353; C. Villacampa Estiarte, «¿Es necesaria una ley integral contra la trata de seres humanos?», *Revista General de Derecho Penal*, Iustel, 2020, n.º 33, p. 16

[40] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.* nota 14, p. 494

aparecen como intermediarios en la aplicación de los derechos fundamentales, protegidos originalmente por los Estados y a favor de las personas, en particular en tanto usuarias y usuarios. Por otro lado, los Estados son intermediarios de los actores digitales frente a dichas personas al prestarles orientación y herramientas para legitimar sus acciones. Sin embargo, debido en parte a una concepción tradicional de la soberanía y a un enfoque principalmente capitalista y neoliberal del sector empresarial, esta interconexión carece de una teoría general. Por ahora sólo se adopta caso por caso, especialmente para la regulación del entorno digital. No obstante, una protección integral de los derechos humanos exige ir más allá de las disposiciones abstractas y requiere desarrollar medidas concretas para emprender su mejora. Dado que el proceso democrático tradicional no se aplica a los actores digitales e incluso tal vez no les sea aplicable, esta teoría general y sus procesos de aplicación tendrían que buscar nuevas bases de legitimidad. Dicho proceso permitiría, en primer lugar, un debate sobre los valores, tanto como orientación general como para su aplicación individual y colectiva. Por ahora, los derechos fundamentales «*expresa[n] un sistema de creencias propiamente occidental*», complementado por otras estructuras de opresión[41]. Esta necesaria retroalimentación constante de lo universal a las aplicaciones casuísticas pone de relieve que «*la idea de derecho no puede pretender la universalidad*» para gozar de plena legitimidad[42]. Para definir estos valores, podrían construirse, y ya se están construyendo, nuevos puentes entre los actores, con la esperanza de mejorar la comunicación y el entendimiento común.

Mientras que los derechos humanos establecen un marco general que carece de orientaciones para su aplicación cotidiana, se supone que el concepto de derecho alcanza la generalidad. Sin embargo, este estudio sobre las herramientas jurídicas para reprimir la cibertrata ha puesto de manifiesto una degradación de la calidad del derecho como herramienta general. Es cada vez más técnico y sectorial. Los regímenes no se modifican de forma exhaustiva, lo que provoca problemas de interpretación, falta de garantías y, tal vez, una disminución de la fuerza legítima del derecho estatal. Como teorizó Emeric bajo la noción de «*derecho fluido*», aquí el derecho «*es ante todo el producto de un discurso político, un ideal de reformadores, una presentación mercadotécnica de la ley*»[43]. El derecho, en concreto el derecho penal, se considera como una herramienta para resolver problemas sociales. El Derecho se magnifica como la solución, especialmente frente a los retos derivados de las nuevas tecnologías. Sin embargo, este solucionismo jurídico, llevado a su extremo, olvida otros sistemas y espacios de regulación de conductas, como la educación o la estructuración del ciberespacio. Como subraya la siguiente pregunta: «*¿estamos confundiendo una herramienta técnica con la cultura que la utiliza para hacer daño*»[44]? Si otras fuentes de normas y políticas, incluidas las privadas, tienen un impacto y una coerción potencial sobre las personas, los académicos del derecho podrían ampliar su perspectiva más allá del derecho estatal. Si el derecho es una herramienta destinada a promover valores, ordenar la sociedad y resolver retos sociales, su estudio exhaustivo quizá no deba obviar el reconocimiento de la realidad de su

[41] A. Supiot, *Homo juridicus essai sur la fonction anthropologique du droit*, Éditions du Seuil, 2005, p. 283

[42] *Ibid.* p. 284

[43] N. Emeric, «Droit souple + droit fluide = droit liquide. Réflexion sur les mutations de la normativité juridique à l'ère des flux», *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, n.º 2, p. 33

[44] K. Maltzahn, *Digital dangers Information & communication technologies and trafficking in women*, APC-200608-WNSP-I-EN-P-0024, Association for progressive communications, Issue Papers, agosto de 2006, p. 2

aplicación, el impacto de las estructuras sociales y económicas preexistentes y una necesaria flexibilidad para acompasarse al ritmo de la sociedad.

INTRODUCTION

> "*It has been almost 400 years since the notorious pirate […] Moerad Raïs scavenged the coasts of Northern and Western Europe looking for European Christian slaves who he could sell off in Algiers. […] In order to avoid detection, Raïs cleverly applied different techniques [such] as sailing under different flags. […* Just*] like him, modern-day traffickers still take advantage of the different vulnerabilities of victims and profit from them while abusing countries' legal and social systems*."[1]

> "*"No one doubts the essential role of corporations in today's economy and politics. But that doesn't mean that nations have no role...*
> *"According to my grandfather, that's exactly what it means," Martin went on, getting angry. "He says they stay in business because it's in the corporations' interest that people continue to believe in them, but they don't really make decisions* anymore.""[2]

1. Theorizing sovereignty through cyber human trafficking. Not far removed from a fictional world in which major corporations control science, build cities, and monitor people with brain implants, the relationships between states and corporations have been nourishing the political and legal literature. In particular, globalization and digitalization have led to the drawing of new boundaries regarding who can coerce, control, and influence people; who possesses the power to set establish and apply norms; et cetera. Legally speaking, the sovereignty of states is questioned, generally understood as "*assum[ing] the exclusive right to exercise political, legal, and judicial authority within a given geographical area*."[3] The "programmed obsolescence of sovereignty" has been a traditional research theme since the 1950s.[4] However, it remains true that "*states [are still] the principal actors on the international stage […*

---

[1] J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1690
[2] A. Alonso, J. Pelegrín, *La torre y la isla*, Anaya, La llave del tiempo no. 1, 2006
[3] J.-P. Vergne, R. Durand, "Cyberespace et organisations « virtuelles » : l'Etat souverain a-t-il encore un avenir ?," *Regards croisés sur l'économie*, La Découverte, 2014, vol. 2014/1, no. 14, p. 130
[4] J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018, p. 17. Although other voices argue that the growing interdependency of states dates back to antiquity, J. Chevallier, C. Jacques, *L'État post-moderne*, LGDJ, 4th ed., 2017, p. 31.

and] by far the most significant political actors within their own territories."[5] Nevertheless, this long-lasting literature on the potential end of (state) sovereignty seems to highlight one factor: This myth "*tends very often to freeze [a] constructed reality in a model that does not have any more concern for reality*."[6] Accordingly, this research aims to approach sovereignty on the basis of a human trafficking, a real phenomenon that has similarly evolved due to globalization and digitalization. The study of the rise of a global and comprehensive strategy to repress this offense highlights where powers of coercion appear and what types of relationships are built between the two main actors at the frontlines of its prevention and prosecution, as well as the protection of its victims. The fight against cyber human trafficking, an offense violating many, if not all, human rights, might be a daily struggle for victims, legal practitioners, and social workers. However, it also grounds the theory of sovereignty in a reality that allows one to question its conceptual basis.

2. Fighting human trafficking facilitated by new technologies: from old to recent calls. Perpetrators of offenses take advantage of available technologies[7] to ensure that they will go unpunished. For instance, the Internet—or, broadly speaking, cyberspace—like any new tool, is a double-edged sword[8] that can be used to support human rights but also to commit offenses. Warnings about the use of new technologies by traffickers have multiplied from the birth of the Internet to the recent supranational crisis. Human trafficking could be broadly defined as a criminal process including all steps from recruitment to the exploitation of victims under conditions denying a possible full consent of the victim. Since 1996, the European Commission has stated that judicial cooperation to repress trafficking should "*consider measures to avoid the abuse of the Internet*."[9] In 2005, the Committee of Ministers of the Council of Europe recognized that "*the use of [information and communication technologies] has*

[5] Q. Skinner, "The sovereign state: a genealogy," *in* H. Kalmo, Q. Skinner (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 44
[6] L. Bal, *Le mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Thesis, Université de Strasbourg, February 3, 2012, p. 18
[7] Technologies include what is broadly called "new technologies," meaning all tools developed with the digital revolution: in the first place, the Internet, but also the development and popularization of mobile phones, computers, etc. See *infra* 27.
[8] M. Chawki, M. Wahab, *Technology Is a Double-Edged Sword: Illegal Human Trafficking in the Information Age*, DROIT-TIC.fr, 2004
[9] European Commission, "Communication to the Council and the European Parliament on trafficking in women for the purpose of sexual exploitation," EU, November 20, 1996, p. 38. See also European Commission, "Communication to the Council and the European Parliament - For further actions in the fight against trafficking in women," EU, December 9, 1998, p. 9

expanded the possibilities for trafficking in human beings and has created a new virtual form of this practice."[10] Today, all major supranational organizations consider cyber trafficking to be a priority,[11] and these calls have multiplied as a result of two recent crises: The use of new technologies in trafficking processes was highlighted during the COVID-19 pandemic[12] as well as following the start of the war between Russia and

[10] Committee of Ministers, "Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society," Council of Europe, May 13, 2005, ¶ 4, CM(2005)56 final

[11] Within the United Nations, see Commission on Crime Prevention and Criminal Justice, "Resolution 27/2 Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies," Economic and Social Council, UN, 2018; the topic is underlined by the reports of the United Nations Office on Drugs and Crime (UNODC), UNODC, *Global report on trafficking in persons 2022*, UN, January 2023, pp. 90-92. The 2022 World Day Against Trafficking in Persons focused "*on the role of technology as a tool that can both enable and impede human trafficking*," United Nations, "World Day Against Trafficking in Persons," *United Nations*, United Nations, no date, online https://www.un.org/en/observances/end-human-trafficking-day (retrieved on August 23, 2022). The Organization for Security and Co-operation in Europe (OSCE) highlights that law enforcement authorities should disrupt "*all forms of trafficking in human beings facilitated by [information and communication technologies], in particular by the Internet*," OSCE, "Decision nº 1107 Addendum to the OSCE Action plan to combat trafficking in human beings: one decade later," December 6, 2013, ¶ III.1.4, PC.DEC/1107/Corr.1. Also in 2019, the OSCE organized the 19th Alliance against Trafficking in Persons conference, which focused on how technology can be turned from a liability into an asset in combating trafficking. The Group of Experts on Action against Trafficking in Human Beings (GRETA) of the Council of Europe has developed various activities on that topic since 2018, see, for instance, GRETA, "8th general report on GRETA's activities covering the period from 1 January to 31 December 2018," Council of Europe, 2019, p. 20; GRETA, "9th general report on GRETA's activities covering the period from 1 January to 31 December 2019," Council of Europe, 2020, ¶¶ 7, 8, 43. The questionnaire for the next round of evaluation of the GRETA focuses in particular on the use of new technologies by authors of trafficking and by anti-trafficking actors, GRETA, "Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties. Fourth evaluation round. Thematic focus: Addressing vulnerabilities to trafficking in human beings," Council of Europe, June 30, 2023, GRETA(2023)11. Finally, within the European Union (EU), the impact of new technologies on trafficking has been taken into account since the first report on the progress made in this fight, up until the last report, European Commission, "Report on the progress made in the fight against trafficking in human beings as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims," EU, May 19, 2016, p. 11, COM(2016) 267 final; European Commission, "Fourth report on the progress made in the fight against trafficking in human beings," EU, December 19, 2022, COM(2022) 736 final. The EU Strategy on Combatting Trafficking in Human Beings 2021-2025 includes "*tackling the digital business model of traffickers*," European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," EU, April 14, 2021, pp. 11-12, COM(2021) 171 final

[12] UNODC, *The effects of the COVID-19 pandemic on trafficking in persons and responses to the challenges - A global study of emerging evidence*, UN, 2021; E. Such et al., "The Risks and Harms Associated with Modern Slavery during the COVID-19 Pandemic in the United Kingdom: A Multi-Method Study," *Journal of Human Trafficking*, Routledge, April 8, 2023, vol. 0, no. 0, pp. 1-21. The other side of the coin, meaning the use of new technologies to prevent risks, in particular exploitation, during crisis periods, has been highlighted as part of the conclusions of M. Alemany Jordán, *La violencia contra las mujeres en los desastres, pandemias y otras emergencias humanitarias*, Tirant lo Blanch, Derechos humanos, 1st ed., 2022, pp. 338-339

Ukraine.[13]

3. Theorizing and researching cyber human trafficking. The interest in the use of technologies by perpetrators of trafficking led to the coining of two terms for this phenomenon: cyber trafficking[14] or e-trafficking. It is broadly defined as "*human trafficking facilitated or enabled or regulated through the use of the Internet and other communication platforms*."[15] However, technologies are not limited to cyberspace but include every technology that could facilitate the trafficking process. Responding to interest in this phenomenon, supranational organizations have funded research on this topic.[16] Nevertheless, the breadth of cyber trafficking has been criticized in studies of this subject.[17] Research commissioned by supranational organizations "*ha[s] short*

[13] Europol, "Human traffickers luring Ukrainian refugees on the web targeted in EU-wide hackathon," *Europol*, June 23, 2022, online https://www.europol.europa.eu/media-press/newsroom/news/human-traffickers-luring-ukrainian-refugees-web-targeted-in-eu-wide-hackathon (retrieved on July 11, 2022); EU Anti-trafficking Coordinator, "Common Anti-Trafficking Plan to address the risks of trafficking in human beings and support potential victims among those fleeing the war in Ukraine," EU, 2022, p. 7; D. Czarnecki, *Trafficking in human beings 2.0 - Digitalisation of trafficking in human beings in Germany - Developments and Courses of Action*, KOK, German NGO Network against Trafficking in Human Beings, 2023, p. 21

[14] V. Greiman, C. Bain, "The Emergence of Cyber Activity as a Gateway to Human Trafficking," *International Journal of Cyber Warfare and Terrorism*, 2012, vol. 12, no. 2, p. 29; A. Sykiotou, "Cyber trafficking: recruiting victims of human trafficking through the net," *in* N.E. Kourakēs, C.D. Spinellis (eds.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017, p. 1549

[15] S. Milivojević, "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, pp. 28-44

[16] D. Hughes, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation A Study of the Users*, Committee for Equality between Women and Men, Council of Europe, May 2001; D. Hughes, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation. Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation*, Committee for Equality between Women and Men, Council of Europe, November 2001; Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, "Final Report," Committee for Equality between Women and Men, Council of Europe, September 16, 2003, EG-S-NT (2002) 9 rev.; A. Sykiotou, *Trafficking in human beings: Internet recruitment - Misuse of the Internet for the recruitment of victims of trafficking in human beings*, Council of Europe, 2007; Anti Slavery, ITUC CSI IGB, CCME, "The role of the Internet in trafficking for labour exploitation," EU Prevention of and Fight against Crime Program, International Trade Union Confederation, 2011; Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020; GRETA, "Online and technology-facilitated trafficking in human beings. Summary and recommendations," Council of Europe, March 2022. At the national level, see, for instance, D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13

[17] J. Mendel, K. Sharapov, "Human Trafficking and Online Networks: Policy, Analysis, and Ignorance: Human Trafficking and Online Networks," *Antipode*, June 2016, vol. 48, no. 3, p. 671; A. Lavorgna, *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*, Thesis, University of Trento, December 2013, p. 115; J. Scoular et al., "Beyond the Gaze

time lines and require[s] policy-relevant findings and conclusions," thereby limiting its quality.[18] Indeed, some research has relied on unsystematic evidence,[19] most of it focusing only on trafficking for sexual exploitation, which is usually conflated with sex work,[20] then hiding some changing realities of forced labor. Moreover, the use of new technologies requires their material availability and a certain level of digital literacy that some traffickers or victims might lack.[21] In general, the breadth of cyber trafficking must be put into perspective: Recruitment and migration still rely strongly on interpersonal relations and word of mouth, money laundering and payments still rely mostly on cash, et cetera.

4. Despite the shortcomings of research on cyber human trafficking, this phenomenon exists and constitutes the case study to which the theory of sovereignty is applied. Thus, the legal frameworks defining trafficking and its criminological evolution are explained (Section 1), and, this phenomenon is framed by the theory of sovereignty (Section 2). As a preliminary section, it is necessary to develop the methodology applied in this research (Section 0).

Section 1. Framing the study: methodological clarifications

5. Methodology. This research is based on various methodological choices, which are listed and explained in the following paragraphs. They detail the reasons for a comparative law approach that is developed in various parts of this study, and they clarify the understanding of the law and the extension of the norms that are studied. All of these methodological choices are connected to a pragmatic approach to the legal field, strongly supported by an interdisciplinary approach.

6. "Comparative law is the oldest profession in the (legal) world."[22] First, this

---

and Well Beyond Wolfenden: The Practices and Rationalities of Regulating and Policing Sex Work in the Digital Age," *Journal of Law and Society*, June 2019, vol. 46, no. 2, p. 212; R. Konrad, A. Trapp, T. Palmbach, "Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications," *European Journal of Operational Research*, June 1, 2017, vol. 259, no. 2, p. 2

[18] L. Kelly, "'You Can Find Anything You Want': A Critical Reflection on Research on Trafficking in Persons within and into Europe," *International Migration*, 2005, vol. 43, no. 1/2, p. 236

[19] S. Milivojević, "The State, Virtual Borders and E-Trafficking: Between Fact and Fiction," *in* S. Pickering, J. McCulloch (eds.), *Borders and crime Pre-crime, mobility and serious harm in an age of globalization*, Palgrave Macmillan, 2012, p. 80

[20] S. Milivojević, H. Moore, M. Segrave, "Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 26. On this division, see *infra* Part 2. Title 1. Chapter 2. Section 1. .

[21] UNODC, *Global report on trafficking in persons 2020*, UN, January 2021, p. 127

[22] S. Goltzberg, *Le droit comparé*, Presses Universitaires de France, Que sais-je ?, 2018, p. 35

study makes use of comparison as a methodological tool. Sovereignty has both a national and an international theory; similarly, human trafficking has both supranational and national definitions. A study of the national drafting and implementation of the law is necessary to adopt a pragmatic perspective on sovereignty; comparative law supports a link between concrete application and abstract theorization.[23] Thus, comparative law is not at the core of this study; rather, it is a methodological approach required to understand various global legal reactions to fight against human trafficking and to regulate new technologies. Furthermore, a study of various countries allows one to understand how national sovereignties and legal orders interact, including by influencing each other as well as highlighting differences, commonalities,[24] shortcomings, and useful practices.[25] The repression of cyber human trafficking is a common object of study to frame a useful comparison.[26] In particular, comparative law seems to be a methodological requirement to study law framed by globalization.[27] Indeed, "*Comparative law acts as a filter and backbone of the international community's complicated normative system*"[28] by selecting specific legal orders and

[23] O. Pfersmann, "Le droit comparé comme interprétation et comme théorie du droit," *Revue internationale de droit comparé*, 2001, vol. 53, no. 2, p. 283

[24] M. Durán Bernardino, "El método comparado en los trabajos de investigación," *in* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 49. In this sense, comparative law highlights "*common denominator[s] likely to inspire an extension of common protection*," Conseil d'État (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 1, p. 16, Keynote Address by Jean-Marc Sauvé

[25] In particular, "*comparative law makes it possible both to reveal the divergence of rights and to examine whether integration is an appropriate response to the dysfunctions that one seeks to address*," V. Robert, L. Usunier, "Conclusion. Du bon usage du droit comparé," *in* M. Delmas-Marty, Université de Paris I: Panthéon-Sorbonne (eds.), *Critique de l'intégration normative: l'apport du droit comparé à l'harmonisation des droits*, Presses Universitaires de France, Les voies du droit, 1st ed., 2004, p. 231. In particular, comparative criminal law becomes "*the means of finding common solutions to common problems in the spirit of a theoretical and practical collaboration on the international level for the purpose of a better organization of the defense of the society against crime. In short, it becomes the basis of a criminal science of universal scope*," Max-Planck-Institut für Ausländisches und Internationales Strafrecht Internationales Kolloquium Freiburg im Breisgau), *Die Vergleichung als Methode der Strafrechtswissenschaft und der Kriminologie = La comparaison en tant que méthode scientifique en droit pénal et en criminologie = Comparison as a method of criminal law and criminology*, Duncker & Humblot, Strafrecht und Kriminologie ; Bd 6, 1980, pp. 99-100

[26] M.-L. Izorche, "Propositions méthodologiques pour la comparaison," *Revue internationale de droit comparé*, 2001, vol. 53, no. 2, p. 293; J.A. Fernández Avilés, "El método comparado en el Derecho del trabajo, relaciones laborales y Seguridad Social ('Pertinencia y Prudencia' en su uso)," *in* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 291

[27] E. Filiberti, "Le droit comparé tient une place grandissante dans notre société," *Petites affiches*, March 14, 2006, no. 52, p. 3

[28] O. Olariu, "El papel del Derecho comparado en la enseñanza del Derecho Internacional Público: el ejemplo de la asignatura Derecho Internacional de los Derechos Humanos," *in* N. Marchal Escalona, M.C. Muñoz González, S. Muñoz González (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 278

studying their particular application of certain global standards, herein the fight against cyber trafficking.

7. Selection of national frameworks. Thus, this research rests primarily on the study of four national legal orders. Both systems of common law and civil law and the legal orders of Western and Eastern Europe are included. France and Spain are at the core of this study, as they are Western European systems that are based on civil law. The selection of two similar systems highlights the differences remaining in legal frameworks despite their geographic proximity. Additionally, a research stay in Romania complements this study with the perspective of an Eastern European country. The three countries have harmonized their basic legislation as a result of their common membership in the European Union (EU). However, some differences remain in legal and institutional elements, such as the definition of trafficking and the institutional development of its repression, and the profiles of the victims are significantly different: Romania is an origin country for trafficking, and Spain and France are destination and transit countries. In particular, the first member state citizenship of EU trafficked victims is Romanian,[29] and, the fight against trafficking is a political priority that is more firmly established.[30] However, as the research stay lasted only three months, the study of the Romanian framework is primarily developed in the first part of this thesis. It should be highlighted that these three European countries are accustomed to cooperating in large anti-trafficking investigations, justifying their concomitant selection.[31] Finally, the

[29] For 2017-2018, see European Commission, *Data collection on trafficking in human beings in the EU*, Publications Office of the EU, 2020, p. 25. Similarly, for 2015-2016, see European Commission, *Data collection on trafficking in human beings in the EU*, EU, 2018, pp. 13, 43

[30] Romania launched its third national anti-trafficking strategy in 2018, which is subdivided into biannual action plans, Guvernul, "Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022," Romania, October 31, 2018. By comparison, France, after almost three years of waiting since the first action plan on anti-trafficking, released the second plan in late 2019, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, "2nd plan d'action national contre la traite des êtres humains 2019-2021," France, 2019. The third action plan has still not been released. The same delay of three years occurred in Spain, between the end of the first plan in 2018 and the beginning of the new comprehensive plan in 2021, Ministerio de Sanidad, Servicios Sociales e Igualdad, "Plan integral de lucha contra la trata de mujeres y niñas con fines de explotación sexual 2015-2018," Spain, 2014; Centro de inteligencia contra el terrorismo y el crimen organizado, "Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023," Secretaría de Estado de seguridad, Ministerio del Interior, Spain, January 2022

[31] Office to monitor and combat trafficking in persons, "Trafficking in Persons Report: France," *US Department of State*, 2023, online https://www.state.gov/reports/2023-trafficking-in-persons-report/france/ (retrieved on July 6, 2023); O. Le Creurer, "Prostitution : un réseau international démantelé depuis Montpellier," *France 3 Occitanie*, March 4, 2021, online https://france3-regions.francetvinfo.fr/occitanie/herault/montpellier/prostitution-un-reseau-international-demantele-depuis-montpellier-1982317.html (retrieved on March 9, 2021)

United States has had a strong influence on the negotiations over the international definition of trafficking. US importance in the global repression of trafficking is still noticeable, in particular through its annual evaluation of countries' policies on this topic.[32] Furthermore, it should be highlighted that many studies on cyber human trafficking originated in the United States, and this US leadership particularly affects the second part of this thesis. For this reason, this research includes the study of the US framework as a common law country, and, this manuscript is written and harmonized in American English (including quotes).

8. The extension of state law. Second, this study rests on a specific understanding of state law. Indeed, although criminal law might be the acme of sovereignty and human trafficking usually might be studied from a criminal perspective, this study cannot be limited to criminal law. The theory of sovereignty and the repression of trafficking require various legal disciplines for a comprehensive study.[33] As such, this thesis relies on an interdisciplinary methodology through an "*articulation of knowledge between disciplines that develop issues that partially overlap*."[34] Indeed, the fight against human trafficking in the context of its evolution due to new technologies pulls together both the various legal disciplines used to approach trafficking and the legal disciplines used to regulate new technologies. The first category extends not only to criminal law in its substantive understanding but also to criminal procedure, and it expands to the protection of victims outside criminal law on the basis of the state's social law or legal fields dedicated to relations with foreign citizens. The second category could be termed digital law, but it similarly groups various traditional legal disciplines—such as contract law, intellectual property, and competition law—into the

[32] See, for instance, Department of State, "Trafficking in persons report," US, June 2023. See also, *infra* 415.

[33] B. Lavaud-Legendre, *Approche globale et traite des êtres humains - De l'« injonction à la coopération » au travail ensemble*, CNRS, July 1, 2018, online https://halshs.archives-ouvertes.fr/halshs-02177213 (retrieved on October 29, 2021)

[34] This study is thus neither a pluridisciplinary study, based on "*the juxtaposition of specific points of view on an object of study*," nor a transdisciplinary study, based on "*an abandonment of the particular points of view of each discipline to produce an autonomous knowledge from which new objects and new methods result*," V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, Dalloz, Méthodes du droit, 2e édition, 2016, pp. 346-348. However, scholars highlight the need for transdisciplinary research on human trafficking, see L. Martin et al., "Learning each other's language and building trust: Community-engaged transdisciplinary team building for research on human trafficking operations and disruption," *International Journal of Qualitative Methods*, April 30, 2022, vol. 21, pp. 1-15; T.C. Sharkey et al., "Better together: A transdisciplinary approach to disrupt human trafficking," *ISE Magazine*, 34-39, November 2021

protection of fundamental rights online.[35] In general, "*Digital law is still something of a puzzle*,"[36] which thus requires an interdisciplinary approach. Furthermore, in this research, the legal discipline is highly connected to the political one, as many of the laws studied have been or are in the process of being amended or adopted. Additionally, the repression of human trafficking and the regulation of new technologies rely on legal texts as well as on political texts, such as national strategies. Thus, "*Between law and politics, the determination is reciprocal, and the mutual implication is constant*."[37] In particular, recent criminal law is particularly nourished by an "*ideological function that consists of producing and spreading an illusory representation and the dramatic discrepancies between appearances and realities. […Thus,] criminal law must be understood as a part of the social politics of the state*."[38] Similarly, the study of legal texts cannot be separated from their implementation: The repression of human trafficking seeks to erase a criminal, yet mainly social, phenomenon, and the study of law applied to new technologies requires practical considerations. As underlined by Ancel, the study of criminal law and policies should be complemented by "*the reactions of public opinion and the resistance […] either by the judges or by the practice or by the administrative services*."[39] Therefore, this study relies on a pragmatic approach to state law and not merely a study of positive law. It includes not only their application, understood as their interpretation by judicial entities, but also the use of law by the different actors in society.

9. The extension of the law. Third, this study does not rely on an understanding of law as limited to state law. The regulation of new technologies requires considering private norms, either drafted as unilateral (statements from digital actors) or

[35] See, for instance, Y. Laurier Ngombé, *Fiches de droit du numérique: rappels de cours et exercices corrigés*, Ellipses, Fiches de, 2022; E.M. Valpuesta Gastaminza, J.C. Hernández Peña (eds.), *Tratado de Derecho Digital*, Wolters Kluwer Legal & Regulatory España, 2021

[36] J. Brigham, A.T.M. Schreiner, "The Semiotics of Digital Law Introduction," *International Journal for the Semiotics of Law*, 2004, vol. 17, no. 3, p. 260

[37] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016, p. 376. Forray and Pimont further criticize this divide between law and politics as leading them to see legal scholars as acting "*in the field of knowledge and not of power*." However, "*the most typical activity of legal knowledge–the description of law–is politically significant*." Consequently, legal scholars should bear a kind of political responsibility in their work, V. Forray, S. Pimont, *Décrire le droit... et le transformer: essai sur la décriture du droit*, Dalloz, 2017, ¶ 408

[38] Max-Planck-Institut für Ausländisches und Internationales Strafrecht Internationales Kolloquium Freiburg im Breisgau), *Comparison as a method of criminal law and criminology*, *op. cit.* note 25, p. 39

[39] M. Ancel, "Le droit pénal comparé en tant que moyen de recherche dans le domaine de la politique criminelle," *in* Max-Planck-Institut für Ausländisches und Internationales Strafrecht Internationales Kolloquium Freiburg im Breisgau) (ed.), *Comparison as a method of criminal law and criminology*, Duncker & Humblot, Strafrecht und Kriminologie ; Bd 6, 1980, p. 81

supposedly bilateral (terms of service) norms, or rules embedded within technologies. The regulation of human trafficking requires attention to supranational norms as well as to local ones due to infra-state competencies. Thus, this research is framed by the hypothesis of legal pluralism: "*The law is not alone; it coexists with other systems of norms*."[40] In postmodern society, it "*seems illusory to think that all legal norms form a system or are ordered in a hierarchical manner that is entirely subordinated to a single superior point*."[41] In the end, "*The identification of law and state is now outdated in the context of networked law and globalization*."[42] In particular, "*Theorizing the regulatory complexities posed by the issue of trafficking resituates it as part and parcel of the processes of globalization more generally rather than as an exception or impediment to what globalization seeks to achieve. Trafficking as a regulatory issue is in need of precisely this form of de-centering*."[43]

10. The extension outside the law. Fourth, this study, while primarily framed in the legal field, also relies on other disciplines. A full understanding of the complex phenomenon of trafficking requires an integration of sociological, medical, anthropological, and economic studies. The regulation of new technologies cannot be grasped without a basic understanding of some notions of informatics. Furthermore, some of the norms studied are quite recent or are in negotiation[44], and they lack academic research regarding their application. Consequently, journalistic references are also used at the margins. These choices are justified since, by default, legal research is limited because "*the image of the social it creates and analyzes is rather the projection, or the shadow, of its own categories, and, in particular, of the way it has configured its privileged object, the law*."[45] However, "*Law is a 'secondary' instrument, which is necessarily grafted onto more original relationships, family, religious, commercial, and political*."[46] Thus, "*Legal formalism consists of considering only positive law and apprehending reality only through the form it takes. The criticism of*

[40] J. Carbonnier, *Flexible droit: pour une sociologie du droit sans rigueur*, Librairie Générale de Droit et de Jurisprudence, 7th ed., 1992, p. 25
[41] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, *op. cit.* note 34, pp. 186-187
[42] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.* note 37, p. 25
[43] P. Kotiswaran, *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, p. 7
[44] This thesis has been updated until July 7, 2023.
[45] A. Bailleux, F. Ost, "Droit, contexte et interdisciplinarité : refondation d'une démarche," *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2013, vol. 70, no. 1, p. 39
[46] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, *op. cit.* note 37, p. 6. Understanding law as a primary instrument leads to a legal "*essentialism*," *Ibid.* p. 35

this expression of formalism consists of widening the conception of sources of law re-valorizing the extralegal factors of production of law, namely, factors of a historical, sociological, economic, or psychological nature."[47] Here, in particular, other disciplines are necessary to set a "*factual context*"[48] and to expand the "*theoretical context*" by relying on their concepts.[49]

11. Methodology: connection. To summarize, this methodology "*can be briefly described as the association of heterogeneous references. It means to organize a dialogue with non-legal texts. [...] Such a method authorizes the use of shifts and reconciliations instead of resorting exclusively to the operations of legal logic. [... This] 'bricolage' [handiwork] makes possible a return to the law at the same time, as it frees us from the constraints of methods exercised by legal science. It frees the path towards unnoticed legal phenomena*."[50] Additionally, this handiwork allows the resistance of "*the attraction that the already constituted, bordered, structured fields of knowledge exert on [scholars. …] It proposes a progression of knowledge based on a principle of resistance*."[51] Multiple references have been gathered for this work. At first, the repression of human trafficking and the regulation of new technologies barely connect in the legal field,[52] but their interconnection is required to comprehensively fight against cyber human trafficking. This interconnection offers a new perspective on the application of the theory of sovereignty. Thus, it connects with the methods applied by feminist analysis, in particular, practical reasoning: "*The feminist starting point is from actual human experience*."[53] The method is pragmatic and inductive, by asking particular questions, here, selecting a case study to question a legal theory.[54] Indeed, in general, "*Practical reasoning in the context of law necessarily works from rules. Rules represent accumulated past wisdom, which must be reconciled with the contingencies and practicalities presented by fresh facts. […] Then,] rules leave room*

---

[47] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, *op. cit.* note 34, p. 171
[48] L. Lalonde, "L'interdisciplinarité comme « contextes », quels usages de l'Autre ?," *in* Journée d'étude sur la méthodologie et l'épistémologie juridiques, G. Azzaria (eds.), *Les cadres théoriques et le droit: actes de la 2e Journée d'étude sur la méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2013, p. 394
[49] *Ibid.* p. 404
[50] V. Forray, S. Pimont, *Décrire le droit*, *op. cit.* note 37, ¶ 91
[51] *Ibid.* ¶ 99
[52] Similarly, a clear divide is usually made between practitioners investigating and prosecuting human trafficking and cybercrimes in a restrictive sense.
[53] G. Binion, "Human Rights: A Feminist Perspective," *Human Rights Quarterly*, Johns Hopkins University Press, 1995, vol. 17, no. 3, p. 513
[54] *Ibid.* p. 516

for the new insights and perspectives generated by new contexts."[55] More specifically, feminist methods and "*reasoning from context can change perceptions about the world, which may then further expand the contexts within which such reasoning seems appropriate, which, in turn, may lead to still further changes in perceptions*."[56]

12. Once the methodological framework has been explained, the first step of this research is to delve into the phenomenon at the basis of the study of the theory of sovereignty: the interlinks between new technologies and human trafficking.

Section 2. Intertwining human trafficking and new technologies

13. The need to repress human trafficking. As highlighted by US Congressman Smith in 2010, "*The Internet has opened a whole new front in the war with human trafficking*."[57] To assess the need to fight against trafficking, including its cyber evolution,[58] many studies rely on statistics.[59] Nevertheless, their methodologies, when they exist, have been highly criticized. In general, "*Among the numerous criticisms are the predominance of weak research designs, poor-quality data, insufficient methodological clarity, questionable assumptions, emotive or politicized rhetoric, ill-founded inferences, and conclusions not properly grounded in the findings*."[60] First, the definitions of the phenomenon and the counted categories "*are often contradictory, ill stated, or missing*."[61] Second, human trafficking creates, by nature, a hidden

[55] K.T. Bartlett, "Feminist Legal Methods [1990]," *in* K.T. Bartlett, R.T. Kennedy (eds.), *Feminist legal theory: readings in law and gender*, Westview Press, New perspectives on law, culture, and society, 1991, p. 378
[56] *Ibid.* p. 381
[57] S. Milivojević, "The State, Virtual Borders and E-Trafficking," *op. cit.* note 19, p. 72
[58] See, for instance, K. Feehs, A. Currier Wheeler, *2019 Federal Human Trafficking Report*, Human Trafficking Institute, 2020, pp. 25, 32: in the United States, almost 37% of defendants in human trafficking cases in 2019 were recruited online; Bundeskriminalamt, *Human trafficking and exploitation National Situation Report 2020*, Germany, 2020, p. 9: in Germany, around 16% of victims of trafficking for sexual exploitation were contacted *via* the Internet; Agenţia Naţională Împotriva Traficului de Persoane, "Raport anual privind fenomenul traficului de persoane in 2019," Romania, 2020, p. 14: in Romania, the Internet is the second most popular recruitment method.
[59] Various supranational reports try to set global trustworthy statistics around the topic, 8.7 Alliance, "Global Estimates of Modern Slavery - Forced labour and forced marriage," International Labour Organization, 2017; UNODC, *Global report on trafficking in persons 2022*, *op. cit.* note 11; European Commission, *Data collection on trafficking in human beings in the EU*, *op. cit.* note 29
[60] E. Cockbain, K. Bowers, L. Vernon, "Using Law Enforcement Data in Trafficking Research," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1710
[61] A.J. Gould, "From Pseudoscience to Protoscience: Estimating Human Trafficking and Modern Forms of Slavery," *Second Annual Interdisciplinary Conference on Human Trafficking*, University of Nebraska, 2010, p. 7. On the variation on the concept, see J. van Dijk et al., *Counting what counts: tools for the validation and utilization of EU statistics on human trafficking*, HOME/2011/ISEC/AG/THB/4000001960, INTERVICT/Universitat Autònoma de Barcelona, TrafStat project, January 1, 2014. In particular on labor

population, meaning "*a group of people for which, membership is either socially stigmatized or constitutes a crime. Due to its hidden nature, the creation of an accurate sampling frame […] is not possible*."[62] Thus, this study, as much as possible, does not rely on statistics, which nourish a "*governance by numbers*,"[63] based on "*guesstimate*" figures,[64] establishing policy priorities on flawed data instead of values.[65] Independently of its prevalence, human trafficking is a violation of human rights.

14. Consequently, it is globally accepted that human trafficking should be criminalized, and that new technologies can facilitate that goal. However, "*Definitions are not neutral; they come with their own assumptions, theoretical and/or empirical, and their own conceptual baggage*."[66] Consequently, human trafficking should be defined (§1) and the evolution of its *modus operandi* should be explained (§2).

---

trafficking, see S.X. Zhang, "Measuring labor trafficking: a research note," *Crime, Law and Social Change*, November 1, 2012, vol. 58, no. 4, pp. 469-482

[62] A.J. Gould, "From Pseudoscience to Protoscience: Estimating Human Trafficking and Modern Forms of Slavery," *op. cit.* note 61, p. 8. This challenge is increased due to the lack of self-identification of many victims, A. Farrell, I. de Vries, "Measuring the Nature and Prevalence of Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 150. Moreover, data from law enforcement authorities is particularly biased by their capacity to recognize trafficking and identify victims, E. Cockbain, K. Bowers, L. Vernon, "Using Law Enforcement Data in Trafficking Research," *op. cit.* note 60, p. 1714. This is particularly criticized in Spain, see M. Jandl, "Investigaciones sobre la trata de personas: lagunas y limitaciones de los datos en los ámbitos del delito y la justicia penal," *in* S. Chawla (ed.), *Foro sobre el delito y la sociedad. Número especial Reunión de datos sobre la delincuencia: indicadores y cuantificadores*, UNODC, UN, 2008, vol. 7, pp. 39-47; A. Villanueva Fernández, F. Fernández-Llebrez González, "La importancia de los datos de trata de seres humanos: una aproximación al sistema de recolección de datos de víctimas de trata en España," *Revista Deusto de derechos humanos*, Instituto de Derechos Humanos Pedro Arrupe, 2019, no. 4, pp. 115-143; M.J. Castaño Reyero et al., *Cultura de datos en la trata de seres humanos: informe técnico de investigación*, Universidad Pontificia Comillas, 1st edition, February 17, 2022, pp. 36-78

[63] A. Supiot, *La gouvernance par les nombres: cours au Collège de France (2012-2014)*, Fayard, 2020

[64] J. Goodey, "Data on Human Trafficking Challenges and Policy Context," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 40

[65] I. De Vries, C. Dettmeijer-Vermeulen, "Extremely wanted: human trafficking statistics—what to do with the hodgepodge of numbers?," *Forum on Crime and Society*, UNODC, 2015, vol. 8, p. 17; G. Peck, "Counting Modern Slaves: Historicizing the Emancipatory Work of Numbers," *in* D.W. Blight, G. LeBaron, J.R. Pliley (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, p. 36. It should nevertheless be recognized that data can be useful to "*raise awareness […], help governments and non-governmental organizations to develop facts-based policies against it, and, last but not least, monitor progress with their implementation*," J. Van Dijk, "Measuring Trafficking in Persons Better: Problems and Prospects," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1672

[66] J. Black, "Critical Reflection on Regulation," *Australian Journal of Legal Philosophy*, January 1, 2002, vol. 27, p. 27

§1. Defining human trafficking

15. Originally, supranational frameworks defined human trafficking (I), but neither national definitions are fully harmonized (II).

I. Supranational frameworks

16. The Palermo Protocol. The first and only widely ratified[67] supranational text that comprehensively defines human trafficking is the 2000 Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children (the Palermo Protocol). It divides the definition of human trafficking into three elements.[68] First, specific material acts of the process of trafficking should be proved, such as the recruitment or transportation of victims; second, those acts must be committed through specific means[69] that nullify any consent from the victim,[70] such as force, coercion, or deception; third, trafficking has a specific intent, the exploitation of the victim. Exploitation "*shall include, at a minimum, […] sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude, or the removal of organs*."[71] Thus, trafficking "*can be viewed as a process rather than a single offense*."[72] However, the Palermo Protocol has two main shortcomings. First, it supplements the 2000 Convention against Transnational Organized Crime, or the Palermo Convention. Therefore, human trafficking is internationally prohibited only when the process is transnational and is performed by an organized criminal group.[73] Second, the Palermo

[67] The Palermo Protocol has 181 parties, including non-state entities such as the EU. Prior international texts on trafficking for sexual exploitation were not as widely ratified. For a list of these texts and the historical origins of the repression of trafficking, see *infra* 80.

[68] C.J. Smith, K. Kangaspunta, "Defining Human Trafficking and Its Nuances in a Cultural Context," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 26

[69] These means are not required for child victims, Article 3.c of the Palermo Protocol. This study is mainly focused on adult victims of trafficking and excludes the specific regulations in favor of the protection of child victims. However, it should be highlighted that the repression of cyber human trafficking highly focuses on the protection of minors online.

[70] Consequently, consent is not an element of the offense, Article 3.b of the Palermo Protocol

[71] Article 3.a of the Palermo Protocol

[72] A. Aronowitz, *Human trafficking, human misery: the global trade in human beings*, Praeger Publishers Inc, 1st ed., 2009, p. 9

[73] Article 4 of the Palermo Protocol. An organized criminal group is here defined as "*a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*," Article 2.a of the Palermo Convention. On this concept, see *infra* 212. However, elements of trafficking can be committed nationally. For example, see a French trend of sexual exploitation that can be qualified as trafficking that is nicknamed "*urban pimping*" (proxénétisme de cité), targeting mainly French minor victims, B. Lavaud-Legendre, "Des qualifications applicables à la prostitution des mineurs organisée en Plans," *Actualité juridique*

Protocol leaves some concepts to be defined by states. For instance, "*abuse of power or of a position of vulnerability*" as a means of trafficking is not defined.

17. European frameworks. To complement the Palermo Protocol, European organizations adopted their own frameworks. First, the Council of Europe drafted the 2005 Convention on Action against Trafficking in Human Beings (Warsaw Convention), which transposes the definition of the Palermo Protocol[74] but erases the conditions of a transnational process and an organized group.[75] Furthermore, the text develops the rights of trafficked victims[76] and creates an evaluation mechanism, the Group of Experts on Action against Trafficking in Human Beings (GRETA).[77] Similarly, the EU, which was known then as, the European Community, adopted measures in 1996 to harmonize the repression of trafficking.[78] Today, the EU framework is divided into two texts. Specific rights for trafficked victims are established by Council Directive 2004/81/EC on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration, who cooperate with the competent authorities. The definition of the offense is set by Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. It relies on the same elements as the Palermo Protocol[79] and has the same scope as the Warsaw Convention. Furthermore, it defines

Pénal, Dalloz, January 2023, p. 17. Similarly, the US policies highly focus on domestic trafficking. Trafficking can also "*vary from single individuals or soloists, to complex networks involving numerous individuals*," A. Aronowitz, G. Theuermann, E. Tyurykanova, *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime*, OSCE, May 2010, p. 27. In a study, authors theorize three levels of structures: individual traffickers, small-to-medium (family-based) organized criminal groups, and large and loose criminal networks, O. Shentov, A. Rusev, G.A. Antonopoulos, *Financing of Organised Crime: Human Trafficking in Focus*, Sofia, Center for the Study of Democracy, EU, 2018, pp. 38-44

[74] Article 4.a of the Warsaw Convention

[75] Article 2 of the Warsaw Convention

[76] Articles 10 to 17 of the Warsaw Convention. In particular, the Warsaw Convention mandates states to create a mechanism to offer a recovery and reflection period and a residence permit to trafficked victims, Articles 13 and 14.

[77] Article 36 of the Warsaw Convention. While it does not have the power to sanction a failing state, it publishes regular national reports with recommendations that can be followed by recommendations by the Committee of Parties, Article 38.7. As the evaluations take into account not only the legal framework but also its practical implementation, the ECHR relies on these reports to scale the effectiveness of the operational procedures, ECHR, *Chowdury and Others v. Greece*, March 30, 2017, no. 21884/15, ¶ 44; ECHR, *S.M. v. Croatia*, June 25, 2020, no. 60561/14, ¶¶ 170-172; ECHR, *Zoletic and Others v. Azerbaijan*, October 7, 2021, no. 20116/12, ¶ 118

[78] See Joint Action 96/700/JHA adopted by the Council on the basis of Article K.3 of the Treaty on European Union, establishing an incentive and exchange programme for persons responsible for combating trade in human beings and the sexual exploitation of children

[79] Article 2.1 of Directive 2011/36/EU

the position of vulnerability[80] and extends the list of forms of exploitation, adding begging and the exploitation of criminal activities.[81]

18. Thus, human trafficking receives three different, although similar, definitions at the supranational level. Consequently, national definitions adapted this definition into their legal frameworks.

II. National frameworks

19. The European definitions. All three European frameworks define human trafficking, according to the Palermo Protocol methodology,[82] but the content of the three elements differs slightly. France, Romania, and Spain consider the acts of trafficking as in the Protocol: recruiting, transporting, transferring, harboring, and receiving.[83] Spain further transposed Directive 2011/36/EU by adding "*the exchange or transfer of control*."[84] The means of trafficking highlight further differences. All three frameworks include the use of coercion, fraud, or deception against the victim, but only France extends it against their family and those with whom the victim has habitual relationships.[85] France and Spain add the use of threat, while Romania explicitly includes the use of abduction. All three criminal codes include the means of abuse of power, but only France defines them;[86] furthermore, the codes differently transposed the means of "*giving or receiving of payments or benefits to achieve the consent of a person having control over another person*"[87] and abuse of vulnerability.[88] Finally, the

[80] As "*a situation in which the person concerned has no real or acceptable alternative but to submit to the abuse involved*," Article 2.2 of the Directive 2011/36/EU
[81] Article 2.3 of Directive 2011/36/EU
[82] The Spanish framework adds further elements. It includes some details on the location of the offense: "*either in Spanish territory, or from Spain, or in transit or to Spain*"; and specifies that the means are to be proven for both national and foreign victims, Article 177 bis.1 of the Código penal. These elements have been seen as misleading and unnecessary, C. Villacampa Estiarte, "El delito de trata de seres humanos en derecho penal español tras la reforma de 2015," *in* E. Pérez Alonso (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 461-463
[83] Article 225-4-1.I of the Code pénal, Article 210.1 of the Codul penal, and Article 177 bis.1 of the Código penal
[84] Article 177 bis.1 of the Código penal in relation to Article 2.1 of Directive 2011/36/EU
[85] Article 225.4.1.I.1° of the Code pénal
[86] The abuse of power is qualified when the perpetrator is an ascendant of the victim or "*a person who has authority over that person or abuses the authority conferred by their functions*," Article 225.4.1.I.2° of the Code pénal.
[87] France deletes the latter condition of control and adds the promise of doing so, Article 225.4.1.I.4° of the Code pénal; Romania adds the verbs "*to offer*" and "*to accept*," Article 210.1.c of the Codul penal.
[88] The Spanish one transposes the EU definition, Article 177 bis.1 of the Código penal in relation to Article 2.2 of Directive 2011/36/EU. In France, vulnerability is limited to listed situations, "*due to age, illness, infirmity, physical or mental deficiency or pregnancy, apparent or known to the perpetrator*," Article 225.4.1.I.3° of the Code pénal. Similarly, the Romanian Codul penal only considers situations of "*obvious vulnerability*," which could be understood as a state visible or known by the perpetrator, Article

purpose of trafficking is differently defined in all three frameworks. The Romanian code does not define nor list forms of exploitation in the offense of trafficking[89] but, rather, along with the expressions of criminal law.[90] There, as in the Spanish offense of trafficking, it includes an exhaustive list of forms of exploitation.[91] By contrast, the French criminal code defines exploitation as "*making the victim available to the perpetrator or to a third party, even if not identified*," to commit one of the listed offenses.[92] Thus, despite a harmonized European definition, national offenses underline state sovereignty to define human trafficking.

20. The US definition. The US Code defines three forms of human trafficking, two of which are severe—sex trafficking of minors and trafficking with respect to peonage, slavery, involuntary servitude, or forced labor—as well as sex trafficking.[93] The forms of exploitation, thus, are more limited than those in supranational frameworks. The severe forms of trafficking are defined as the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, or for commercial sex when the victim is younger than 18 years old.[94] The usual means of trafficking, therefore, are not required. The general definition of sex trafficking considers two situations:[95] The first relates to the acts of trafficking: when someone knowingly "*recruits, entices, harbors, transports, provides, obtains, advertises, maintains, patronizes, or solicits*" a person for a commercial sex act,[96] and the second finds that trafficking is also committed when someone knowingly "*benefits, financially or by receiving anything of*

210.1.b. Abuse of vulnerability is equated with "*taking advantage of the impossibility of defending oneself or expressing one's will*."

[89] However, the offense is included in Chapter VII of the Codul penal, on trafficking and exploitation. The offense is thus defined along the offenses of slavery forced or compulsory labor, pimping, and exploitation of begging, Articles 209, 212 to 214.

[90] Article 182 of the Codul penal, J. Hiah, "(Anti-)trafficking for Labor Exploitation in Romania: A Labor Perspective," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1136-1137

[91] Both countries include forced labor, slavery, and similar practices (Spain explicitly adds servitude), forced begging, sexual exploitation, including in pornography, and the removal of body organs (Romania adds the removal of tissues or other cells). The Spanish code adds forced marriage. On the contrary, the French case law refuses to extend trafficking for the purpose of forced marriage, according to the principle of legality, Cour de cassation, Chambre criminelle, May 11, 2023, no. 22-85425; R. Mesa, "Le transport de mineurs aux fins de mariages arrangés n'est pas constitutif du délit de traite des êtres humains," *Actualité juridique Pénal*, Dalloz, 2023, p. 288

[92] Article 225-4-1.I of the Code pénal. These are pimping, sexual aggression, slavery, forced labor, servitude, organ removal, begging exploitation, working or living conditions contrary to the dignity of the victim, and to compel the victim to commit any crime or misdemeanor.

[93] According to the Trafficking Victims Protection Act of 2000 and its subsequent reauthorizations, see 22 US Code (USC) §7102(11) A and B.

[94] 18 USC § 1590 and § 1591

[95] 18 USC § 1591

[96] 18 USC § 1591.a.1

value, from participation in a venture which has engaged in an act described" in the first scenario.[97] In both scenarios, the perpetrator must know or, except where the act is advertising, act in reckless disregard "*of the fact that means of force, threats of force, fraud, and coercion*" were used against the victim. Therefore, the US law thus includes only a limited number of the means considered in the international framework.

21. Once human trafficking is defined, this study requires an explanation of its criminological evolution. Indeed, "*If we find that the legal texts also require knowledge of reality, we [cannot] limit ourselves to the legal texts by comparing legal norms. We have to compare the text with reality*."[98]

§2. The evolution of human trafficking

22. The opportunities for perpetrators of human trafficking were multiplied by both globalization (I) and digitalization (II). Although "*it is technically impossible to separate [them] neatly*" due to late capitalism,[99] these phenomena highlight differently the evolution of the *modus operandi* of trafficking and its origins.

I. Globalization

23. Defining globalization. Globalization led to various mutations of society, summarized as follows: the creation of a global financial market, the increased interdependence of economies and cultures, the progress of digital technologies, the construction of Europe, the weakening of the capacity of the welfare state, the emergence of private powers with transnational corporations and non-governmental organizations (NGOs), the rise in power of judges and the cult of human rights, multiculturalism within states, and the growth of individualistic pressures.[100] Thus,

---

[97] 18 USC § 1591.a.2. Here, participation is defined as "*knowingly assisting, supporting, or facilitating*," 18 USC § 1591.a.4. Venture is defined as "*any group of two or more individuals associated in fact, whether or not a legal entity*," 18 USC § 1591.a.6

[98] Max-Planck-Institut für Ausländisches und Internationales Strafrecht Internationales Kolloquium Freiburg im Breisgau), *Comparison as a method of criminal law and criminology*, *op. cit.* note 25, p. 65

[99] T. Terranova, "Free Labor," *in* T. Scholz (ed.), *Digital labor: the Internet as playground and factory*, Routledge, 2013, p. 66

[100] F. Ost, M. van de Kerchove, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications des facultés universitaires Saint-Louis, 2010, p. 12. Castells defines the global economy as the one "*whose core components have the institutional, organizational, and technological capacity to function as a unit in real time, or at a set time, on a planetary scale*," M. Castells, *La sociedad red*, Alianza Editorial SA, La era de la información: economía, sociedad y cultura, June 30, 2005, vol. 1, p. 141. Agnew criticizes this "myth" of globalization as only linked to the economy and to markets, J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 4, p. 24

globalization brings not only positive evolution but states also face a "*negative globalization*."[101] One challenge is the globalization of crimes,[102] in particular, human trafficking.[103]

24. Push and pull factors. Today, many scholars rely on the theory of the push and pull factors to explain human trafficking[104], in other words, why "*potential victims who live in 'source countries' or 'sending countries' are pushed towards 'destination countries'"* and how the latter pulls victims.[105] From the perspective of the traffickers, attracting factors may include "*high demand for cheap or uncompensated labor, weak or no laws against various forms of forced servitude*," et cetera.[106] Conversely, "*perceived opportunity for something better combined with a lack of awareness*" can attract potential victims.[107] Push factors can refer to individual characteristics such as gender, age, "*childhood abuse and/or neglect, lack of education, […] criminal history, drug and/or substance abuse, and financial stress*."[108] From a macro perspective, trafficking factors can include "*political instability[, …] income differentials between developed and developing countries[,…] the universal devaluation and marginalization of women and children[, …] urbanization and centralization of educational and employment opportunities, cultural thinking and attitude, traditional practices, domestic violence, corruption, [or] conflicts*."[109] However, the causes of trafficking are multiple

---

[101] Z. Bauman, *Liquid times: living in an age of uncertainty*, Polity Press, 2007, p. 7

[102] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit no. 1, 2004, p. 41

[103] R. Pati, "Human Trafficking: An Issue of Human and National Security," *University of Miami National Security and Armed Conflict Law Review*, 2013, vol. 4, p. 32; T. Zhidkova, "Globalization and the Emergence of Violent Non-state Actors: The Case of Human Trafficking," *New Global Studies*, De Gruyter, April 1, 2015, vol. 9, no. 1, p. 20

[104] J. Winterdyk, "Explaining Human Trafficking: Modern Day-Slavery," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1259-1260

[105] M. van Meeteren, S. Bannink, "A Transnational Field Approach to the Study of Labor Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1753

[106] L.E. Nagle, "Selling Souls: The Effect of Globalization on Human Trafficking and Forced Servitude," *Wisconsin International Law Journal*, 2008, vol. 26, no. 1, pp. 137-138; R. Pati, "Human Trafficking: An Issue of Human and National Security," *op. cit.* note 103, pp. 41-42

[107] J. Winterdyk, "Explaining Human Trafficking: Modern Day-Slavery," *op. cit.* note 104, pp. 1259-1260

[108] V. Bouché, *An Empirical Analysis of the Intersection of Organized Crime and Human Trafficking In the United States*, National criminal justice reference service - Office of Justice Programs, July 2017, p. iv

[109] E.M. Wheaton, E.J. Schauer, T.V. Galli, "Economics of Human Trafficking," *International Migration*, July 19, 2010, vol. 48, no. 4, p. 121. See also L.E. Nagle, "Selling Souls," *op. cit.* note 106, pp. 137-138; I. Churakova, A. van der Westhuizen, "Human Trafficking in the Russian Federation: Scope of the Problem," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1080. For another list and explanation of push and pull factors, see A. Stanojoska, B. Petrevski, "Theory of push and pull factors: a new way of explaining the old," *Conference: Archibald Reiss Days*, Belgrade, Serbia, March 1, 2012. The "*patriarchal order*" has

and vary for every victim. Thus, this theory is criticized and should be broadened.[110]

25. Increasing vulnerabilities and criminal opportunities. Nevertheless, many causes of trafficking are enhanced by globalization.[111] Thus, globalization per se is seen as a cause of trafficking.[112] In particular, one push factor is vulnerability, including poverty[113] and, more generally, the lack of opportunities. In the origin countries, globalization increases the powerlessness of vulnerable populations,[114] such as the poorest populations and minorities. When populations are migrating, globalization increases inequalities, creating a gap between those who have the economic and informational resources to migrate independently and those who need to rely on migration networks, increasing the risks of posterior trafficking.[115] At the same time, other consequences of globalization ease the traffic for exploiters. First, the globalization of information offers easy access to "*actual or potential opportunities in large cities, neighboring countries, or other destinations*."[116] As a pull factor, the

---

also been cited due to the prevalence of women and girls as victims, J. Turner, "Root Causes, Transnational Mobility and Formations of Patriarchy in the Sex Trafficking of Women," *in* M. Malloch, P. Rigby (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 194-209

[110] This division, as well as the difference between source and destination countries, has been criticized: it classifies "*whole countries as either of the following: A country that solely attracts victims; A country that solely repels victims; A country that neither repels nor attracts victims, […] Simply classifying countries into one of these categories could result in tunnel vision*," and in blind spots during identification, S.L.J. Kragten-Heerdink, C.E. Dettmeijer-Vermeulen, D.J. Korf, "More Than Just 'Pushing and Pulling': Conceptualizing Identified Human Trafficking in the Netherlands," *Crime & Delinquency*, December 1, 2018, vol. 64, no. 13, p. 1768. This theory is criticized for creating a "*bipolar framework of analysis opposing sending and receiving countries that reinforces the borders between the two*," S. Cheng, "A critical engagement with the 'pull and push' model Human trafficking and migration into sex work," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, pp. 500, 504. See also, S. Mezzadra, R. Nunes, "The gaze of autonomy Capitalism, migration and social struggles," *in* V. Squire (ed.), *The contested politics of mobility: borderzones and irregularity*, Routledge, Routledge advances in international relations and global politics no. v. 87, 2011, p. 127

[111] J. Winterdyk, "Explaining Human Trafficking: Modern Day-Slavery," *op. cit.* note 104, pp. 1259-1260; H. Cameron, "The New Raw Resources Passing Through the Shadows," *in* M. Malloch, P. Rigby (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, p. 210

[112] E.M. Wheaton, E.J. Schauer, T.V. Galli, "Economics of Human Trafficking," *op. cit.* note 109, p. 121; H. Askola, "Regional Responses to Human Trafficking in Southeast Asia and Australasia," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 903

[113] G. Sekhon, "Combating Trafficking in Persons Through Public Awareness and Legal Education of Duty Bearers in India," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 731; P.L. Kerr, "Push and Pull: The Intersections of Poverty, Health Disparities, and Human Trafficking," *Public Health & Social Justice, Cancer InCytes Magazine*, 2014, vol. 3, no. 2, pp. 1-5

[114] J. Winterdyk, "Explaining Human Trafficking: Modern Day-Slavery," *op. cit.* note 104, pp. 1257-1274

[115] K. Alden Dinan, "Globalization and national sovereignty: From migration to trafficking," *in* S. Cameron, E. Newman (eds.), *Trafficking in humans: social, cultural and political dimensions*, UN University Press, 2008, p. 64

[116] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 72, p. 26

globalization of information feeds motivations to migrate, giving an already-prepared speech to exploiters to deceive their victims. Second, globalization facilitates travel and "*the ability to embed illegal activities within legal and normal activities*."[117]

26. The current globalization is not "*entirely new*,"[118] but this iteration is original due to the "*digital revolution*,"[119] characterized by "*technologies that make the circulation of goods and capital, as well as cultural and scientific information, almost instantaneous*."[120]

II. Digitalization

27. Defining digitalization and new technologies. Strictly understood, three concepts can be distinguished under the concept of digitalization. On the one hand, "*digitization is the transition from analog to digital, and digitalization is the process of using digitized information to simplify specific operations. […] On the other hand,] informatization […] is the process by which information technologies […] have transformed economic and social relations*."[121] In general, digitalization thus relies on a wide range of technologies. "New technologies" are not so new, depending on what are believed to be new technologies.[122] Since 1940, three sectors have evolved quickly: "*microelectronics, computers, and telecommunications*,"[123] and the expansion of these technologies became global "*in less than two decades, from the mid-1970s to the mid-1990s*."[124] Castells highlights five characteristics of this digital revolution: (1) The raw material of this new society is information or data;[125] (2) This revolution affects

---

[117] P. Williams, "Trafficking in women: The role of transnational organized crime," *in* S. Cameron, E. Newman (eds.), *Trafficking in humans: social, cultural and political dimensions*, UN University Press, 2008, p. 148

[118] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 4, p. 26

[119] M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique*, Michalon Editions, 2010; M. Castells, *La sociedad red*, *op. cit.* note 100, p. 30

[120] M. Delmas-Marty, "Le droit pénal comme éthique de la mondialisation," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2004, p. 1

[121] J. Vrana, R. Singh, "Digitization, Digitalization, and Digital Transformation," *in* N. Meyendorf et al. (eds.), *Handbook of Nondestructive Evaluation 4.0*, Springer International Publishing, 2021, p. 3

[122] Recalling, for instance, the inventions of the phone by Bell in 1876, or the radio by Marconi in 1898. Moreover, the term "new technologies of information and communication" is now reduced to information and communication technologies, S. Sontag Koenig, *Technologies de l'information et de la communication et défense pénale*, Mare & Martin, Bibliothèque des thèses, 2016, p. 54. Thus, this term is "*flexible, changing as tools and means are invented and integrated into the technical background of societies*," L. Gilbert, "Présentation : Regards sur les nouvelles technologies," *Revue d'anthropologie du contemporain*, Altérités, 2008, vol. 5, no. 1, p. 4

[123] M. Castells, *La sociedad red*, *op. cit.* note 100, p. 70

[124] *Ibid.* pp. 61-63

[125] Data is the "*representation of information for automatic processing*," European Commission for the Efficiency of Justice, "European ethical Charter on the use of Artificial Intelligence in judicial systems

all sectors of the economy and all processes of life; (3) These technologies are based on a logic of interconnection between systems; (4) They are flexible, the processes are reversible, and organizations can be modified; and (5) New technologies are less distinguishable, and all technologies fit into the network society. From a material perspective, they usually integrate the same product, and from an organizational perspective, companies work together to innovate.[126] To summarize, in this study, new technologies broadly include "*all the techniques used in the processing and transmission of information*,"[127] with a particular focus on the Internet.[128]

28. Thus, digitalization opens a new chapter in globalization offering new opportunities for perpetrators (A) and leading to the global evolution of the *modus operandi* of the crime (B).

A. Digitalization facilitating human trafficking

29. Access. The facilitation of offenses, including human trafficking, by new technologies can rest on the "*triple-A engine*" theory: access, affordability, and anonymity.[129] First, cyber trafficking allows perpetrators easier access to victims.[130] Traffickers can post job offers on many websites, create a false website to lure victims, or hunt for victims on social networks. They take advantage of all online information,

---

and their environment," Council of Europe, December 4, 2018, p. 70. The notion of information "*calls for a wide interpretation of the concept, regardless of the nature or content of the information, and the technical format in which it is presented*," Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data," EU, June 20, 2007, p. 25

[126] M. Castells, *La sociedad red*, *op. cit.* note 100, pp. 105-106

[127] M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 15

[128] Generally defined as "*a global network of telecommunication resources, servers, and clients for the exchange of server and client computers, intended for the exchange of electronic messages, multimedia information, and files*," A. Desforges, E. Déterville, "Lexique sur le cyberespace," *Hérodote*, La découverte, 2014, vol. 2014/1, no. 152-153, p. 24. Further, it is "*a distributed, collaborative system structured in layers: physical infrastructure (cables, radio relays, etc.), logical infrastructure (protocols, routers, naming and addressing), applications (e-mail, Web), and a social layer*," B. de La Chapelle, "Souveraineté et juridiction dans le cyberespace," *Hérodote*, La découverte, 2014, vol. 2014/1, no. 152-153, p. 180; N. Choucri, D.D. Clark, "Who controls cyberspace?," *Bulletin of the Atomic Scientists*, SAGE Publications, September 1, 2013, vol. 69, no. 5, p. 22

[129] A. Cooper, "Sexuality and the Internet: Surfing into the New Millennium," *CyberPsychology & Behavior*, January 1998, vol. 1, no. 2, p. 187. Similarly, see G. Antonopoulos, G. Baratto, A. Di Nicola, *Technology in human smuggling and trafficking: case studies from Italy and the United Kingdom*, Springer, Springerbriefs in criminology, 2020, pp. 31-32

[130] As simplistically summarized, "*organized crime groups […] are able to buy and sell women with the ease of a mouse-click*," L. Shelley, "Human trafficking as a form of transnational crime," *in* M. Lee (ed.), *Human trafficking*, Willan, 2007, p. 119; P. Williams, "Trafficking in women," *op. cit.* note 117, p. 148

highlighting the vulnerabilities of potential victims.[131] Thus, they have "*access to a much broader pool of potential victims because traditional physical and geographical limitations do not exist*."[132] Moreover, traffickers gain new opportunities for controlling victims through cameras, permanent messaging,[133] and the like, and their control extends to victims already extracted from the exploitative situation and assisted by NGOs.[134] In this direct access, "*mobile telephones [are] a key communication channel*."[135] Conversely, digitalization offers new opportunities to access any other actor in the trafficking chain. At the transportation stage, communications between smugglers and document counterfeiters are easier and quicker. At the exploitation stage, digitalization offers new ways to advertise victims and to find people looking for their services. At the last stage, digitalization makes contact with money launderers easier. Facilitated access allows for the quickening of processes and the diversification of and specializing actors. On the contrary, impunity is increased by limiting the access of law enforcement authorities, in particular, by encryption and closed cyber spaces.[136]

30. Affordability. Second, digitalization facilitates trafficking because access is affordable. Mobile phones and computers, for example, are becoming less expensive,[137] and social networks and many websites for advertisements are free to use or require only an email address, which is also usually easy and free to create, to register. When these tools are not free, their prices can be lowered through the specialization of actors, for instance, in document fraud. Moreover, these tools are affordable as they are legal and develop in poorly regulated sectors.[138] For instance,

---

[131] S. Yu, "Human Trafficking and the Internet," *in* M. Palmiotto (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 66

[132] Secretariat of the Working Group on Trafficking in Persons, *Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons Background paper*, Conference of the Parties to the United Nations Convention against Transnational Organized Crime, UN, July 23, 2021, ¶ 12, CTOC/COP/WG.4/2021/2

[133] M. van der Watt, B. Kruger, "Breaking Bondages: Control Methods, 'Juju,' and Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 939; D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 25

[134] C. Chen, N. Dell, F. Roesner, "Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors," *Proceedings of the 28th USENIX Security Symposium*, Santa Clara, CA, USA, August 16, 2016, p. 93

[135] E. Cockbain, *Offender and Victim Networks in Human Trafficking*, Taylor & Francis Ltd, 2020, p. 123

[136] GRETA, *Online and technology-facilitated trafficking in human beings*, *op. cit.* note 16, p. 14

[137] M. Dank et al., *Estimating the Size and Structure of the Underground Commercial Sex Economy in Eight Major US Cities*, Research Report, The Urban Institute, March 2014, p. 3

[138] E. Heil, A. Nichols, "Hot spot trafficking: a theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States," *Contemporary Justice Review*, Routledge, October 2, 2014, vol. 17, no. 4, p. 428

digitalization creates new labor sectors, in which exploitation can be committed. Regarding sexual exploitation, traffickers do not necessarily need physical contact between the victim and the "client," for example, when the exploitation consists of "virtual" sex, such as live videos, webcam sex,[139] or sex chats.[140] Some types of digital labor, such as crowdsourcing services or content moderation, can occur in exploitative conditions and could be qualified as trafficking depending on the case.[141] Digitalization also affords new ways to launder money, such as neo-banking or transactions through messaging applications,[142] especially when procedures are online. In general, digitalization allows traffickers to ignore territories and rely on national legislation.

31. Anonymity. Third, digitalization fosters the anonymity of every actor in the trafficking chain. It is what Truong calls a "*virtual enclave [which] is the use of the cyberspace for [trafficking] through nearly untraceable networks*."[143] On the one hand, this process means using pseudonyms (different names) and falsifying data (changing gender,[144] ages, pictures, etc.). On the Internet, people are usually not required to identify themselves to create an email account, register on a website, and the like, allowing minor victims to become older and traffickers to hide behind an apparently legal business. On the other hand, although digitalization means keeping track of all data, law enforcement authorities must know how and where to find such data. However, proof is volatile; traffickers can erase their message applications content,

[139] Conseil fédéral, *Prostitution et traite d'êtres humains à des fins d'exploitation sexuelle Rapport*, Switzerland, June 5, 2015, p. 71; UNODC, *Global report on trafficking in persons 2020*, *op. cit.* note 21, pp. 120-123

[140] Conseil fédéral, *Prostitution et traite d'êtres humains*, *op. cit.* note 139, p. 71

[141] B. Petit, "Formes légales de travail et formes contemporaines d'esclavage," *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, pp. 220-230; A.A. Casilli, "Digital Labor Studies Go Global: Toward a Digital Decolonial Turn," *International Journal of Communication*, 2017, vol. 11, no. Special section "Global Digital Culture", p. 3938; S.T. Roberts, *Derrière les écrans*, La Découverte, October 15, 2020; J. Linchuan Qiu, "Labor and Social Media: The Exploitation and Emancipation of (almost) Everyone Online," *in* J. Burgess, A. Marwick (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 298

[142] D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 33; UNODC, *Global report on trafficking in persons 2020*, *op. cit.* note 21, p. 44

[143] T.-D. Truong, *Human trafficking and organised crime*, Institute of Social Studies, Working paper series no. 339, 2001, pp. 10-11

[144] For instance, in a French case of trafficking for the purpose of exploitation in the pornography sector, the male recruiter appeared to victims as a female Facebook profile, L. de Foucher, N. Chapuis, S. Laurent, "« C'était des viols déguisés en vidéo » : le réseau, le recruteur et les proies," *Le Monde.fr*, December 15, 2021, online https://www.lemonde.fr/police-justice/article/2021/12/15/c-etait-des-viols-deguises-en-video-le-reseau-le-recruteur-et-les-proies_6106152_1653578.html (retrieved on December 15, 2021)

post only temporary advertisements, suppress an account on a website,[145] and use specific software to foster anonymity, such as a virtual private network.[146] In summary, even if a police officer finds an online pattern of human trafficking, identifying the real person behind it might be a lengthy process.

32. As digitalization facilitates human trafficking, all of its stages are evolving.

B. A criminological study of the evolution of human trafficking

33. Cyber trafficking of humans is particularly developed at the recruitment (1) and exploitation (2) stages. However, all steps in between and thereafter are also affected (3).

1. Recruitment

34. Proactive strategies. When traffickers recruit victims, they traditionally rely on two techniques: The proactive, or "hunting," strategy consists of the trafficker actively looking for a victim and luring them, and the reactive, or "fishing," strategy consists of the trafficker setting a bait and waiting for a victim to catch it.[147] When the former strategy is developed online, the trafficker may actively look like an employer recruiting for a false job[148] or they might use cyber seduction,[149] including the lover boy method[150] or the grooming of minor victims.[151] These situations are based on the creation of

[145] J. Middleton, "From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 476

[146] GRETA, *Online and technology-facilitated trafficking in human beings*, *op. cit.* note 16, p. 14

[147] UNODC, *Global report on trafficking in persons 2020*, *op. cit.* note 21, p. 16; Secretariat of the Working Group on Trafficking in Persons, *Successful strategies for addressing the use of technology to facilitate trafficking in persons*, *op. cit.* note 132, ¶ 13

[148] See, for instance, A. Albertini, "Un vaste réseau de prostitution démantelé à Paris," *Le Monde.fr*, June 10, 2021, online https://www.lemonde.fr/police-justice/article/2021/06/10/un-vaste-reseau-de-prostitution-demantele-a-paris_6083529_1653578.html (retrieved on June 17, 2021)

[149] Commission on Crime Prevention and Criminal Justice, *Resolution 27/2*, *op. cit.* note 11

[150] A. Lavorgna, *Transit crimes in the Internet age*, *op. cit.* note 17, p. 121; Department of State, "Trafficking in persons report," US, June 2019, p. 200; F. Bovenkerk, M. van San, "Loverboys in the Amsterdam Red Light District: A realist approach to the study of a moral panic," *Crime, Media, Culture: An International Journal*, August 2011, vol. 7, no. 2, pp. 185-199; G. Antonopoulos, G. Baratto, A. Di Nicola, *Technology in human smuggling and trafficking*, *op. cit.* note 129, p. 48. For a Spanish example, see Unidad de extranjería, "Diligencias de seguimiento del delito de trata de seres humanos año 2020," Fiscalía General del Estado, Spain, 2021, p. 20

[151] Special Rapporteur on the sale of children, child prostitution and child pornography, "Report on the sale of children, child prostitution and child pornography," Commission on Human Rights, Economic and Social Council, UN, December 23, 2004, p. 2, E/CN.4/2005/78 ;

specific feelings of trust, friendship, and love to prepare the victims for later abuse.[152] The traffickers usually rely on legal means to find their victims;[153] on preexisting but magnified vulnerabilities;[154] by using profiling technology,[155] such as available data on Facebook;[156] or on any other types of digital footprints.[157]

35. Reactive strategies. When "fishing" for the victim, the trafficker will set various types of bait online. In general, "*Contact between victims and offenders [is] not just offender-initiated. There was evidence of demonstrable efforts made by victims, too, to sustain the relationships*."[158] The bait is usually a job advertisement.[159] Indeed, "*Traffickers frequently place spurious, promising advertisements on employment, dating, and marriage websites for jobs including administration, cleaning, home help, childcare, waitressing, hostessing, pole dancing, transportation, the collection and delivery of charity bags, agricultural farming and construction roles, educational courses, or work in the tourism sector*."[160] The offer might lie about the content of the later exploitation or about the conditions of work. Sex work might be hiding sexual exploitation,[161] any job offer might hide labor exploitation,[162] offering the work in a

---

[152] J.A. Kloess, A.R. Beech, L. Harkins, "Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics," *Trauma, Violence, & Abuse*, April 2014, vol. 15, no. 2, p. 128

[153] H. Brayley, E. Cockbain, G. Laycock, "The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking," *Policing*, June 1, 2011, vol. 5, no. 2, p. 137

[154] S. Howell, "Systemic Vulnerabilities on the Internet and the Exploitation of Women and Girls: Challenges and Prospects for Global Regulation," *in* H. Kury, S. Redo, E. Shea (eds.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, p. 576

[155] Europol, "The challenges of countering human trafficking in the digital era," EU, October 2020, p. 2

[156] A. Di Nicola, G. Baratto, E. Martini, *Surf and sound - The role of the internet in people smuggling and human trafficking*, Faculty of Law, University of Trento, ECrime Research Reports, March 2017, p. 42; UNODC, *Global report on trafficking in persons 2020*, *op. cit.* note 21, p. 122

[157] S. Yu, "Human Trafficking and the Internet," *op. cit.* note 131, p. 65, such as physical location through GPS tracking, F. Gerry Q.C., P. Shaw, "Emerging and Future Technology Trends in the Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants," *First International Conference on Transdisciplinary AI*, Laguna Hills, CA, USA, IEEE, September 2019, p. 2

[158] E. Cockbain, *Offender and Victim Networks in Human Trafficking*, *op. cit.* note 135, p. 127

[159] For instance, targeting people fleeing Ukraine, L. Tondo, "Ukraine prosecutors uncover sex trafficking ring preying on women fleeing country," *The Guardian*, July 7, 2022, online https://www.theguardian.com/global-development/2022/jul/07/ukraine-prosecutors-uncover-sex-trafficking-ring-preying-on-women-fleeing-country (retrieved on July 29, 2022)

[160] G. Antonopoulos, G. Baratto, A. Di Nicola, *Technology in human smuggling and trafficking*, *op. cit.* note 129, p. 44. See also, L. Holmes, "Introduction: the issue of human trafficking," *in* L. Holmes (ed.), *Trafficking and human rights: European and Asia-Pacific perspectives*, Edward Elgar, 2010, p. 9

[161] A. Sykiotou, *Trafficking in human beings: Internet recruitment*, *op. cit.* note 16, p. 32 ; A. Di Nicola, G. Baratto, E. Martini, *Surf and sound*, *op. cit.* note 156, p. 62

[162] S. Copić, M. Simeunović-Patić, "Victims of Human Trafficking Meeting Victims' Needs?," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 265. For an example, see, International Trade Union Confederation, Anti Slavery, Churches' Commission for Migrants in Europe, *The role of the Internet in trafficking for labour exploitation*, Project FINE TUNE, Co-financed by EU Prevention of and Fight against Crime Program, 2011, pp. 11, 13. However, a German analysis stated that "*the use of*

cannabis farm might hide the exploitation of forced criminality,[163] and advertisements for selling organs might hide the consequences of the operation or lie about the price.[164]

36. Cyber spaces for recruitment. At first, these contacts can take place in very highly diverse online spaces: public spaces, such as forums open to public view or comments on a public Facebook post as well as private spaces that are, not open to public view. The most-cited spaces are Facebook[165] and its message application Messenger, WhatsApp, Instagram, and Twitter.[166] In particular, the use of applications seems to depend on the age of the potential victims—for instance, Snapchat and TikTok[167] are more prevalent in the recruitment of minor victims—and on their geographical origin, since some applications are best known in some regions. Advertisement platforms are also used to advertise job openings. More organized processes might rely on legitimate-looking agency websites,[168] such as employment agencies and mail-order bride agencies,[169] by offering work, study, marriage, or travel

technology to recruit individuals for the purpose of labor exploitation appears to be less widespread," D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 22

[163] For examples, see Unidad de extranjería, *Diligencias de seguimiento del delito de trata de seres humanos año 2020*, *op. cit.* note 150, p. 23; M. Buchanan, S. Swann, "Comment le téléphone d'un adolescent a permis de démanteler un réseau de trafic d'êtres humains," *BBC News Afrique*, February 4, 2023, online https://www.bbc.com/afrique/64484326 (retrieved on February 20, 2023)

[164] E. Pearson, "Organ Trafficking – Challenges and Perspectives," *in* Sector Project against Trafficking in Women (ed.), *Challenging Trafficking in Persons - Theoretical Debate & Practical Approaches*, Federal Ministry for Economic Cooperation and Developement, Allemagne, Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH, 2005, p. 59

[165] L.B. Gezinski, K.M. Gonzalez-Pons, "Sex Trafficking and Technology: A Systematic Review of Recruitment and Exploitation," *Journal of Human Trafficking*, Routledge, February 15, 2022, vol. 0, no. 0, p. 6

[166] S. Tidball, M. Zheng, J.W. Creswell, "Buying Sex On-Line from Girls: NGO Representatives, Law Enforcement Officials, and Public Officials Speak out About Human Trafficking—A Qualitative Analysis," *Gender Issues*, March 2016, vol. 33, no. 1, p. 62; J. Middleton, "From the Street Corner to the Digital World," *op. cit.* note 145, p. 48; A. Di Nicola, G. Baratto, E. Martini, *Surf and sound*, *op. cit.* note 156, pp. 43, 50, 63

[167] B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures – Quelles réalités sociales et juridiques ?*, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020, pp. 19-20

[168] E. Morawska, "Trafficking into and from Eastern Europe," *in* M. Lee (ed.), *Human trafficking*, Willan, 2007, p. 101

[169] A. Lavorgna, *Transit crimes in the Internet age*, *op. cit.* note 17, p. 117; UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," Austria Center Vienna, UNODC, UN, February 2008, p. 8; S. Sarkar, "Use of technology in human trafficking networks and sexual exploitation: A cross-sectional multi-country study," *Transnational Social Review*, January 2, 2015, vol. 5, no. 1, p. 63; S. Copić, M. Simeunović-Patić, "Victims of Human Trafficking Meeting Victims' Needs?," *op. cit.* note 162, p. 269; A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 72, p. 131; A. Sykiotou, "Cyber trafficking," *op. cit.* note 14, p. 40; A. Sykiotou, *Trafficking in human beings: Internet recruitment*, *op. cit.* note 16, p. 60

abroad.[170] Once the conversation is in a bilateral private space, the trafficker will develop its strategy by assessing the potential victim.

37. Thus, online recruitment allows traffickers to connect with the victims, their environment, and their personal data.[171]. The lack of verification of the information on the content of the job makes it easier to hide exploitation, which is also affected by new technologies.

2. Exploitation

38. Traditional exploitation. New technologies facilitate classical forms of exploitation and create opportunities for new types of exploitation. Regarding the former, technologies are mainly used for advertisements, control, and communication. For trafficking for sexual exploitation, victims can be advertised online,[172] on general websites for global use,[173] or on specific websites dedicated to adult content.[174] These advertisements can be managed by traffickers or underlings,[175] but victims can also

[170] S. Sarkar, "Trans-border sex trafficking: identifying cases and victims in the UK," *Migration and Development*, January 2, 2014, vol. 3, no. 1, p. 96

[171] Thus, traffickers do not use cyber spaces where potential victims will not be found, such as the Dark Net, GRETA, *Online and technology-facilitated trafficking in human beings*, *op. cit.* note 16, p. 12

[172] Advertisements seem to follow the evolution of the Internet, first relying on bulletin boards for older cases, M. Graw Leary, "Fighting Fire with Fire: Technology in Child Sex Trafficking," *Duke Journal of Gender Law & Policy*, 2014, vol. 21, pp. 307-309

[173] Mainly, advertisement websites such as Craigslist and Backpage, and social networks, in particular, Facebook, L.B. Gezinski, K.M. Gonzalez-Pons, "Sex Trafficking and Technology," *op. cit.* note 165, p. 6. Are also used private groups on WhatsApp or Telegram, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 16, p. 14 ; dating applications, S. Tidball, M. Zheng, J.W. Creswell, "Buying Sex On-Line from Girls," *op. cit.* note 166, p. 62; B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures (1)*, *op. cit.* note 167, p. 45; European Commission, *Fourth report*, *op. cit.* note 11, p. 6. On the contrary, trafficked victims are not significantly advertised on the Dark Net, while it "*remains an important platform for the exchange of child sexual abuse material*," Europol, "Internet organised crime threat assessment," EU, 2021, p. 25; G. Antonopoulos, G. Baratto, A. Di Nicola, *Technology in human smuggling and trafficking*, *op. cit.* note 129, p. 29

[174] Such as general advertisement websites with a specific section for adult meetings, J. Middleton, "From the Street Corner to the Digital World," *op. cit.* note 145, p. 471; J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *Social Politics*, 2014, vol. 21, no. 3, p. 467; K. Feehs, A. Currier Wheeler, *2019 Federal Human Trafficking Report*, *op. cit.* note 58, p. 29; B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures (1)*, *op. cit.* note 167, p. 45; websites dedicated to sex work, including review boards, escort or sugar-daddy websites, K. Feehs, A. Currier Wheeler, *2019 Federal Human Trafficking Report*, *op. cit.* note 58, p. 29; J.J.M. Van Rij, *The trafficking and sexual exploitation of native Hungarian speaking women in the Netherlands. A case study into the nature of forced prostitution and the modus operandi of organised crime groups involved in human trafficking in Europe*, Thesis, Inholland University of Applied Sciences, June 2014, p. 37. The website can even be created specifically by the traffickers, A. Albertini, "Un vaste réseau de prostitution démantelé à Paris," *op. cit.* note 148

[175] A.C. Henderson, S.M. Rhodes, "'Got Sold a Dream and It Turned into a Nightmare': The Victim-Offender Overlap in Commercial Sexual Exploitation," *Journal of Human Trafficking*, Routledge, January 2, 2022, vol. 8, no. 1, p. 39

manage their own advertisements and calls.[176] Depending on the legislation about sex work, these advertisements might be more or less explicit, using certain codes and emojis.[177] Similarly, online advertisements are used to recruit victims for trafficking for the removal of organs through dedicated websites or general ones to announce the to-be-transplanted organs or brokers managing these operations.[178] Traffickers can also advertise babies for adoption,[179] or victims for forced marriage.[180] On the contrary, for labor exploitation, technologies mainly facilitate control:[181] Phones and cameras allow traffickers to constantly watch their victims.[182] Similarly, control by new technologies is used in forced criminality, such as GPS control during burglaries.[183]

39. Larger exploitation. Second, new technologies enable or facilitate the

[176] Department of State, "Trafficking in persons report," US, June 2017, p. 173. For an example, see AFP, "Démantèlement d'un réseau de prostitution qui exploitait des femmes dans le Nord et le Vaucluse," *La Dépêche*, June 1, 2021, online https://www.ladepeche.fr/2021/06/01/demantelement-dun-reseau-de-prostitution-qui-exploitait-des-femmes-dans-le-nord-et-le-vaucluse-9579683.php (retrieved on June 17, 2021); A. Griessel, "France, Colombie, Espagne : un réseau international de proxénétisme démantelé," *France Inter*, December 2, 2022, online https://www.radiofrance.fr/franceinter/france-colombie-espagne-un-reseau-international-de-proxenetisme-demantele-8069358 (retrieved on December 2, 2022)

[177] d. boyd et al., *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the US*, Microsoft Research Connections, December 2011, pp. 5-6; C. Deluzarche, "Les emojis, nouveau langage codé du crime," *Korii.*, November 11, 2020, online https://korii.slate.fr/et-caetera/emojis-emoticones-nouveau-langage-code-criminels-mafia-terroristes-messages (retrieved on November 17, 2020)

[178] M. Chawki, *La traite des êtres humains à l'ère numérique*, Éditions de Saint-Amans, 2010, p. 42; C. Fraser, "An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading," *International Journal of Development Issues*, July 4, 2016, vol. 15, no. 2, pp. 100-104, 111; Commission on Crime Prevention and Criminal Justice, *Resolution 27/2*, *op. cit.* note 11; Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 16, p. 15. Contrary to sexual exploitation, "*in the case of niche markets like organ trafficking, however, the dark web is indeed a relevant marketplace*," D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 31

[179] Committee of ministers, "Recommendation no. R (91)11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults," Council of Europe, September 9, 1991, p. 3 ; A. Sykiotou, "Cyber trafficking," *op. cit.* note 14, p. 1554 ; Special Rapporteur on the sale of children, child prostitution and child pornography, "Report," Human Rights Council, General Assembly, UN, December 22, 2014, ¶ 35, A/HRC/28/56

[180] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 16, p. 15

[181] Although there have been reports of online advertisements for selling victims for domestic work, O. Pinnell, J. Kelly, "Slave markets found on Instagram and other apps," *BBC News*, October 31, 2019, online https://www.bbc.com/news/technology-50228549 (retrieved on September 24, 2021); C. Duffy, "Facebook has known it has a human trafficking problem for years. It still hasn't fully fixed it," *CNN*, October 25, 2021, online https://www.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking/index.html (retrieved on November 7, 2021)

[182] Inter-agency coordination group against trafficking in persons, *Human trafficking and technology: trends, challenges and opportunities*, Issue Brief, no. 7, UN, 2019, p. 2

[183] See, for example, AFP, "Nancy : trois clans de Roms jugés pour «vols» et «traite d'êtres humains»," *Le Figaro.fr*, November 16, 2020, online https://www.lefigaro.fr/flash-actu/nancy-trois-clans-de-roms-juges-pour-vols-et-traite-d-etres-humains-20201116 (retrieved on November 19, 2020)

organization of wider operations, for instance, sex tours or tourism and transplant tourism. Prosecution is more difficult due to the involvement of various territories and the multiple flows of different actors.[184] Transplant tourism[185] interacts with trafficking for the removal of organs[186] with the complicity of medical insurance agents or travel agencies specializing in medical tourism.[187] Sex tours "*are increasingly reported*" in the EU.[188] In some cases, "*the whole chain is managed remotely,* via *the Internet: recruitment, apartment rentals on public platforms, publication of the [advertisements …] and the management of appointments*."[189]

40. Newer exploitation. Third, new technologies enable new forms of exploitation without direct contact between the victims and the people who benefit from their exploitation. However, it is not true to say that trafficking takes place online:[190] the offense is committed somewhere, and its consequences are real for the victim. Child sexual abuse material, or child pornography, is usually the first of these newer forms to be mentioned. Nevertheless, depending on national legislation, the facts might be prosecuted as trafficking or not.[191] Regarding adult victims, the recruitment methods of some pornography producers can also be qualified as trafficking.[192] Exploitation might

---

[184] J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation," *op. cit.* note 1, p. 1699

[185] A. Sykiotou, "Cyber trafficking," *op. cit.* note 14, p. 1556 ; Global programme against trafficking in human beings, "Toolkit to Combat Trafficking in Persons," UNODC, UN, 2008, p. 506

[186] A. Caplan et al., *Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs*, Council of Europe and UN, 2009, p. 58

[187] K. Bruckmüller, "Trafficking of Human Beings for Organ (Cells and Tissue) Removal," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 328

[188] European Commission, *Fourth report*, *op. cit.* note 11, p. 4

[189] L. Colcombet, "Proxénétisme en ligne : rencontre avec les limiers de la PJ qui luttent contre cette menace « gigantesque »," *Leparisien.fr*, July 31, 2022, online https://www.leparisien.fr/faits-divers/proxenetisme-en-ligne-rencontre-avec-les-limiers-de-la-pj-qui-luttent-contre-cette-menace-gigantesque-31-07-2022-HECM4QK5LFDQBA64MDJDDMP2DQ.php (retrieved on August 2, 2022)

[190] I. Chatzis, "Traite, esclavage et travail forcé au XXIe siècle : un état des lieux," *Diplomatie*, December 2020, no. 106, p. 44

[191] S.C. Mapp, "Domestic Sex Trafficking of Children," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 355. Indeed, "*Not all practices that involve exploitation should necessarily be treated as trafficking. Consequently, a restrictive interpretation of child trafficking is advocated here, based on the rights of the child at stake. Child trafficking can be understood as preparatory actions for the exploitation of children - the recruitment/movement of children with exploitative intention which receives a penalty; the exploitation of children, itself, usually carries its own, separate penalty, and this distinction should be maintained*," H. Sax, "Child trafficking - a call for rights-based integrated approaches," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 253

[192] R. D'Angelo, "Une enquête pour traite des êtres humains expose les pratiques de l'industrie du porno," *Mediapart.fr*, November 23, 2020; M. Marlasca, L. Rendueles, "Territorio Negro: La estrecha relación entre el cine porno y la trata de personas," *Ondacero*, March 20, 2023, online https://www.ondacero.es/programas/julia-en-la-onda/audios-podcast/territorios/negro/territorio-negro-

occur through different types of production of sexual content, such as photographs, sex chats, or live videos.[193] Furthermore, the person who benefits might be an entire population, for instance, for peaceful online interactions. Casilli highlights that "*Today, most of these digital relations of production are shaped by wage labor, slave labor, unpaid labor, precarious labor, and freelance labor, making the international division of digital labor a vast and complex network of interconnected, global processes of exploitation*."[194] In the gig economy, these digital relationships can be found in "*crowdsourcing services that match recruiters and workers to perform small, repetitive, and often unskilled tasks*"[195] or for content regulation online, as the use of foreign human moderators is on the rise.[196]

41. Among all stages of trafficking, recruitment and exploitation are the most affected by new technologies and the most researched by scholars. However, all other stages are also facilitated.

3. Other stages of the process

42. Transportation and accommodation. At all stages of the trafficking process, traffickers take advantage of online opportunities to organize their traffic. In particular, the Internet is used to book tickets for planes, trains, and buses;[197] similarly, online housing solutions, such as Airbnb[198] or Booking.com[199] are used by traffickers. Additionally, online administrative processes might be advantageous for traffickers to

estrecha-relacion-cine-porno-trata-personas_20230313640f4b0996c07c00017f63d6.html (retrieved on March 23, 2023); J. Alvarez, "Detenido por trata de personas el polémico 'streamer' que intentó vacilar a Greta Thunberg," *ElHuffPost*, December 30, 2022, online https://www.huffingtonpost.es/entry/andrew-tate-detenido-rumania-streamer-intento-vacilar-greta-thunberg-detenido-rumania-por-trata-de-personas_es_63ae2335e4b0d6f0b9f28625 (retrieved on January 2, 2023)

[193] Conseil fédéral, *Prostitution et traite d'êtres humains*, *op. cit.* note 139, p. 71; Europol, "Intelligence Notification 15/2014 Trafficking in human beings and the internet," EU, October 2014, p. 1; Eurojust, "Strategic project on Eurojust's action against trafficking in human beings Final report and action plan," EU, October 2012, p. 16; D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 28

[194] A.A. Casilli, "Digital Labor Studies Go Global," *op. cit.* note 141, p. 3950

[195] *Ibid.* p. 3938

[196] S.T. Roberts, *Derrière les écrans*, *op. cit.* note 141. See also Committee of Ministers, "Recommendation CM/Rec(2022)21 to member States on preventing and combating trafficking in human beings for the purpose of labour exploitation," Council of Europe, September 27, 2022, pp. 17-18

[197] Europol, *Intelligence Notification 15/2014*, *op. cit.* note 193, p. 2; O. Shentov, A. Rusev, G.A. Antonopoulos, *Financing of Organised Crime: Human Trafficking in Focus*, *op. cit.* note 73, p. 88

[198] R. D'Angelo, "Une enquête pour traite des êtres humains expose les pratiques de l'industrie du porno," *op. cit.* note 192; B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures (1)*, *op. cit.* note 167, p. 47; B. Lavaud-Legendre, *Approche globale et traite des êtres humains*, *op. cit.* note 33, p. 71

[199] A. Lavorgna, *Transit crimes in the Internet age*, *op. cit.* note 17, p. 124

obtain travel documentation due to the lack of physical verification. To conceal their identities, they can buy forged documents online[200] or pay remotely "*by using compromised credit card data*."[201]

43. Money laundering. Finally, the laundering of the proceeds of the offense is the last part of the trafficking process.[202] Globally prohibited under the norms published by the Financial Action Task Force,[203] the laundering stage consists of ways to reintegrate money obtained from an offense into the legal economy. To achieve this aim, traffickers can rely on alternative solutions to cash and the banking system,[204] although the former is still the most-used.[205] However, the development of online forms of exploitation supports the use of online transactions and virtual currencies.[206] In general, innovative laundering methods are not specific to human trafficking;[207] for example, traffickers can use prepaid credit cards,[208] remittance money services such as Western Union or MoneyGram,[209] or informal value transfer services such as the "hawala system"[210] that also have an online equivalent.[211] Warnings also exist regarding the use of

[200] Global programme against trafficking in human beings, *Toolkit to Combat Trafficking in Persons*, *op. cit.* note 185, p. 201; UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," *op. cit.* note 169, p. 18; A. Di Nicola, G. Baratto, E. Martini, *Surf and sound*, *op. cit.* note 156, p. 78

[201] G. Antonopoulos, G. Baratto, A. Di Nicola, *Technology in human smuggling and trafficking*, *op. cit.* note 129, p. 50

[202] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 72, pp. 9-10; A. Aronowitz, G. Theuermann, E. Tyurykanova, *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime*, *op. cit.* note 73, pp. 53, 72

[203] Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - 2012 Recommendations," 2022. See, in particular, Financial Action Task Force, Asia/Pacific Group on Money Laundering, "Financial Flows from Human Trafficking," July 2018

[204] Especially since it is highly regulated in most countries, O. Shentov, A. Rusev, G.A. Antonopoulos, *Financing of Organised Crime: Human Trafficking in Focus*, *op. cit.* note 73, p. 19

[205] *Ibid.* p. 24

[206] US Government Accountability Office, *Virtual currencies. Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, US, December 2021, p. 18, GAO-22-105462

[207] Europol, "The THB financial business model - Assessing the Current State of Knowledge," Europol public information, July 2015, p. 3

[208] D. Hughes, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *A Study of the Users*, *op. cit.* note 16, p. 14; Europol, *The THB financial business model - Assessing the Current State of Knowledge*, *op. cit.* note 207, p. 8

[209] Financial Action Task Force, "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants," July 2011, p. 7; D. Czarnecki, *Trafficking in human beings 2.0*, *op. cit.* note 13, p. 32

[210] OSCE, "Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings," 2014, p. 14

[211] Moneyval, *Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction*, Research Report, Council of Europe, March 2012, p. 40

cryptocurrencies,[212] despite not appearing "*to be widely used in the context of [human trafficking] (on the contrary, they are used to purchase live streaming of child sexual abuses)*."[213]

44. Conclusion of the section. Human trafficking is an internationally criminalized offense, although national definitions might vary. Its processes have evolved along with the opportunities offered by globalization and digitalization. According to this brief criminological study, three elements can be highlighted. First, regarding the technological tools used, traffickers seem to be keeping pace with the general population. To put it simply, traffickers follow potential victims. By the mirror effect, tools that are not widely used by the general population seem to be little used by traffickers as well. Second, there is a phenomenon of increased apparent autonomy for victims. Although their identity documents are often confiscated, it turns out that, in some cases, victims can keep a phone and manage their own agenda under the control of the trafficker. This can enhance a lack of self-identification or identification as a trafficked victim. Third, technology is primarily used to forge and maintain connections, whatever they may be. These links are multiple and often bidirectional—victim/trafficker, trafficker or victim/client, and trafficker/intermediaries—with all of these connections creating evidence that could be used by law enforcement authorities. Additionally, anti-trafficking strategies are also evolving, in particular the study of who has the power to regulate and enforce anti-trafficking actions and to what extent that study is grounded in the legal field, more specifically, in an application of the theory of sovereignty.

Section 3. Framing cyber human trafficking in the theory of sovereignty

45. Consideration of the powers of repression, coercion, and independence to regulate a criminal phenomenon relates to the theory of sovereignty. Although this remains a central concept in the legal theory of the state, it has been written countless times that it is shrinking or disappearing. In the worst cases, the theory of sovereignty

[212] J. Hoyer, "Sex trafficking in the digital age: The role of virtual currency-specific legislation in keeping pace with technology," *Wayne Law Review*, 2017, vol. 63, p. 84; Moneyval, *Typologies report on laundering the proceeds of organised crime*, Council of Europe, April 17, 2015, p. 21
[213] GRETA, *Online and technology-facilitated trafficking in human beings*, *op. cit.* note 16, p. 12

was seen as a fiction[214] or a pointless notion.[215] Thus, it appears clear that sovereignty is "*under threat or at least in transition*."[216] Before explaining how the repression of cyber human trafficking can be connected to the theory of sovereignty (§3), this concept must be defined (§1) alongside its latter evolution when facing digitalization (§2).

§1. Defining sovereignty

46. Bodin's theory of sovereignty. To understand the "*concentration of sovereignty in nations*,"[217] the historical origin of the concept must be explained.[218] During the Middle Ages, the Old French word "*sovrain*"[219] described the highest level of something or designated the position of chief.[220] Given the elusive definition of sovereignty until the Renaissance, its first conceptualization is usually attributed to Bodin.[221] However, his main goal, instead of theorizing sovereignty, was to construct guidance for a commonwealth.[222] Bodin defines it as "*the rightly ordered government of a number of families and of those things which are their common concern by a sovereign power*."[223] The basis of the modern state is not sovereignty but the sum of

[214] M. Massé, "La souveraineté pénale," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 1999, p. 907
[215] D. Herzog, *Sovereignty, RIP*, Yale University Press, 2020, p. 261
[216] D. Dyzenhaus, "Kelsen, Heller and Schmitt: Paradigms of Sovereignty Thought," *Theoretical Inquiries in Law*, 2015, vol. 16, no. 2, p. 338
[217] S. Sassen, *Losing control: sovereignty in an age of globalization*, Columbia University Press, University Seminars: Leonard Hastings Schoff Memorial Lectures, 1996, p. 8
[218] The birth of the concept is not clear; some authors consider it to have only appeared with the work of Jean Bodin first published in 1576, M. David, *La souveraineté du peuple*, Presses universitaires de France, Questions, 1st ed., 1996, p. 67; while others conceive it was used before the 16th century, O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, p. 35. Theorists such as Bodin grounded their work on the philosophy of eminent thinkers such as Aristotle: sovereignty is "*not created* ex nihilo," D. Herzog, *Sovereignty, RIP*, *op. cit.* note 215, p. 14. It supports the idea that the concept existed in practice since long ago, although the word was not used nor "*clearly established amongst the ancients*," D. Baranger, "The apparition of sovereignty," *in* H. Kalmo, Q. Skinner (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 51. However, this philosophy was not aimed at defining the state, less sovereignty, but guiding the governing of the Republic, J. Bodin, *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie no. 4619, 1993, p. 59
[219] M. David, *La souveraineté du peuple*, *op. cit.* note 218, p. 39
[220] Those definitions seemed to be similar in, for example, the Spanish and Italian languages. However, the German language uses different words for the unique concept established in the French language. "*Staatsouveränität*" is supposed to mean the abstract sovereignty of State; "*Staatsgewalt*" the practical and material power of state; or "*Organsouveränität*" the practical and organic power of state, O. Beaud, *La puissance de l'Etat*, *op. cit.* note 218, p. 18.
[221] M. David, *La souveraineté du peuple*, *op. cit.* note 218, p. 67; O. Beaud, *La puissance de l'Etat*, *op. cit.* note 218, pp. 29-35
[222] Or Republic, depending on translations.
[223] J. Bodin, *Les six livres de la République*, *op. cit.* note 218, p. 57

families, in which the husband, father, and slaveholder exercise "sovereignty" over the other members. [224]. The first understanding of sovereignty was at the individual level, and beyond the household, this family sovereign became a citizen, equal, and "*free subject dependent on the sovereignty of another*."[225] At the state level, sovereignty became the "*absolute and perpetual power of a commonwealth*."[226] It is perpetual: It is a general power, not depending on the one or various persons who were granted certain powers for a certain period of time.[227] Additionally, it is absolute: Whoever is granted such power "*cannot in any way be subject to the commands of another, for it is he who makes law for the subject, abrogates law already made, and amends obsolete law*."[228]

47. Development of sovereignty due to geopolitical context. Nevertheless, this legal theory was meant to solve a specific geopolitical context. First, at the beginning of the Renaissance, the French monarchy was "*deeply marked by seigneurial and feudal influence*."[229] The state was not the only entity to enact and implement laws. Therefore, sovereignty arose "*to legitimately enforce internal order*,"[230] in "*opposition to and struggles with the feudal estates*."[231] Sovereignty supported a state organized as an absolute monarchy. Second, the monarchy was facing geopolitical "*external threat[s]*."[232] European states were not totally independent due to the "*double tutelage of the pope and the Holy Roman Empire*."[233] Therefore, sovereignty was an "*external claim to autonomy […] directed against the universalisms of emperor and pope*."[234] Finally, some authors also underline that sovereignty was meant to create a solution to the ongoing war of religions. The political struggles challenging royal power resulted in years of invasions and civil wars.[235] The internal unity of states and their

[224] *Ibid.* chap. III, IV, V
[225] *Ibid.* p. 93
[226] *Ibid.* p. 111
[227] *Ibid.* pp. 112-119
[228] *Ibid.* p. 120
[229] M. David, *La souveraineté du peuple*, *op. cit.* note 218, p. 39. Even outside France, other entities in other states could enact law, like "*city-states in Italy, and city-leagues in Germany*," S. Sassen, *Losing control*, *op. cit.* note 217, p. 8
[230] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 4, p. 9
[231] J.L. Cohen, *Globalization and sovereignty: rethinking legality, legitimacy and constitutionalism*, Cambridge University Press, 2012, p. 27
[232] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 4, p. 9
[233] P. Beauvais, "Les mutations de la souveraineté pénale," *in* Collectif (ed.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 71
[234] J.L. Cohen, *Globalization and sovereignty*, *op. cit.* note 231, p. 28
[235] D. Herzog, *Sovereignty, RIP*, *op. cit.* note 215, p. 2, it should be noted that the author points out that those wars were not only based on religious dissent, but also on social matters.

independence from both the Holy Empire and the Catholic Church would allow for replacing "*the international unity of Christendom […] by* cuius regio, eius religio*: the ruler of each realm decides what its religion is*."[236]

48. Due to a specific geopolitical context, sovereignty was meant to justify, by contemporary theorists, starting with Bodin,[237] "*a positive conception of powers, ascribed to the legislative head of state*."[238] While the concept was originally developed to apply to individual enforcers of rules and leaders, the contemporary theory of sovereignty applies exclusively to states. While some, such as Weber, argue for the disenchantment of the world due to "*the disappearance of God from the institutional scene*," Supiot argues in favor of the enchantment of the world due to the modern creation of states, "*promoted to almighty Subject, living and supreme source of laws*."[239] However, the original basis of sovereignty and states, grounded in patriarchy and a supposed hierarchy of races, is not widely accepted any longer. Thus, this old theory faces challenges with the evolution of society and, in particular, digitalization. Facing global changes, our "*conception of sovereignty must be renewed*."[240] A new concept then appears: digital sovereignty.

§2. <u>Evolving sovereignty: digital sovereignty</u>

49. From informational sovereignty to data and technological sovereignties. Alongside the rise and growth of communication technologies appeared a new element on which sovereignty could be asserted: the control of information.[241] Classically, states control information through their techniques, by opening letters, checking the press, and listening to phone calls.[242] Thus, Gotlieb theorized the concept of informational sovereignty[243] as "*the state's ability to obtain access to information*

[236] *Ibid.* p. 13
[237] Followed by Hobbes, Grotius, Pufendorf, Vattel, …, *Ibid.* pp. 18-26
[238] J.L. Cohen, *Globalization and sovereignty*, *op. cit.* note 231, p. 27
[239] A. Supiot, *Homo juridicus essai sur la fonction anthropologique du droit*, Éditions du Seuil, 2005, p. 43
[240] M. Delmas-Marty, "Gouverner la mondialisation par le droit," *Le Grand Continent*, March 18, 2020, online https://legrandcontinent.eu/fr/2020/03/18/coronavirus-mondialisation-droit-delmas-marty/ (retrieved on July 30, 2021)
[241] P. Bellanger, *La souveraineté numérique*, Stock, 2014, p. 151
[242] M.E. Price, *Media and sovereignty: the global information revolution and its challenge to state power*, MIT Press, 2002, p. 4
[243] A. Gotlieb, C. Dalfen, K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles," *American Journal of International Law*, Cambridge University Press, April 1974, vol. 68, no. 2, p. 229

central to its governmental decision-making processes."[244] However, this concept was limited to the question of transnational flows of data and the material place of "*data accumulation and storage*."[245] This concept is interpreted today under the restrictive notion of data sovereignty.[246] A second concept has been developed: technological sovereignty. Within the EU,[247] member states should foster "*technological capabilities in a way that empowers people and businesses to seize the potential of the digital transformation*."[248] The emphasis is on the European development of critical infrastructure and digital services to reduce foreign and private dependencies.[249] Thus, it "*may encompass the advancing of the techno-economic interests […] by influencing global standard-setting, regulating international trade and competition in the technology, or by anchoring the global values which govern the development and the deployment of the technology*."[250]

50. Digital sovereignty. Data and technological sovereignties are restrictive concepts, but digital sovereignty, a more comprehensive concept, is not legally born.[251] From a positive normative perspective, digital sovereignty would be the "*power to regulate [more generally to control] what is going on in cyberspace and in the digital*

[244] *Ibid.* p. 236
[245] *Ibid.* p. 247
[246] K. Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet*, 2012, vol. 4, no. 3-4, pp. 41, 50; in particular, personal data, P. Bellanger, "Les données personnelles : une question de souveraineté," *Le débat*, Gallimard, 2015, vol. 2015/1, no. 183, pp. 14-25
[247] The lack of clarity in the use of all of these concepts in the EU literature is particularly criticized, H. Roberts et al., "Safeguarding European values with digital sovereignty: an analysis of statements and policies," *Internet Policy Review*, Alexander Von Humboldt Inst Internet & Soc, 2021, vol. 10, no. 3, pp. 4-5
[248] European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - 2030 Digital Compass: the European way for the Digital Decade," EU, September 3, 2021, p. 1. See also European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital future," EU, February 19, 2020
[249] D. Broeders, F. Cristiano, M. Kaminska, "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," *JCMS: Journal of Common Market Studies*, 2023, p. 7. Indeed, "*A new 'technological sovereignty' narrative has been increasingly and proactively disseminated to build EU-wide consensus around the need to preserve European leadership and autonomy in key technological areas. This discourse captures a constellation of past, existing and future policy activities and practices normalizing a traditionally state-centric, high-politics logic of strategic autonomy and sovereignty building, uprooted at the EU-level across defense, civilian technological and digital initiative*," R. Csernatoni, "The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty," *European Security*, Routledge, July 3, 2022, vol. 31, no. 3, p. 405
[250] M. Varju, "The Protection of Technology Sovereignty in the EU: Policy, Powers and the Legal Reality," *European law review*, Sweet & Maxwell, 2022, no. 4, pp. 569-570
[251] Derosier even argues that the word sovereignty is not accurate since it is more of a sector of regulation than an element of sovereignty, J.-P. Derosier, "Les limites du concept de souveraineté numérique," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 87

sphere, including the activities of big tech."[252] In that sense, "*Digital sovereignty is the expression of its control over the virtual mirror of the economy and the population. This virtual mirror is mainly constituted by the data of individuals or institutions, which are an increasingly strategic resource from an economic point of view and also a national security issue*."[253] From a negative normative perspective, digital sovereignty highlights the difficulties for states to regulate such spaces and then compete with private entities mastering those technologies.[254]

51. These three concepts theorize three dimensions of sovereignty facing digitalization: "*First […]: How can we preserve the traditional components of our sovereignty in a context where digital technology challenges state monopolies […]? [Second]: How can we maintain our autonomous capacity to assess, decide, and act in cyberspace? [Third]: How can we control our networks, our electronic communications, and our data, whether public or personal?*"[255] As both human trafficking and sovereignty evolve with digitalization, interlinks can be drawn from complex individual realities to a general theory.

§3. Cyber human trafficking questioning sovereignty

52. Cyber trafficking challenging state sovereignty. In this study, at the crossroads of the repression of human trafficking and the evolution of new technologies, lies the theory of sovereignty. Cyber trafficking is part of a more global recognition of cybercrimes,[256] and their prosecution requires adapting the legal framework to new objects and subjects or adopting new legal tools. In particular, the fight against cybercrimes mainly raises the problems of the definition of offenses and criminalization; the procedural powers of law enforcement authorities, including the use of artificial intelligence systems; the obtaining of electronic evidence, including when facing encryption; jurisdiction; international cooperation; and the responsibility of digital

[252] T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, p. 11
[253] S. Guillou, *La souveraineté numérique française passera par l'investissement dans les technologies numériques*, Sciences Po Paris, Chaire Digital, Gouvernance, et Souveraineté, 2020, p. 3
[254] F. G'Sell, "Remarques sur les aspects juridiques de la « souveraineté numérique »," *La revue des juristes de Sciences Po*, 2020, no. 19, pp. 52-53
[255] C. Landais, "Cyberdéfense : quelle stratégie pour la France ?," *Cahiers français*, La documentation française, June 2020, no. 415, pp. 68-69
[256] On this notion, see *infra* 296.

actors[257] regarding both criminal liability and social responsibility. All of these challenges are at the core of the repression of cyber trafficking[258] and question the sovereignty of the states. First, cyber human trafficking should be part of the cyber security strategy of states, understood as "*the set of rules that protect goods and people against the attacks that can be made on them through technologies*."[259] However, trafficking and the exploitation of people are increasingly facilitated by new technologies. Second, states should maintain independent control over their data and technological sovereignties. Nonetheless, not all states are equal in their ability to do so, and most of this control is increasingly resting in the hands of private entities: digital actors.

53. Defining digital actors. As the digital sector is increasingly involved in the repression of human trafficking, digital actors should be defined. A wide vocabulary is used to describe businesses that shape the online world: multinational companies or transnational corporations,[260] the GAMMA (Google, Apple, Microsoft, Meta, and Amazon),[261] social media or networks, platforms, online service providers, intermediaries, et cetera.[262] There is no harmonized terminology in the legal framework, and the current legal definitions "*devised for particular purposes [only] obscure a search for a broader understanding of the phenomenon*."[263] Therefore, it seems better to rely on non-legal concepts, such as platforms or online intermediaries. As intermediaries, they "*do not initiate decisions to disseminate the content, products, or services that transverse their networks or servers*."[264] However, this perspective

[257] UNODC, *Comprehensive Study on Cybercrime*, UN, February 2013, p. 69
[258] See GRETA, *Online and technology-facilitated trafficking in human beings*, *op. cit.* note 16
[259] M. Quéméner, *Le droit face à la disruption numérique*, *op. cit.* note 127, p. 67
[260] That "*refers to an economic entity operating in more than one country or a cluster of economic entities operating in two or more countries - whatever their legal form, whether in their home country or country of activity, and whether taken individually or collectively*," Commission on human rights, "Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights," Economic and Social Council, UN, August 26, 2003, ¶ 20, E/CN.4/Sub.2/2003/12/Rev.2
[261] It is possible to add the NATU (Netflix, Airbnb, Tesla, and Uber) and the BATX (Baidu, Alibaba, Tencent, and Xiaomi).
[262] R. Wentrup, P. Ström, "Online Service Providers: A New and Unique Species of the Firm?," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 157
[263] G. Dinwoodie, "Who are Internet Intermediaries?," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 56; T. Douville, "Quel droit pour les plateformes ?," *in* X. Delpech (ed.), *L'émergence d'un droit des plateformes*, Editions Dalloz, 2021, p. 221. This wide variety of digital actors "*leads to a denser legislative process*," C. Castets-Renard, V. Ndior, L. Rass-Masson, "Le marché unique numérique : quelles réalités matérielles et conceptuelles ?," *Recueil Dalloz*, Dalloz, 2019, no. 17, p. 956
[264] OECD, "The economic and social role of Internet intermediaries," 2010, p. 9 Online intermediaries are here defined as those that "*bring together or facilitate transactions between third parties on the*

offers a passive vision of these actors, while they interact in active ways to build the technical settings of cyberspace.[265] In that sense, Gillespie argues that "*platforms are not intermediaries*,"[266] while recognizing that the former notion is a "*slippery term*."[267] The concept of platforms[268] seems limited to a "*particular computer technology*" or "*method of communication*."[269] While "*there is no consensus about which services constitute 'platforms,'*" as for the notion of intermediaries, they "*can obscure or trivialize a service's editorial and publication functions*."[270] Thus, the broad concept of digital actors[271] is used to highlight their active role in shaping new technologies, online experiences, and, lately, the fight against human trafficking.

54. Rethinking sovereignty. Originally, human trafficking triggered the state's duty to protect, as the traditional sovereign. However, this theory could be disconnected

---

Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties." Online intermediaries are not defined by EU norms, while some categories are, see, for instance, Article 3 of the Digital Services Act.

[265] M. Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?*, Cambridge University Press, Cambridge Intellectual Property and Information Law, 2017, p. 13

[266] T. Gillespie, "Platforms Are Not Intermediaries," *Georgetown Law Technology Review*, July 21, 2018, vol. 2, pp. 198-216. Similarly, X. Delpech, "Propos introductifs," *in* X. Delpech (ed.), *L'émergence d'un droit des plateformes*, Editions Dalloz, 2021, p. 9

[267] T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018, p. 18

[268] Defined as "*online sites and services that a) host, organize, and circulate users' shared content or social interactions for them, b) without having produced or commissioned (the bulk of) that content, c) built on an infrastructure, beneath that circulation of information, for processing data for customer service, advertising, and profit […]: d) platforms do, and must, moderate the content and activity of users, using some logistics of detection, review, and enforcement*," *Ibid.* pp. 18-21. Common characteristics of platforms are the following: "*First, there are the economies of scale. […] There are also economies of scope: the same data can be used for different applications, for different purposes, which reduces the cost of use. There are also economies of experience and the feedback loop phenomenon: a platform that has been collecting information on its customers for a long time will be able to learn from their behavior. […] And, [there are] network effects. This concept refers to the fact that a user is all the more satisfied to use a good or service the more users use it. […As a consequence, there is a] natural tendency towards market concentration*," E. Combe, "Les plateformes : notion, enjeux et pistes d'évolution," *L'émergence d'un droit des plateformes*, Editions Dalloz, 2021, pp. 16-19

[269] See the Cambridge dictionary definitions (online).

[270] E. Goldman, *The United States' Approach to "Platform" Regulation*, SSRN Scholarly Paper, ID 4404374, Defeating Disinformation UnConference, 2023, p. 5

[271] In questioning the notion of sovereignty and the sources of regulation, other adjectives for private actors have already been used: economic actors (S.J. Kobrin, "Sovereignty@Bay: Globalization, Multinational Enterprise, and the International Political System," *in* A.M. Rugman, T. Brewer (eds.), *The Oxford Handbook of International Business*, Oxford University Press, September 2, 2009, p. 9), information economy and for-profit actors (J.E. Cohen, *Between truth and power: the legal constructions of informational capitalism*, Oxford University Press, 2019, pp. 145, 267), social actors (J. Black, "Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world," *Current Legal Problems*, Oxford University Press, February 21, 2001, vol. 54, no. 1, pp. 106-110), non-state actors (G. Shaffer, M. Pollack, "Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance," *Boston College Law Review*, September 1, 2011, vol. 52, no. 4, p. 719), corporate actors (D. Danielsen, "Corporate power and global order," *in* A. Orford (ed.), *International Law and its Others*, Cambridge University Press, 2006, p. 88). Here, the adjective aims to focus on their main sector of activity.

from the states[272] by relying on the concept of the monopoly of legitimate coercion. An evolving notion of coercion pragmatically considers its multiple sources and what is at stake to comprehensively repress human trafficking. By focusing on criminal procedure law, the state's coercion is questioned, and the role of digital actors is underlined: They control online data and the related infrastructure. Thus, a new vision of sovereignty could be applied to digital actors. By extending this study outside of criminal law, various types of relationships appear between states and digital actors. At the core of the theory of sovereignty is the independence of sovereigns. However, throughout this study, this concept is both applied and criticized. Coercion is exercised not only against a population by its sovereign but also as states and digital actors face the strategies of conflict and cooperation. Independence fades when states rely on digital actors as enforcers of law and when digital actors' actions are legitimized by states' laws. Human trafficking is a complex offense linked to and originating from many types of factors, and the crime is deeply interdependent on the evolution of society. Similarly, the theory of sovereignty relies on independence as its basis, yet, when applied to a case study, the notion of interdependence creates a new perspective of how to comprehensively and legitimately apply coercion.

55. Core question of the study. As human trafficking is facilitated by the use of new technologies by perpetrators, the strategies for its repression must be adapted. However, rather than being adapted, the traditional theory of the coercion of the sovereign seems to extend beyond the framework of the state. As various entities, particularly states and digital actors, are to contribute to the repression of cyber human trafficking and to exercise coercion, the theory of sovereignty is challenged. Instead of a demonstration in favor of its demise, this study aims to rethink the basis of the theory of sovereignty to offer a new perspective on its application, using the fight against cyber human trafficking as a case study.

56. Architecture of the study.[273] To answer this core question, this research is divided into two parts.[274] First, the repression of cyber human trafficking requires a study of who exercises coercion, particularly to establish the obligations of states as

[272] In this sense, sovereignty as an exclusive element of states is a "*prejudice of law*," V. Forray, S. Pimont, *Décrire le droit*, *op. cit.* note 37, ¶ 317

[273] The footnotes are independent in each section of the study: they start from one for every introduction and conclusion of parts and titles, as well as for every chapter.

[274] For a similar division, see C. Byk, "L'ère du numérique conduit-elle à l'émergence de nouveaux acteurs et formes de souveraineté ?," *Cahiers Droit, Sciences & Technologies*, PUP, November 17, 2022, no. 15, ¶ 8

sovereigns and the existence of new sovereigns as well as to question the role of digital actors. Second, when various sovereigns emerge, this study focuses on the ordering of coercion between them, particularly the strategies they develop and their impact on the repression of cyber human trafficking.

PART 1. CYBER TRAFFICKING AND SOVEREIGNTY: EXERCISING COERCION

57. At the crossroads between cyber human trafficking and sovereignty lies the question of the actors who are charged with fighting against this international phenomenon. For legal theorists, this question is nonsensical: Sovereignty is held by states. This theory was built to support the birth of the modern state, arguing for its absolute powers of coercion within its borders and for its radical independence from other entities, especially other states. Thus, in legal theory, the state is seen mainly as a closed system, organized by a pyramid of norms, legitimizing itself. However, when facing globalization and digitalization, the sovereignty of states is deemed to be in danger, threatened, and dying. One of these threats is human trafficking, a global criminal phenomenon resulting in the exploitation of an uncountable number of people. This process is facilitated by our globalized and digitalized society. However, from another perspective, sovereignty can be disconnected from the state and its legal system. Instead of questioning its existence, its extension, or its demise, a wider theory of coercion can be built to discuss sovereignty outside of the state. If sovereignty is no longer exclusively linked to the state, then the issue of its holders can logically be questioned. As an example of sovereign powers in action, the repression of cyber human trafficking still highlights the importance of the classical theory of sovereignty: The state remains its core (Title 1). Nonetheless, while the state increases its powers of coercion to adapt its actions to the evolution of trafficking, the particularities of cyberspace and new technologies underline the need for cooperation with other entities. In particular, in the repression of trafficking, the state cannot exist and act in a closed system; its legal framework must be complemented to be efficient. As a result, digital actors appear as core partners in the fight against cyber trafficking. In the evolution of their necessary cooperation with the state, by applying their own forms of coercion, they rise as complementary holders of coercion and, thus, of sovereignty (Title 2).

TITLE 1. STATES: APPLYING SOVEREIGNTY TO REPRESS CYBER TRAFFICKING

58. Today, sovereignty is still "*one of the most important areas of study on legal theory*."[1] At the core of this theory lies the state: Sovereignty was meant to define and theorize the state. Thus, legalists consider the state to be the central institution of legal systems, particularly to investigate, prosecute, and convict criminal offenders. As such, it is no surprise to position the state as the core actor to combat cyber human trafficking. However, this automatic consideration of legal thinkers hides the explanation behind this conclusion. Indeed, the criminal law system sanctions only the worst offenses that attack both society and the state. The principle of proportionality organizing this system supposes that human trafficking creates a specific threat to a state's sovereignty. Specifically, this threat increases when trafficking is facilitated by new technologies or is committed partly online. Although states are violated by trafficking, the theory of sovereignty also provides the tools they can use to confront this phenomenon (Chapter 1). While the theory offers the general concept of legitimate coercion, the acme of sovereignty, criminal law, provides for specific legal concepts to adapt the state's repression to the new realities of cyber trafficking. In particular, the state develops new tools of digital coercion, to broaden its jurisdiction to encompass cyberspace and to provide law enforcement authorities new means of investigation (Chapter 2). Thus, the theory of sovereignty details why and how the state is at the core of the repression of cyber human trafficking.

[1] T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, p. 3

Chapter 1. The necessity of the state's sovereignty to face cyber human trafficking

59. This first chapter frames in detail the links between state sovereignty and the offense of human trafficking, including when this crime is facilitated or committed through new technologies. While trafficking has already been defined, there is no stable definition for the theory of sovereignty. Developed to be equated with the state, a first perspective on sovereignty rests on its definition through the three material elements of a state: population, territory, and government. However, as these elements evolve or are challenged by globalization and digitalization, trafficking also hinders the state's control over them. The classical commission of the offense threatens the state, but its cyber evolution increases the possibility of violations. As such, (cyber) human trafficking is a threat to the state and its sovereignty (Section 1). Adopting a different approach to sovereignty can also offer the basis for the repression of trafficking through the legitimate coercion exerted by the state. This power evolves in a digital form to comprehensively understand the evolution of the material elements of the state and of offenses. As the theory of sovereignty gains a new layer, it seems to be an appropriate theory to frame sovereignty in the repression of human trafficking (Section 2).

Section 1. Human trafficking: a threat to the state's sovereignty

60. Threatening states, human trafficking is ranked as the second[1] or third[2] largest transnational crime worldwide. In particular, trafficking hinders the three material elements usually used to define the sovereign state, which are already in peril as a result of the variability of their definition and their evolution due to globalization[3] and digitalization.[4] In particular, globalization affects the elements of the sovereign state through the "three D" processes: "de-compartmentalization," disintermediation, and

[1] R. Pati, "Human Trafficking: An Issue of Human and National Security," *University of Miami National Security and Armed Conflict Law Review*, 2013, vol. 4, p. 33
[2] "*After arms and drug trade*," M.A. Rahman, "Human Trafficking in the era of Globalization: The case of Trafficking in the Global Market Economy," *Journal of Global Studies Transcience*, 2011, vol. 2, no. 1, p. 65
[3] H. Ruiz Fabri, "Immatériel, territorialité et État," *Archives de Philosophie du Droit*, Éditions Dalloz, 1999, vol. 43, p. 204.
[4] P. Türk, "La 'souveraineté numérique' : un concept pertinent en droit constitutionnel ?," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, pp. 21-24

deregulation.[5] Trafficking, influenced by these two phenomena, negatively affects a state's population (§1§), territory (§2), and government (§3).[6]

§1. A challenge to the state's duty to protect and power to control the population

61. Population is the first element of a state, and one of the aims of organizing states' power is to protect a determined group of people.[7] According to Bodin, this duty to protect is the first obligation of the sovereign, since such power of protection is designed to be the "*most effective*."[8] The duty to protect has two components. First, the state must protect its population from any external act of war by raising an army and developing international relations. Second, the state must ensure the equal enjoyment of life among members of its population by making rules and enforcing them. Therefore, sovereignty is the "*firewall that will protect peoples*."[9] However, the definition of this element is difficult to establish, in particular through its evolution due to globalization and digitalization (I). In all cases, human trafficking challenges the duty to protect (II).

I. Defining population to delimit sovereignty

62. Nationality: a criticized criterion. To trigger its duty to protect, the state must define who is included within its population, and the institutionalist branch calls on the legal concept of nationality to do so.[10] An objective and binary definition is that each

[5] H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 188; J. Chevallier, C. Jacques, *L'État post-moderne*, LGDJ, 4th ed., 2017, pp. 32-34

[6] P. Bellanger, "De la souveraineté numérique," *Le débat*, Gallimard, 2012, vol. 2012/3, no. 170, p. 149; Conseil d'État (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 2, pp. 67-68; W.P. Nagan, C. Hammer, "The Changing Character of Sovereignty in International Law and International Relations," *Columbia Journal of Transnational Law*, 2004, vol. 43, pp. 150-151. See also the 1933 Montevideo Convention on the Rights and Duties of States, Article 1, stating that "*The state as a person of international law should possess the following qualifications: a. a permanent population; b. a defined territory; c. government; and d. capacity to enter into relations with the other states*." On the last element, see *infra* 311 to 313.

[7] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, p. 69; That is also the foundation of the theory of Hobbes, M. David, *La souveraineté du peuple*, Presses universitaires de France, Questions, 1st ed., 1996, p. 87

[8] J. Bodin, *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie no. 4619, 1993, p. 103

[9] C. Vallar, "La souveraineté numérique : rapport de synthèse," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 227

[10] And citizenship. However, the status of citizen is, in a *stricto sensu* sense, limited to persons with civic and political rights offered by the state, S. Guinchard et al., *Lexique des termes juridiques*, Dalloz, Lexiques, 28th ed., 2020, p. 182. Therefore, it does not encompass all nationals and is very restrictive. Furthermore, other kinds of citizenship grow at the supranational level, such as European citizenship, which allows new rights on a wider territory, such as European movement freedom, J. Chevallier, C.

person, based on their administrative status, is or is not part of the population, and this determination provides the legal and political link between a person, natural or legal, and a state.[11] Nevertheless, it is a criticized criterion to wholly delimit the state's duty to protect. The division of states by nationality is no longer equivalent to their division by territory, and the common identity of nationals is blurred. This arises from societal changes, such as the "*crumbling national identity, the crisis of civic-mindedness, migratory flows, identity-based withdrawal*."[12] Additionally, it comes from legal changes. For example, states recognize "*new rights and the opening of these rights to new categories of beneficiaries*,"[13] not only to nationals of such states. This is particularly true for foreign victims of trafficking: Although they are not national victims, the unfairness of their situation triggers the state's duty to protect, particularly through residence permits.[14] Consequently, although nationality could be an "easy" criterion to define a population, other standards are needed to specifically delineate the population to be protected by the state.

63. The power to control. Differently, a general definition of such a state component could be a "*human group, i.e., the nation established on a territory delimited by borders [and] characterized by a common identity*."[15] This link between population and territory hides another idea: the power to control. The state is in a better position to protect people if they are located in territory the state controls. Consequently, the Kelsen branch defines population as "*all the people subjected to state domination*."[16] The criterion is not inherent to each person; instead, it depends on the state. On its

---

Jacques, *L'État post-moderne*, *op. cit.* note 5, pp. 281-298, or corporation citizenship, a common culture between people economically dependent on the same private entity, S. Vaidhyanathan, *The googlization of everything: and why we should worry*, University of California Press, Updated edition, 2012, p. 145

[11] The nationality condition is obtained from birth based on soil or blood rights, or can later be obtained upon specific conditions and procedures, depending on each national legislation. See S. Guinchard et al., *Lexique des termes juridiques*, *op. cit.* note 10, p. 702

[12] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, pp. 281-298. On the other side of the spectrum, it can be highlighted that people "*do not live in states as such but in much smaller areas defined by the predominant and routine activities of everyday life*," J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018, p. 45

[13] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, pp. 281-298; see also M. Delmas-Marty, *Résister, responsabiliser, anticiper, ou, Comment humaniser la mondialisation*, Seuil, 2013, p. 112

[14] Upon certain conditions, see Article 14 of the Warsaw Convention and Council Directive 2004/81/EC of 29 April 2004 on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration, who cooperate with the competent authorities

[15] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, pp. 22-23

[16] O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, pp. 118-119

territory, the state is presumed to control and protect its population. The case law of the European Court of Human Rights (ECHR) broadened this theory by considering the Convention for the Protection of Human Rights and Fundamental Freedoms (CPHR) applicable outside the jurisdiction[17] of a determined state when controlling people outside its borders.[18] Although those cases are rare and exceptional and are applicable mainly to military control, a state can be responsible for the violation of human rights of a population when it has "*physical*,"[19] "*effective*,"[20] "*full and exclusive*" control, even if only "de facto,"[21] over a territory.

64. Disintermediation. Setting aside the variability of its definition, the element of population is also questioned by globalization and, in particular, disintermediation broadly understood as the end of compartmentalization between institutions,[22] leading to a weakening of the link between the state and its population. On the one hand, by facilitating people's movement, globalization further divides the state and the status of nationality and complicates the control over people by just one state. On the other hand, people can rely on other intermediaries or technology to avoid the control of the state. While new intermediaries or technologies do not substitute for states, they create additional opportunities for the population to rely not solely on institutions controlled by the state.[23] One example would be the classical monetary function of the state,[24] which can be partially avoided today through the use of cryptocurrencies.[25]

65. People to users. A population is also challenged by digitalization by changing people into users,[26] and digitalization can be considered the birth of a "*global civil*

[17] The CPRH does not use the word "territory" but "jurisdiction."
[18] On criminal non-territorial competences, see *infra* 149 to 152.
[19] ECHR, *Loizidou v. Turkey (preliminary objections)*, March 23, 1995, no. 15318/89, ¶ 57
[20] *Ibid.* ¶ 62
[21] ECHR, *Medvedyev and Others v. France*, March 29, 2010, no. 3394/03, p. 67
[22] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit no. 1, 2004, p. 46. On the contrary, strictly defined, it tends to focus primarily on the evolution of the financial market, as "*International operators can resort directly to financial markets, without using traditional financial and banking intermediaries*," H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 200
[23] Disintermediation is mainly a myth, since it is primarily the creation of new intermediaries, at the detriment of classical ones, like the state.
[24] "*Financial issues are the backbone of the Republic*," J. Bodin, *Les six livres de la République*, *op. cit.* note 8, pp. 285, 293
[25] J.-P. Vergne, R. Durand, "Cyberespace et organisations « virtuelles » : l'Etat souverain a-t-il encore un avenir ?," *Regards croisés sur l'économie*, La Découverte, 2014, vol. 2014/1, no. 14, p. 137
[26] Although not all users are humans. Bratton includes in its User layer: animal users, artificial intelligence users and machine users, B.H. Bratton, *The stack: on software and sovereignty*, MIT Press, Software studies, 2015, p. 481

society."[27] Nonetheless, even when populations are interconnected, a global nationality or population is not created.[28] Cyberspace creates new groups of users through "*local-culture movements*."[29] At the same time, these movements are below the state level, as they do not necessarily depend on a link to a national identity or a unique nationality, and supranational, as they can amalgamate many people from different states. The categorization of those groups does not depend on the state but, for example, on similarities of interest, the use of the same platform, or the habit of playing the same game. Another distinction is drawn from this first one: Significant inequalities appear between users and non-users.[30] Originally, some users of cyberspace believed its access should be limited to those aficionados of digitalization with knowledge of informatics.[31] However, as cyberspace is theoretically now accessible globally, it is still true that there is a gap between those who have the opportunity to buy the material components to enter cyberspace and those who do not. Moreover, material components are not enough, and digital literacy is one of the states' goals to ensure that their population has the knowledge to take advantage of the global network. This division is particularly questioned regarding the use of new technologies by trafficked victims.[32]

66. The definition of the population, the first element of a state and its sovereignty, is not clear and unquestioned. Nevertheless, trafficking challenges the states' duty to protect by violating the fundamental rights of victims.

II. The violation of the population's fundamental rights

67. Human rights frameworks. Trafficked victims suffer human rights[33] violations

[27] S. Vaidhyanathan, *The googlization of everything*, *op. cit.* note 10, p. 145
[28] Which could be the origin of a global state as imagined by Kant, I. Kant et al., *Idée d'une histoire universelle au point de vue cosmopolite*, Gallimard, 2009
[29] S. Vaidhyanathan, *The googlization of everything*, *op. cit.* note 10, p. 148
[30] M. Castells, *La sociedad red*, Alianza Editorial SA, La era de la información: economía, sociedad y cultura, June 30, 2005, vol. 1, p. 418
[31] *Ibid.* p. 423
[32] J. Elliott, K. McCartan, "The Reality of Trafficked People's Access to Technology," *The Journal of Criminal Law*, June 2013, vol. 77, no. 3, pp. 255-273; A. Malpass et al., "Overcoming Digital Exclusion during the COVID-19 Pandemic: Impact of Mobile Technology for Survivors of Modern Slavery and Human Trafficking – A Mixed Method Study of Survivors and Support Service Provider Views," *Journal of Human Trafficking*, Routledge, March 29, 2022, vol. 0, no. 0, pp. 1-20
[33] Defined as "*fundamental rights to which every human being is entitled just because she or he is a human being*," J. Renzikowski, "Trafficking in human beings as a crime and as a human rights violation," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 13

during all three stages of trafficking.[34] Human (including cyber) trafficking has "*political, demographic, social, labor, and health costs*."[35] Specifically, it violates the rights protected under the 1966 International Covenant on Civil and Political Rights (ICCPR), the International Covenant on and on Economic, Social, and Cultural Rights (ICESCR),[36] and the CPHR.

68. Slavery. The human rights framework prohibits slavery,[37] and trafficking can end in slavery.[38] However, not all trafficking is slavery, and these two concepts should not be conflated.[39] Slavery is "*the status or condition of a person over whom any or all of the powers attaching to the right of ownership are exercised*."[40] People are considered mere objects, without any rights or respect. A significant example could be when traffickers sell their victims, which can happen online. The victim "belongs" to the person who bought them, who considers having the rights to use, sell, or even destroy them. Nonetheless, supranational judges extended this original definition of "chattel slavery"[41] to further types of "slavery,"[42] saying that enslavement includes not only but

[34] C. Dauvergne, *Making people illegal: what globalization means for migration and law*, Cambridge University Press, Law in context, 2008, p. 73. And it should be highlighted that victims of trafficking also usually suffer human rights violations before being trafficked, since the authors of the crime rely on preexisting vulnerabilities and the phenomenon is "*inseparable from global political and economic inequalities, uneven economic development and poverty*," J. O'Connell Davidson, "Absolving the State: the Trafficking-Slavery Metaphor," *Global Dialogue*, Summer/Autumn 2012, vol. 12, no. 2, p. 40. A study found that 60% of the trafficked victims interviewed suffered "*some form of violence prior to being trafficked, with 32% having been sexually abused and 50% physically assaulted*," C. Zimmerman et al., *Stolen smiles: a summary report on the physical and psychological health consequences of women and adolescents trafficked in Europe*, London School of Hygiene & Tropical Medicine, 2006, p. 9

[35] L. Shelley, *Human trafficking A global perspective*, Cambridge University Press, 2010, p. 60

[36] However, such division between civic and political rights and economic, social, and cultural rights can be criticized, considering they all interact together. From a practical point of view, they are interdependent, and from a theoretical point of view, the criteria used to divide them rely on the classical role of the state. Delmas-Marty argues for the indivisibility of human rights and for a hierarchy of values instead, M. Delmas-Marty, *Trois défis pour un droit mondial*, Seuil, Seuil essais, 1998, pp. 44-57

[37] Article 8 of the ICCPR and Article 4 of the CPHR

[38] Their links are recognized in the preamble of the Warsaw Convention ("*Considering that trafficking in human beings may result in slavery for victims*") and in the EU Charter of Fundamental Rights, Article 5, which prohibits human trafficking and slavery.

[39] Some authors criticize such use of the word "slavery" applied to human trafficking. See *infra* 482.

[40] Article 1.1, Slavery Convention (1926). The definition of slavery is deemed part of customary international law, Appels Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*, June 12, 2002, IT-96-23 & IT-96-23/1-A, ¶ 124

[41] The "*'acquisition' or 'disposal' of someone for monetary or other compensation*," Trial Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*, February 22, 2001, IT-96-23-T&IT-96-23/1-T, ¶ 542

[42] The international tribunal for ex-Yugoslavia affirmed that the notion should evolve "*to encompass various contemporary forms of slavery*," Appels Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Kunarac et al.*, *op. cit.* note 40, ¶ 117

also can be drawn from "*control of sexuality and forced labor*"[43] or "*human trafficking*."[44] Similarly, the ECHR expanded the prohibition of slavery: It does not require a "*genuine right of legal ownership*" but the mere deprivation of "*personal autonomy*."[45] Later, the court explicitly encompassed the concept of human trafficking within Article 4 of the CPHR, highlighting that "*trafficking in human beings, by its very nature and aim of exploitation, is based on the exercise of powers attaching to the right of ownership*."[46]

69. Health. Human trafficking also violates the right to bodily integrity.[47] Trafficking has important consequences for victims' health, both physical and psychological,[48] which have been highlighted by studies on victims of trafficking for sexual exploitation, domestic servitude,[49] and labor exploitation,[50] with violations reported during both the journey and the exploitation. For now, information is limited on the health consequences due to cyber trafficking, that might be specifically significant for the victims' mental health. These can include consequences resulting from online

[43] *Ibid.* ¶ 119

[44] Trial Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Kunarac et al.*, *op. cit.* note 41, ¶ 542

[45] ECHR, *Siliadin v. France*, July 26, 2005, no. 73316/01, ¶ 122

[46] ECHR, *Rantsev v. Cyprus and Russia*, January 7, 2010, no. 25965/04, ¶ 281

[47] Not explicitly mentioned in the ICCPR nor the ICESCR but derived from the right to security, Article 9, the prohibition of torture and inhuman or degrading treatment or punishment, Article 7, and the right to life, Article 6, when violations may threaten it, also from Article 12 of the ICESCR though the "*highest attainable standard of physical and mental health*"; derived from Articles 2 and 3 of the CPHR. Explicitly mentioned at Article 3 of the EU Charter of Fundamental Rights (between the right to life and the prohibition of torture and inhuman or degrading treatment or punishment). When the violence is pushed to the extreme, it also violates the prohibition on torture or cruel, inhuman or degrading treatment or punishment, Article 7 of the ICCPR and Article 3 of the CPHR. Torture is defined as "*any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as […] punishing him […], or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind*," Article 1.1 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984). The convention also requires that the act is "*inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity*." However, the ECHR does not require such criteria and applies Article 3 when the acts are perpetrated by private individuals, see ECHR, *A. v. the United Kingdom*, September 23, 1998, no. 100/1997/884/1096; ECHR, *Z. and Others v. the United Kingdom*, May 10, 2001, no. 29392/95. Sometimes, trafficked victims suffer extreme violence, for example, to make them comply with the demands of traffickers or as a punishment. It can be beating, deprivation of food or water, cigarettes burning, threat to their family…

[48] For a review of research on this topic, see L. Ottisova et al., "Prevalence and risk of violence and the mental, physical and sexual health problems associated with human trafficking: an updated systematic review," *Epidemiology and psychiatric sciences*, April 12, 2016, vol. 25, no. 4, pp. 317-341

[49] C. Zimmerman et al., *The Health Risks and Consequences of Trafficking in Women and Adolescents Findings from a European Study*, London School of Hygiene & Tropical Medicine, 2003; C. Zimmerman et al., *Stolen smiles*, *op. cit.* note 34

[50] S. Oram et al., "Human Trafficking and Health: A Survey of Male and Female Survivors in England," *American Journal of Public Health*, June 1, 2016, vol. 106, no. 6, pp. 1074-1076; E. Turner-Moss et al., "Labour Exploitation and Health: A Case Series of Men and Women Seeking Post-Trafficking Services," *Journal of Immigrant and Minority Health*, June 1, 2014, vol. 16, no. 3, p. 8

harassment, for instance.

70. Discrimination. Furthermore, human trafficking hinders the prohibition of discrimination.[51]. Indeed, it "*is the only area of transnational crime in which women are significantly represented—as victims, perpetrators, and as activists*."[52] In 2020, 60% of detected trafficking victims were women and girls, accounting for 91% of the detected victims trafficked for sexual exploitation.[53] Another example would be trafficking for the forced marriage of girls,[54] which "*perpetuates the cycle of women's poverty and child marriage*."[55] In general, human trafficking is widely established on a variety of discriminations, not only gender but also race, social origin, et cetera.[56]

71. Liberty and security. Third, every person has a right to liberty and security,[57]

---

[51] Human rights should be respected and protected "*without distinction of any kind, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status*," Article 2.1 of the ICCPR, Article 2.2 of the ICESCR, Article 14 of the CPHR (adding "*association with a national minority*") and Article 1 of the 12th Protocol of the CPHR

[52] L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 16

[53] UNODC, *Global report on trafficking in persons 2022*, UN, January 2023, pp. 25, 33. See also M. Nicot, "Femmes et filles, les premières victimes de la traite dans le monde," *Diplomatie*, December 2020, no. 106, p. 54

[54] Freedom of marriage is also a human right, Article 23 of the ICCPR, Article 10 of the ICESCR, Article 12 of the CPHR.

[55] "*Girls married early demonstrate significantly higher personal vulnerability and lower levels of empowerment*," N. Sarachaga-Barato, "Forced Child and Arranged Marriages," *in* L. Walker, G. Gaviria, K. Gopal (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 86-90; see also S. Kakar, "Child/Forced/Servile Marriages ⇄ Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 503-519

[56] These considerations led to a gendered approach to the phenomenon. First, it underlined the potential of trafficking to hinder women's rights, in particular in the titles of treaties, for instance: Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children–underlined by the author. However, this approach is widely discussed. On the one hand, this approach tends to disproportionately focus on sexual exploitation and hinders the possibilities for men, boys, and non-cisgender people to be identified as victims, European Commission, *Study on the gender dimension of trafficking in human beings: executive summary*, EU, 2016, p. 2. Law enforcement authorities sometimes reproduce gendered stereotypes, G. Mainsant, *Sur le trottoir, l'État: la police face à la prostitution*, Éditions du Seuil, La Couleur des idées, 2021, pp. 196-239. On the other hand, actors repressing human trafficking can impose on women a determined way to be free from trafficking without considering their own agency. At the state level, it can materialize through mandatory repatriation without taking into account the consent of the victims. Bernstein theorizes these harms under the concept of "*militarized humanitarianism*," E. Bernstein, "Militarized Humanitarianism Meets Carceral Feminism: The Politics of Sex, Rights, and Freedom in Contemporary Antitrafficking Campaigns," *Signs: Journal of Women in Culture and Society*, The University of Chicago Press, September 1, 2010, vol. 36, no. 1, pp. 45-71. For a list of harms to trafficked victims caused by the state, see A.T. Gallagher, "Human Rights and Human Trafficking: Quagmire or Firm Ground? A Response to James Hathaway," *Virginia Journal of International Law*, 2009, vol. 49, no. 4, p. 831. For a study onthe gaps between the victims' needs considered by the state and their actual needs, see C.M. Renzetti, "Service providers and their perceptions of the service needs of sex trafficking victims in the United States," *in* M. Dragiewicz (ed.), *Global Human Trafficking Critical issues and contexts*, Routledge, 2014, pp. 138-152. On the concept of agency, see *infra* 558 and 559.

[57] Article 9 of the ICCPR, Article 5 of the CPHR. Article 10 of the ICCPR will not be examined, on the obligation to be treated with humanity while deprived of liberty, since those privations are illegal. Regarding violence suffered by victims, see *supra* 69 (paragraph). It should be noted that such violations

including the right not to be deprived of such liberty for not being unable to fulfill a contractual obligation,[58] and a right to freedom of movement.[59] Traffickers usually control victims to prevent their escape through violence or by "*false imprisonment*,"[60] arranging all of their movements.[61] This privation of liberty can be justified by the trafficker because of a supposed contractual obligation, meaning the need to reimburse the costs of the travel they paid to transfer the victims, or the costs of lodging and food.[62] This practice is called debt bondage.[63] New forms of control are developed in cyber trafficking processes, whether by regularly checking on the victims' situation through phone calls, by geotagging their phones, by controlling the content they publish online or their private messages, or by using surveillance cameras. Therefore, human trafficking can potentially violate every each victim's civic and political rights,[64] which triggers the sovereign state's duty to protect.

72. Right to work and to fair working conditions. Human trafficking also hinders economic, social, and cultural rights. First, related to economic rights, every person has the right to work, including "*the opportunity to gain his living by work which he freely chooses*."[65] On the one hand, trafficked victims sometimes did not freely choose

---

can also come from the state if it detains trafficked victims, considering them authors of crimes like illegal migration or prostitution.

[58] Article 11 of the ICCPR, Article 1 of the 4th protocol of the CPHR

[59] Article 12 of the ICCPR, Article 2 of the 4th protocol of the CPHR

"[60] J. Winterdyk, B. Perrin, P.L. Reichel, "Introduction," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 5; C. Renshaw, "The Globalisation Paradox and the Implementation of International Human Rights: the Function of Transnational Networks in Combating Human Trafficking in the ASEAN Region," *Law and Society Association Australia and New Zealand (LSAANZ) Conference 2008 'W(h)ither Human Rights'*, University of Sydney, December 10, 2008, p. 3, online https://ses.library.usyd.edu.au/handle/2123/4045 (retrieved on June 8, 2021)

[61] S. Oram et al., "Human Trafficking and Health," *op. cit.* note 50, p. 1074

[62] C. Zimmerman et al., *The Health Risks and Consequences of Trafficking in Women and Adolescents*, *op. cit.* note 49, p. 38

[63] Legally defined as "*the status or condition arising from a pledge by a debtor of his personal services or of those of a person under his control as security for a debt, if the value of those services as reasonably assessed is not applied towards the liquidation of the debt or the length and nature of those services are not respectively limited and defined*," Article 1.a of the Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery (1956)

[64] Human trafficking also hinders all other human rights. For instance, the right to privacy, Article 17 of the ICCPR, Article 8 of the CPHR (for example, when the victim does not have a private space, is monitored, or must answer to their trafficker); the freedom of thought, conscience, and religion, Article 18 of the ICCPR, Article 9 of the CPHR (if the victim is prohibited from practicing their religion or is forced to realize some kind of ritual, as in the case of Nigerian victims, M. van der Watt, B. Kruger, "Breaking Bondages: Control Methods, 'Juju,' and Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 935-951); the freedom of expression, Article 19 of the ICCPR, Article 10 of the CPHR (if the victim is not able to express his or her opinion). Given their situations, in many cases, victims will not be able to exercise their political rights, Article 25 of the ICCPR.

[65] Article 6 of the ICESCR

to work for their exploiter or were defrauded of the type of work they were supposed to perform. In that sense, trafficking is closely linked to forced labor as defined by Convention No. 29 of the International Labour Organisation.[66] On the other hand, victims do not benefit from their work: Profits remain, in total or in significant part, in the hands of the exploiter.[67] Second, even when the victims freely choose a particular job, they are usually defrauded regarding the conditions of such work. Every person has the right to just and favorable working conditions,[68] but human trafficking usually violates the very basic labor rights norms regarding wages, times of work and rest, and safety.[69] Moreover, even when the trafficked victims consent to the work and its conditions, the International Labor Office underlines that this choice is valid only if the person was offered an alternative at the beginning and throughout the contract.[70] This approach is confirmed by the ECHR, since the consent of the person is not enough to exclude the possibility of forced work.[71]

73. Other rights. Additionally, every person has a right to an adequate standard of living, including the necessary food, clothing, and housing.[72] However, research reveals that many trafficked victims live in overcrowded rooms with poor basic hygiene, inadequate food and drinking water, and no clean clothing.[73] Since victims are usually working illegally and are sometimes administratively undocumented, they are unable to form or join trade unions[74] or to rely on social security systems.[75] Moreover, victims

[66] Article 2.1 of the 1930 convention
[67] One study found that "*twenty-two of thirty [trafficked] women reported keeping little (8) to none (14) of their earnings*," C. Zimmerman et al., *The Health Risks and Consequences of Trafficking in Women and Adolescents*, *op. cit.* note 49, p. 5
[68] Article 7 of the ICESCR
[69] In one study, half of the men victims worked between 9 and 12 hours per day, 25% worked more than 13 hours; and 40% of the women victims did not have fixed hours, S. Oram et al., "Human Trafficking and Health," *op. cit.* note 50, p. 1074. Another study found that 29% of victims out of 30 worked in unsafe conditions, 57% did not receive information on how to work safely, and 46% did not have protective equipment, E. Turner-Moss et al., "Labour Exploitation and Health," *op. cit.* note 50, p. 20
[70] International Labour Office (ed.), *The cost of coercion: global report under the follow-up to the ILO Declaration on Fundamental Principles and Rights at Work ; International Labour Conference, 98th Session*, International Labour Office Geneva, Report / International Labour Conference no. 98,1,B, 2009, p. 6
[71] ECHR, *Chowdury and Others v. Greece*, March 30, 2017, no. 21884/15, ¶ 96; ECHR, *Zoletic and Others v. Azerbaijan*, October 7, 2021, no. 20116/12, ¶ 167
[72] Article 11 of the ICESCR
[73] S. Oram et al., "Human Trafficking and Health," *op. cit.* note 50, p. 1074. See also E. Turner-Moss et al., "Labour Exploitation and Health," *op. cit.* note 50, p. 20
[74] Article 8 of the ICESCR
[75] Article 9 of the ICESCR. Additionally, studies found that many victims lack access to health information and medical care. On the contrary, some victims are forced to drink alcohol, illegal drugs, or medications, C. Zimmerman et al., *The Health Risks and Consequences of Trafficking in Women and Adolescents*, *op. cit.* note 49, p. 5; E. Turner-Moss et al., "Labour Exploitation and Health," *op. cit.* note 50, p. 20.

lack access, in many cases, to education[76] or a cultural life.[77] Finally, the CPHR protects the right to property,[78] and exploiters can confiscate part or all of the victims' earnings and, in many cases, the victims' identity documents.[79] For the ECHR, "*retention of documents [is] indicative of possible physical and mental coercion and work extracted under the menace of penalty*," and is thereby a factor in exploitation and trafficking.[80] Although data are not property, the control that exploiters have exercise the phones and social networks of the victims hinders their right to privacy.[81]

74. Independently from the definition of the "population" element of a sovereign state, trafficking, as a human crime facilitated by globalization and digitalization, hinders every fundamental right of the victims, Although comprehensive studies of the specific impacts of cyber trafficking are still lacking, trafficking challenges the state's duty to protect and power to control. Furthermore, trafficking remains an obstacle to the control of its second element: its territory.

§2. A challenge to the state's territory

75. The second material component that defines states is territory, which is the main concept permitting the delimitation of states.[82] However, its definition is blurred both by a theoretical perspective and in the light of its evolution through globalization and digitalization (I). When it is transnational, trafficking threatens this element of the state (II).

I. Defining territory to delimit sovereignty

76. The legal territory. Historically, territories were considered to be mainly property owned by lords and monarchs,[83] and such properties evolved with the

[76] Article 13 of the ICESCR, Article 2 of the first protocol to the CPHR. The lack of education is usually highlighted for children when victims of domestic servitude are told they will be given an education.
[77] Article 15 of the ICESCR
[78] Article 1 of the first protocol to the CPHR
[79] One study found that 42% of men victims and 69% of women victims had no access to their identity documents, S. Oram et al., "Human Trafficking and Health," *op. cit.* note 50, p. 1074.
[80] ECHR, *Zoletic*, *op. cit.* note 71, ¶¶ 166-168
[81] Article 8 of the CPHR
[82] S. Sassen, *Losing control: sovereignty in an age of globalization*, Columbia University Press, University Seminars: Leonard Hastings Schoff Memorial Lectures, 1996, p. 16; O. Beaud, *La puissance de l'Etat*, *op. cit.* note 16, p. 53; J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 12, p. 2
[83] J.A. Barberis, "Les liens juridiques entre l'Etat et son territoire : perspectives théoriques et évolution du droit international," *Annuaire français de droit international*, 1999, vol. 45, no. 1, p. 193; it is the theory of the "*territory-object*," where the state exercises rights *in rem*, but it cannot encompass the element of

construction of central powers and modern states:[84] The territorial basis permitted the unity of an internally divided monarchy, and lead to the sovereign state. Over time, those new borders were challenged or validated through wars and legal divisions, and their construction finally occurred with the decolonization process.[85] Today, from an institutional perspective, "territory" refers to the geographical spaces linked to a state as a natural reality.[86] From the positive legal perspective, Kelsen considers territory to be the limits of the validity of the legal order of the state,[87] which includes "*all the spaces over which a particular state has exclusive* dominion *and in which it has, in principle, an* imperium*, exclusive or concurrent, over the internal subjects*."[88] This definition aligns with the theory of Bodin: Sovereignty defines where the control of the state is absolute and acts as a "*territory limit*"[89] to such control. Therefore, by linking sovereignty to the state, Foucault underlined that sovereignty "*is only the result of a systematic process of squaring the territory by the law*."[90] However, this squaring is still variable, depending on past and current divisions of spaces and legal orders, without any criteria to define it in an abstract and geographical way.[91]

77. De-compartmentalization. This blurry definition is further questioned by globalization, which weakens national borders through the facilitation of the movement[92] of capital, products, services, humans, information, and crimes.[93] Actually, globalization translates territories into spaces, questioning the "*association between sovereignty and territory*."[94] At the same time, it also fosters the "*emergence*

territory within the concept of sovereignty, since it is mainly a power directed over people and not over a mere soil, H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 193

[84] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 12, p. 79

[85] A.-L. Amilhat Szary, *Qu'est-ce qu'une frontière aujourd'hui ?*, Presses Universitaires de France, 2015, pp. 18-24

[86] O. Beaud, *La puissance de l'Etat*, *op. cit.* note 16, pp. 122-123

[87] J.A. Barberis, "Les liens juridiques entre l'Etat et son territoire," *op. cit.* note 83, p. 140

[88] J. Combacau, S. Sur, *Droit international public*, LGDJ, 2014, p. 403

[89] H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 193. However, it is also argued that the jurisdiction defines more the positive competence than the negative one: sovereignty as territory determines "*the spatially competent state rather than the impotence of all others*," J. Combacau, "Pas une puissance, une liberté : la souveraineté internationale de l'Etat," *Pouvoirs*, 1993, no. 67, p. 134

[90] O. Beaud, *La puissance de l'Etat*, *op. cit.* note 16, p. 53

[91] V. Franssen, D. Flore, "Introduction : le droit pénal à l'ère numérique," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 10

[92] As Castells argues, territory is a specific spatial organization based on places, and he advocates for a new spatial organization based on flows. Therefore, more important than territories would be spaces, socially defined as "*the material support of the social practices shared at a specific time*," M. Castells, *La sociedad red*, *op. cit.* note 30, pp. 457, 487

[93] S. Sassen, *Losing control*, *op. cit.* note 82, p. 9

[94] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 12, p. 1

of a polycentric space."[95] The territory as well as the borders do not take into account networks and flows:[96] classically, there are flows of capital,[97] products,[98] services,[99] and people,[100] but there also are flows of information, technology, organizational interaction, images, sounds, and symbols.[101] However, states' borders remain, with a stronger legal framework seeking to control these flows, creating increasing inequalities when one wants to cross a border to take advantage of these flows. Borders must be analyzed as "*borderities*."[102]

78. Territory to cyberspace. Additionally, digitalization mainly changes the concept of territory to prefer the notion of "spaces." In particular, it creates a new type of space or place:[103] the cyberspace.[104] Digitalization disrupts "*the hitherto known balances*,"[105] especially due to its characteristics of interconnection and speed of the transfer of information.[106] The state, whose control historically relied on a physical geographical space, must face the immateriality of cyberspace:[107] "*The sovereignist order is overwhelmed*."[108] As a result of the interconnection allowed by cyberspace, the borders are difficult to draw, hindering the states' ability to control it.

79. Territory, like population, is a variable element of the sovereign state. However, when territory is classically defined as official borders, transnational trafficking is seen as a threat to sovereignty.

II. Trafficking as a threat to territory

80. Origin of trafficking. Setting aside the variability of the notion of "territory," the

[95] M. Delmas-Marty, "Les processus de mondialisation du droit," *in* C.-A. Morand (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no. 46, 2001, p. 65
[96] *Ibid.* p. 66
[97] Protected in the EU by Article 63 of the Treaty on the Functioning of the European Union
[98] Article 28 of the Treaty on the Functioning of the European Union
[99] Article 56 of the Treaty on the Functioning of the European Union
[100] Article 20 of the Treaty on the Functioning of the European Union
[101] M. Castells, *La sociedad red*, *op. cit.* note 30, p. 488
[102] A.-L. Amilhat Szary, *Qu'est-ce qu'une frontière aujourd'hui ?*, *op. cit.* note 85, p. 105
[103] F.G. Lastowka, *Virtual justice: the new laws of online worlds*, Yale University Press, 2012, p. 10
[104] For a definition of cyberspace, see *infra* 130.
[105] C. Husson-Rochcongar, "La gouvernance d'Internet et les droits de l'homme," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 49
[106] M. Delmas-Marty, *Libertés et sûreté dans un monde dangereux*, Seuil, La couleur des idées, Éditions du seuil, 2010, p. 177
[107] H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 189; C. Tulloue, "L'irréalisable souveraineté française sur les données : quels enjeux économiques ?," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 122
[108] M. Delmas-Marty, *Libertés et sûreté dans un monde dangereux*, *op. cit.* note 106, p. 198. The French original text uses the adjective "*débordé*," which could also be translated as "out of borders."

state's protection of this element is challenged by its links to trafficking. This concept was originally meant to protect states' borders. The first international treaty, the International Agreement for the suppression of the White Slave[109] Traffic[110] (1904), focused on the control of borders and the repatriation of women who were sexually exploited in foreign countries.[111] Later, the International Convention for the Suppression of the White Slave Traffic (1910) offered the first definition of trafficking— as the recruitment of women for the purpose of sexual exploitation committed in different countries[112]— and focused on international cooperation.[113] The term "white slavery" disappeared in 1921 with the International Convention for the Suppression of the Traffic in Women and Children. Those texts were meant to control territory through "*controlling immigration of women suspected of prostitution*,"[114] in the post-war xenophobic context.[115] Therefore, the historical trend indicates a focus on national security and border control.[116]

81. Trafficking versus smuggling. Transnational human trafficking

[109] On the link between human trafficking and slavery, see *supra* 68

[110] The term "white slavery" was not defined but could mean "*the procurement, by force, deceit, or drugs, of a white woman or girl against her will, for prostitution*." Although such cases were widely disseminated by the media and governments, historical research deemed that it was more of a "*myth*," J. Doezema, "Loose women or lost women? The re-emergence of the myth of white slavery in contemporary discourses of trafficking in women," *Gender Issues*, December 1999, vol. 18, no. 1, pp. 25-26; J.-M. Chaumont, C. Machiels, *Du sordide au mythe: l'affaire de la traite des Blanches (Bruxelles, 1880)*, Presses universitaires de Louvain, Histoire, justice, sociétés, 2009. See also, J. Berman, "(Un)Popular Strangers and Crises (Un)Bounded: Discourses of Sex-trafficking, the European Political Community and the Panicked State of the Modern State," *European Journal of International Relations*, SAGE Publications Ltd, March 1, 2003, vol. 9, no. 1, pp. 37-86. As such, "white slavery" is considered a "*moral panic*," M.A. Irwin, "'White Slavery' As Metaphor Anatomy of a Moral Panic," *Ex Post Facto: The History Journal*, 1996, vol. V

[111] L. Lammasniemi, "International Legislation on White Slavery and Anti-trafficking in the Early Twentieth Century," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 71. On the texts prior to the Palermo Protocol, see also E. Pomares Cintas, "La prostitución, rehén permanente del discurso de la trata de personas," *RELIES: Revista del Laboratorio Iberoamericano para el Estudio Sociohistórico de las Sexualidades*, Universidad Pablo de Olavide, December 7, 2020, no. 4, pp. 173-192

[112] Article 1 of the Convention

[113] L. Lammasniemi, "International Legislation on White Slavery," *op. cit.* note 111, pp. 72-73; in that sense, sovereignty is also seen as a limit to fighting against human trafficking, due to its territorial limits: "*Present strategies are inherently limited by state sovereignty*," L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 111

[114] L. Lammasniemi, "International Legislation on White Slavery," *op. cit.* note 111, p. 74

[115] Two more conventions were adopted afterwards, with very little impact, the first being the International Convention for the Suppression of the Traffic in Women of Full Age (1933). The subjective limitation to women has been abandoned with the Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others (1949). See *Ibid.* pp. 75-76

[116] J. O'Connell Davidson, "The Right to Locomotion? Trafficking, Slavery and the State," *in* P. Kotiswaran (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, p. 158

approximates the notion of human smuggling,[117] which is defined as "*the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident*."[118] Usually, three criteria are used to legally differentiate trafficking from smuggling.[119] The first is consent: Migrants are believed to consent to the smuggling, while the trafficked victims do not.[120] The second is exploitation: Smuggling ends with the arrival of the migrants, while the objective of trafficking is further exploitation of the victims. Finally, the third element is the transnational characteristic of the process: Smuggling must cross borders, while trafficking can be national. In that sense, "*Human trafficking is a violation of individual human rights, whereas migrant smuggling is a violation of state sovereignty*."[121] However, "*In reality the two phenomena may well overlap*."[122] Both phenomena grow from each other, in a "*continuum of facilitation*,"[123] also called known as the "*migration–trafficking nexus*."[124] Indeed, victims of trafficking can be willing to migrate and to work, but they may not know the actual conditions they

[117] E.M. Bruch, "Models wanted: The search for an effective response to human trafficking," *Stanford Journal of International Law*, 2004, vol. 40, p. 2; A. Aronowitz, "Smuggling and Trafficking in Human Beings: The Phenomenon, The Markets that Drive It and the Organisations that Promote It," *European Journal on Criminal Policy and Research*, 2001, vol. 9, no. 2, pp. 163-195

[118] Article 3.a of the Protocol against the Smuggling of Migrants by Land, Sea and Air supplementing the Palermo Convention (2000)

[119] K.A. Duong, "Human Trafficking and Migration: Examining the Issues from Gender and Policy Perspectives," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1822; UNODC, *Organized crime involvement in trafficking in persons and smuggling of migrants*, Issue Paper, UN, 2010, p. 18; W. Corrêa Da Silva, "La interseccionalidad en la trata de seres humanos: un encuentro necesario para el enfoque de derechos humanos," *in* N. Cordero Ramos, P. Zúñiga Cruz (eds.), *Trata de personas, género y migraciones en Andalucía (España), Costa Rica y Marruecos: retos y propuestas para la defensa y garantía de los derechos humanos*, Dykinson, 2019, pp. 46-47

[120] Consent is not an element to define human trafficking, see Article 3.b of the Palermo Protocol

[121] J. Winterdyk, B. Perrin, P.L. Reichel, "Introduction," *op. cit.* note 60, p. 5

[122] S. Scarpa, "UN Palermo Trafficking Protocol Eighteen Years On: A Critique," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 635; N. Prasad, B. Rohner, "Undocumented Migration, Labour Exploitation and Trafficking," *in* Sector Project against Trafficking in Women (ed.), *Challenging Trafficking in Persons - Theoretical Debate & Practical Approaches*, Federal Ministry for Economic Cooperation and Developement (Germany), Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH, 2005, p. 39; J. van der Leun, A. van Schijndel, "Emerging from the shadows or pushed into the dark? The relation between the combat against trafficking in human beings and migration control," *International Journal of Law, Crime and Justice*, March 2016, vol. 44, pp. 26-42; J. Petin, M. Poelemans, "La réponse de l'Union européenne à la traite des êtres humains," *in* B. Lavaud-Legendre (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 125; C. Bauloz, M. McAdam, J. Teye, "Human trafficking in migration pathways: Trends, challenges and new forms of cooperation," *in* International Organization for Migration (ed.), *World Migration Report 2022*, May 21, 2020, p. 255

[123] R. Skeldon, "Trafficking: A Perspective from Asia," *International Migration*, September 2000, vol. 38, no. 3, p. 10

[124] M. Lee, "Introduction : Understanding human trafficking," *in* M. Lee (ed.), *Human trafficking*, Willan, 2007, p. 13

will face.[125] On the contrary, some smuggled people might migrate, as a result of wars, persecutions, or climate change. Furthermore, smuggling might cause one to contract a debt, creating a fertile ground for exploitation. In summary, this difference is just a "*strange legal fiction*,"[126] and smuggling, as well as trafficking, may hinder state sovereignty.[127]

82. The broadness of transnational trafficking. However, transnational trafficking can be mitigated: Territory is not the main threat to sovereignty. First, the estimation of the United Nations Office on Drugs and Crime (UNODC) concludes that, in 2020, 60% of trafficked victims were trafficked domestically.[128] This trend seems to be less relevant within the EU, where approximately 37% of the registered victims were citizens of the reporting country in 2019–2020. Nevertheless, more than half of the victims registered in the EU were regionally trafficked within the EU.[129] Second, while trafficking should be transnational according to the Palermo Protocol,[130], this criterion has been erased in Europe since the Warsaw Convention.[131] However, the characteristic of a transnational process gains a new understanding in cyber trafficking: The facilitation of the process through cyberspace multiplies the connections to various

[125] J.O. Finckenauer, K. Chin, "Sex trafficking: a target for situational crime prevention?," *in* K. Bullock, R.V.G. Clarke, N. Tilley (eds.), *Situational prevention of organised crimes*, Willan, Crime science series, 2010, pp. 14-15

[126] A.T. Gallagher, "Human Rights and Human Trafficking," *op. cit.* note 56, p. 792

[127] In particular, before the 2015 reform, both offenses were conflated in the Spanish framework, in Article 177 bis of the Código penal. It takes up a large part of the doctrine to discuss the fundamental right protected by both offenses. See for instance, M. Cabanes Ferrando, *La trata de seres humanos: concepto desde el marco normativo: una aproximación al delito*, J.M. Bosch Editor, 2022, pp. 169-196; E.J. Pérez Alonso, "El bien jurídico protegido en el delito de trata de seres humanos," *in* E.B. Marín de Espinosa Ceballos et al. (eds.), *El derecho penal en el siglo XXI: Liber amicorum en honor al profesor José Miguel Zugaldía Espinar*, Tirant lo Blanch, 1st ed., 2021, pp. 521-546; C. Villacampa Estiarte, "El delito de trata de seres humanos en derecho penal español tras la reforma de 2015," *in* E. Pérez Alonso (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 447-467

[128] UNODC, *Global report on trafficking in persons 2022*, *op. cit.* note 53, p. 42

[129] European Commission, "Commission Staff Working Document Statistics and trends in trafficking in human being in the European Union in 2019-2020 Accompanying the document Report on the progress made in the fight against trafficking in human beings (Fourth Report)," EU, December 19, 2022, pp. 8-9, SWD(2022) 429 final

[130] Article 4 of the Palermo protocol. See S. Scarpa, "UN Palermo Trafficking Protocol Eighteen Years On: A Critique," *op. cit.* note 122, p. 632; A. Gallagher, *The international law of human trafficking*, Cambridge University Press, 2010, p. 74

[131] Article 2 of the Warsaw Convention: "*This Convention shall apply to all forms of trafficking in human beings, whether national or transnational*." The Directive 2011/36/EU does not explicitly address this topic but applies a wide understanding of the offense (Paragraph 9 of the preamble). For example, see Article 225-4-1 of the Code pénal (France), Article 177 bis of the Código penal (Spain, "*either in Spanish territory, or from Spain, or in transit or to Spain*"), and Articles 210 and 211 of the Codul penal (Romania).

territories and blurs the delimitation of a state's borders to repress human trafficking.

83. Although trafficking is not only transnational, it also hinders the state's border control. Therefore, it is a threat to the state's territory and, by extension, to its sovereignty. Furthermore, trafficking challenges the last element of sovereignty: government.

§3. A challenge to the state's government

84. The last component of the state is its government. Although government is the concept used to delimit both population and territory, it is the most difficult to define, both from a legal theory perspective and when facing globalization and digitalization (I). As a crime and as an attack on its population and territory, human trafficking threatens the government of the sovereign state (II).

I. Defining government to delimit sovereignty

85. Legal thinkers define government. First, from an organizational point of view, government can be defined as the institutions governing a state.[132] Broadly interpreted, "government" meant the owner of sovereignty. In the 16th century, the term "sovereign" became synonymous with "king," or "absolute ruler."[133] Afterwards, the sovereign evolved through time. During the 18th century,[134] some authors argued whether people directly or people through a representational body owned sovereignty, instead of the head of state: The legitimacy came from "*the bottom*,"[135] from the nation.[136] However, these definitions rest on the holder of sovereignty: a physical person, a specific or abstract status, or an organ. They do not offer a general concept since it depends on the internal organization of each state at a specific time. If the government equates to

[132] J.L. Cohen, *Globalization and sovereignty: rethinking legality, legitimacy and constitutionalism*, Cambridge University Press, 2012, p. 27

[133] Particularly, the sovereignty concept of Bodin was supposed to support its ownership by a monarch, J. Bodin, *Les six livres de la République*, *op. cit.* note 8; it is actually one of the criticisms against its theory, conflating sovereignty with the chief of a state, M. David, *La souveraineté du peuple*, *op. cit.* note 7, p. 68

[134] It should be noted that other authors already argue that people had power before the 18th century, even before the sovereignty of Bodin. The Estates General of 1484 were an example of the transfer of sovereignty ownership to the population M. David, *La souveraineté du peuple*, *op. cit.* note 7, p. 50

[135] W.P. Nagan, C. Hammer, "The Changing Character of Sovereignty in International Law and International Relations," *op. cit.* note 6, p. 166

[136] P. Mortier, *Les métamorphoses de la souveraineté*, Thesis, Université d'Angers, January 1, 2011, ¶¶ 24-31. For example, Montesquieu considered that, within a democracy, the sovereignty holder was the people, M. David, *La souveraineté du peuple*, *op. cit.* note 7, p. 121. Rousseau argued that people are holders of sovereignty, which is inalienable and organized through a social contract, *Ibid.* p. 85

the nation, it must define its element, which is the population. Hence, the meaning of government as the final component of the state should be separated from its material owner to define state and sovereignty.[137] Setting aside these considerations, human trafficking relies on and contributes to the weaknesses of governments, diminishing the power of the state over its territory and on its population.

86. Deregulation. Due to globalization, deregulation "*implies the retreat of nation states from important areas of decision-making*."[138] For Sassen, "*Deregulation is another name for the declining significance of the state*."[139] From an economic point of view, it is supposed to mean the development of regulation by the market actors and the withdrawal of the welfare state. However, this argument does not hold up when considering the "*recrafting [of] welfare programs and [the imposition of] austerity measures*" after the 2008–2009 global economic crisis.[140] The evolution of such regulations seems more dependent on the economic context than on a permanent consequence of globalization. However, deregulation could mean the expansion of the governance movement at the expense of government power. The term "governance" originated in the 13th century and means the art of governing.[141] With globalization, regulation does not derive only from the state: New entities, such as companies,[142] can exert a form of control on spaces or people.[143]

87. Government and digitalization. Furthermore, digitalization questions the capacity of states to govern in cyberspace. The Internet was built mainly around a cyber-libertarian ideology,[144] which was first stated by Barlow in his 1996 cyberspace independence declaration. States are "*not welcome among us*," he declared.[145] This is

---

[137] F. Mélin-Soucramanien, P. Pactet, *Droit constitutionnel: 2021*, 2020, p. 38

[138] K. Alden Dinan, "Globalization and national sovereignty: From migration to trafficking," *in* S. Cameron, E. Newman (eds.), *Trafficking in humans: social, cultural and political dimensions*, UN University Press, 2008, p. 59

[139] S. Sassen, *Losing control*, *op. cit.* note 82, p. 11

[140] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 12, p. 26

[141] A. Supiot, *La gouvernance par les nombres: cours au Collège de France (2012-2014)*, Fayard, 2020, p. 45

[142] Especially when such controls are exercised by the economic private sector, "*It substitutes calculation for law as the basis for the legitimacy of the norm*," *Ibid.* p. 174

[143] G. Lhuilier, *Le droit transnational*, Dalloz, Méthodes du droit, 2016, p. 459

[144] M. Stevenson, "From Hypertext to Hype and Back Again: Exploring the Roots of Social Media in Early Web Culture," *in* J. Burgess, A. Marwick (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 75. This ideology had "*a clear affinity with the laissez-faire ideology of the 1980s and 1990s and the prevailing ideal of minimal state and other regulatory intervention*," K.F. Aas, "Beyond 'the desert of the real': crime control in a virtual(ised) reality," *in* Y. Jewkes (ed.), *Crime online*, Willan, 2007, p. 171.

[145] M. Mossé, "Le numérique et le retour de la souveraineté," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 55; J. Perry Barlow, "Déclaration d'indépendance du

what Lessig calls "*The No Law Rule*."[146] Also known as techno libertarians, they advocated for "*a free and self-governing Internet*."[147] However, such ideology was a utopian dream, because the states did not surrender their ability to govern cyberspace. However, as territory and population are no longer clearly delimited, and in the absence of multilateral government in cyberspace,[148] this has resulted in the potential application of various sovereign national orders.[149] In practice, some parts of cyberspace are effectively regulated by various states,[150] while other spaces are left without any control.

88. The element of government also rests on a blurry and flexible definition, as do the two prior elements, population and territory. The capacity of states to actually be sovereign is further questioned by globalization and digitalization. This capacity to exercise power and to control both a population and a territory is further threatened by human trafficking.

II. Trafficking as a threat to government

89. Corruption. Trafficking threatens the state's government in various ways. First, trafficking is strongly linked to corrupt practices.[151] On the one hand, corrupt governments favor trafficking,[152] while on the other hand, trafficking favors corruption, for example, to facilitate the acquisition of migration documents such as visas, to cross

cyberespace," *in* O. Blondeau, F. Latrive (eds.), *Libres enfants du savoir numérique*, éd. de l'éclat, 2000, pp. 47-54

[146] L. Lessig, *Code*, Basic Books, 2nd ed., 2006, p. 302

[147] F.G. Lastowka, *Virtual justice*, *op. cit.* note 103, p. 80

[148] Sometimes, entities such as the Internet Corporation for Assigned Names and Numbers are deemed to govern the Net. However, that governance is only sectorial and does not offer a global regulation of the cyberspace.

[149] What Lessig calls "*The Many Laws Rule*," L. Lessig, *Code*, *op. cit.* note 146, p. 306

[150] Which produces problems of conflicting laws, J.R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology," *Texas Law Review*, 1998, vol. 76, no. 3, p. 556; J.L. Goldsmith, T. Wu, *Who controls the Internet? Illusions of a borderless world*, Oxford University Press, 2006, pp. 158-160

[151] Corruption is defined as the intentional act to "*offer, promise or give any undue pecuniary or other advantage, whether directly or through intermediaries, to a foreign public official, for that official or for a third party, in order that the official act or refrain from acting in relation to the performance of official duties, in order to obtain or retain business or other improper advantage in the conduct of international business*," Article 1.1 of the OECD Convention on Combating Bribery of Foreign Public (1997)

[152] M.A. Rahman, "Human Trafficking in the era of Globalization," *op. cit.* note 2, p. 63. Aronowitz distinguishes between "*proactive (such as actively assisting traffickers in procuring travel documents) or passive (a failure to react by turning a blind eye)*" support by the states, A. Aronowitz, *Human trafficking, human misery: the global trade in human beings*, Praeger Publishers Inc, 1st ed., 2009, p. 62

borders,[153] or to avoid law enforcement patrol surveillance.[154] Corruption "*leads to the moral and legal deterioration of a government*."[155] Trafficking linked to corruption directly hinders the power of the government and its means to fulfill its obligations as a state.[156] In that sense, Truong considers that trafficking relies on a "*social enclave […] created through social networks and links with regulated social space, [for example], the use of identities of convenience […] obtained through corruption, and bribery as well as purchase of protection services*."[157]

90. Organized criminal groups.[158] Second, trafficking weakens the power of the state when committed through by organized criminal groups,[159] from street gangs[160] to crime syndicates[161]. Those types of organizations "*directly challenge and/or disrupt the*

[153] R. Väyrynen, *Illegal Immigration, Human Trafficking, and Organized Crime*, no. DP2003-72, World Institute for Development Economic Research, WIDER Working Paper Series, 2003, p. 6
[154] E.M. Wheaton, E.J. Schauer, T.V. Galli, "Economics of Human Trafficking," *International Migration*, July 19, 2010, vol. 48, no. 4, p. 117
[155] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 152, p. 9
[156] J. Bigio, R.B. Vogelstein, *Ending Human Trafficking in the Twenty-First Century*, no. 91, Council on Foreign Relations, US, Council Special Report, June 2021, p. 19. It also hinders the rule of law, M. Delmas-Marty, *Le relatif et l'universel*, *op. cit.* note 22, p. 281
[157] T.-D. Truong, *Human trafficking and organised crime*, Institute of Social Studies, Working paper series no. 339, 2001, pp. 10-11
[158] Some of those criminal organizations relying on human trafficking can be "*terrorist organizations*," R. Pati, "Human Trafficking: An Issue of Human and National Security," *op. cit.* note 1, p. 39; J. Bigio, R.B. Vogelstein, *Ending Human Trafficking in the Twenty-First Century*, *op. cit.* note 156, p. 19. They will also hinder the power of states and legitimate governments. For terrorist organizations, these links offer sources of profits, and persons to exploit, for example women for sexual exploitation or forced marriages, or "*children as suicide bombers and beggars*," Counter-terrorism committee executive directorate, "Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing," UN Security Council, 2019, p. 10; Security Council, "Resolution 2331 (2016)," UN, December 20, 2016, p. 2, S/RES/2331 (2016); Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, *Trafficking in Human Beings and Terrorism: Where and How They Intersect - Analysis and recommendations for more effective policy responses*, OSCE, 2021. Terrorist organized groups do not receive a legal definition or the infraction of terrorism. The financing of specific acts prohibited by treaties is interdicted by the International Convention for the Suppression of the Financing of Terrorism (1999). Within the Council of Europe, the conventions to repress and prevent terrorism use the same technic of referral to other conventions (European Convention on the Suppression of Terrorism (1977), Article 1; Council of Europe Convention on the Prevention of Terrorism (2005), Article 1.1). Within the EU, terrorist offenses are defined by a list of intentional acts such as an attack upon a person, a hostage taking, or a seizure of aircraft, with one of the three aims that follow: "*(a) seriously intimidating a population; (b) unduly compelling a government or an international organization to perform or abstain from performing any act; (c) seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization*.," Article 3 of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism
[159] Which is one of the requirements to apply the Palermo protocol (Article 4 in relation with Article 2.a of the Palermo Convention). On this concept, see *infra* 212.
[160] M. Lambine, G. Gaviria, "Organized Crime, Gangs, and Trafficking," *in* L. Walker, G. Gaviria, K. Gopal (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 111-116
[161] R. Pati, "Human Trafficking: An Issue of Human and National Security," *op. cit.* note 1, p. 39

state."[162] Truong considers that there are "*territorial enclave[s as forms] of space unregulated by the state and regulated by"*[163] organized crime groups. In the worst cases, trafficking fuels "*black spots*," which are "*areas governed by transnational criminal, terrorist, and insurgent organizations that are outside effective state-based government control and are sustained by illicit economic activities*."[164] Of the 80 black spots studied by Brown and Hermann, 53% involved human trafficking.[165] The consequence is that the "*black spot becomes the 'sovereign territory' of the organization assuming political authority over the area*."[166] However, some authors criticize the lack of empirical evidence regarding the number of criminal groups that conduct human trafficking.[167] Trafficking can take place through a single perpetrator or a full criminal network.[168] According to the estimations of the UNODC, of the 686 cases studied that concluded with a conviction between 2012 and 2020, 46% involved a

[162] K.E. Bravo, "Interrogating the State's Role in Human Trafficking," *Indiana International & Comparative Law Review*, 2015, vol. 25, no. 1, p. 31. See also, D. Sansó-Rubert Pascual, "Fenómenos criminales organizados y déficit democrático. Hacia una reinterpretación del nexo político-criminal," *in* J. del Carpio Delgado (ed.), *Criminalidad en un mundo global: criminalidad de empresa, transnacional, organizada y recuperación de activos*, Tirant lo Blanch, Monografías, 2020, pp. 357-393; D. Sansó-Rubert Pascual, "Estrategias geopolíticas de la criminalidad organizada. Desafíos de la inteligencia criminal," *in* L. Zúñiga Rodríguez (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, pp. 106-110. It has also been recognized in the European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025," EU, April 14, 2021, p. 2, COM(2021) 170 final

[163] T.-D. Truong, *Human trafficking and organised crime*, *op. cit.* note 157, pp. 10-11

[164] S.S. Brown, M.G. Hermann, *Transnational Crime and Black Spots Rethinking Sovereignty and the Global Economy*, Palgrave MacMillan, International Political Economy Series, 2020, p. 1

[165] *Ibid.* p. 6

[166] *Ibid.* p. 27

[167] J. Jones, "Is It Time to Open a Conversation About a New United Nations Treaty to Fight Human Trafficking That Focuses on Victim Protection and Human Rights?," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1806. Shelley considers that "*small-scale entrepreneurship […] characterizes much of human trafficking*," L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 3. Similarly, in the study of Cockbain, the "*offender networks displayed no hierarchy and little formal structural organization: rather than looking like sophisticated criminal enterprises*," E. Cockbain, *Offender and Victim Networks in Human Trafficking*, Taylor & Francis Ltd, 2020, pp. 90-91

[168] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 152, p. 65. For the latter, he considers ten roles: investors, recruiters, transporters, corrupted public officials or protectors, informers, guides, crew members, enforcers, debt collectors, money launders, and supporting personnel and specialists. Organized criminal groups operating human trafficking "*typically operate in independent cells that deal with the various stages of recruitment transport and exploitation*," Europol, "European Union serious and organised crime threat assessment - Crime in the age of technology," EU, 2017, p. 52. In a recent French study based on judicial procedures on the prostitution of minors, other roles are distinguished. Core roles are those of patrons, tutors, and prostitutes; satellite roles are those of service providers, with a wide range of activities (logistics, control, recruitment…), B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures – Quelles réalités sociales et juridiques ?*, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020, pp. 58, 59, 80, 81

business-enterprise-type of organized criminal group.[169] However, the facilitation of trafficking through cyberspace loosens the connections between individuals, facilitating temporary and fluid networks that are more difficult to apprehend.

91. Money laundering. Third, human trafficking generates money to be laundered,[170] primarily through the financial sector. Deposits of criminal money are volatile by nature, as they are destined to be reused in short periods of time; this volatility negatively influences the liquidity and solvency of banks. Since these requests do not correspond to the needs of households and businesses, they can affect inflation and distort the results of the state's monetary policies.[171] Laundering using commercial mechanisms, such as the purchase of real estate or the export and import of goods, will distort prices, which may prevent the development of licit activities. The volatility of prices and the unpredictability of the money flows make it more difficult for the state to establish an effective economic policy.[172] From a global perspective, trafficking also creates financial losses for the state. As money escapes the grip of the state,[173] the latter also incurs expenses to finance criminal investigation, victims' and witnesses' protection, associations fighting against trafficking, and assistance to the victims.

92. Social development. Fourth, human trafficking "*contribute[s] to social inequality [and disrupts] fair competition in the market competition by exploiting slave labor at lower or no cost*."[174] Trafficking violates labor and social laws and fosters

[169] Defined as "*three or more traffickers systematically working together to traffic persons as a core component of their criminal activities*," UNODC, *Global report on trafficking in persons 2022*, *op. cit.* note 53, pp. 48-49

[170] Money laundering was historically defined in the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988, Article 3). Regarding human trafficking, Article 6.1 of the Palermo Convention offers the following definition: "*(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of his or her action; (ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; (b) Subject to the basic concepts of its legal system: (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime; (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the offenses established in accordance with this Article.*"

[171] UNODC, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, UN, October 2011, pp. 109-117

[172] B.L. Bartlett, *The negative effects of money laundering on economic development*, Regional Technical Assistance Project No.5967, The Asian Development Bank, May 2002, pp. 21-43, online https://search.informit.org/doi/abs/10.3316/agispt.20030578 (retrieved on September 2, 2021)

[173] Because tax evasion is linked to human trafficking.

[174] T. Zhidkova, "Globalization and the Emergence of Violent Non-state Actors: The Case of Human Trafficking," *New Global Studies*, De Gruyter, April 1, 2015, vol. 9, no. 1, p. 10

inequality and vulnerabilities in the population; it is a development issue.[175] The phenomenon contributes to the reproduction of racist and xenophobic behaviors, which are part of wider societal problems. When a state fails to prosecute trafficking, creating a "*juridical enclave*," Truong stresses that it promotes "*social practices such as erasure of evidence as well as cultural and psychological factors that act as an impediment for victims, witnesses, and society to come forward and prosecute perpetrators*."[176] As Shelley summarizes, the spreading of human trafficking "*will be a decline of democracy and the rule of law in established democracies and increased authoritarianism in many potentially democratic states*."[177]

93. Conclusion of the section. From its beginning, sovereignty was conflated with the state. As a result, its definition was usually linked to the latter's elements: population, territory, and government. Each of these elements is threatened by trafficking challenging the state's duty to protect its population, control its borders, and manage its government. However, each of these elements refers to the others to be defined: They change over time, and they are questioned by globalization and digitalization. This seems to be an unstable way to delimit sovereignty. Therefore, it is possible to rely on what is deemed the monopoly of the state: legitimate coercion. To repress trafficking, the sovereign states will exercise their legitimate coercion.

Section 2. State sovereignty: a solution to human trafficking

94. To distinguish what is specific to sovereignty, independent from variable components, although still theorized in the context of the state, this analysis then rests on the concept of legitimate coercion. This concept is particularly useful to delimit the powers of the state to protect its sovereignty when facing human trafficking, particularly when trafficking is facilitated by new technologies (§2). However, to adapt the usefulness of the concept of legitimate coercion, it is necessary to broaden its definition to a new, digital version (§1).

[175] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 152, p. 24. A specific example would be the incidence on public health, as trafficking, in particular for sexual exploitation, can contribute to the spread of sexually transmitted diseases, including the HIV. Oram found that "*7.7% of men and 22.5% of women reported diagnosed [sexually transmitted infections]*," S. Oram et al., "Human Trafficking and Health," *op. cit.* note 50, p. 1076.
[176] T.-D. Truong, *Human trafficking and organised crime*, *op. cit.* note 157, pp. 10-11. See also J. Bigio, R.B. Vogelstein, *Ending Human Trafficking in the Twenty-First Century*, *op. cit.* note 156, pp. 20-22
[177] L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 113

§1. From legitimate coercion to digital legitimate coercion

95. The concept of legitimate coercion is usually attributed to Weber.[178] In attempting to define politics, he ascribed his work to defining political organizations, which he equates to modern states. His definition of the state is historical and sociological, relying on its specific "*means*" instead of its goals.[179] This classical theory, developed in 1919 (I), should today be extended to digital forms of legitimate coercion (II).

I. Defining classical legitimate coercion

96. Weber claimed that the specific means of the state is the monopoly of legitimate physical violence (B), or, in a more general understanding, coercion (A).[180] Both elements of the concept should be defined separately. In the theory of sovereignty, criminal law appears to be the acme of coercion (C).

A. From violence to coercion

97. Violence and sovereignty. Weber's definition of the monopoly of the state is coherent with precedent works on sovereignty.[181] Bodin claimed that "*the prince is obliged to safeguard the persons, possessions, and families of his subjects, by force of arms, and by force of law*."[182] The first expression of a state's violence and the "*last*

[178] But other authors already relied on the monopoly of coercion to define the state. In 1877, von Jhering compared the state to a monopoly of coercion. In 1900, Jellinek relied on the concept of legal coercion to design the state. In 1911, Sohm considered legal coercion the exclusive monopoly of the state, C. Colliot-Thélène, "La fin du monopole de la violence légitime ?," *Revue d'études comparatives Est-Ouest*, Persée - Portail des revues scientifiques en SHS, 2003, vol. 34, no. 1, pp. 14-15

[179] M. Eabrasu, "Les états de la définition wébérienne de l'État," *Raisons politiques*, Presses de Sciences Po, May 4, 2012, vol. 45, no. 1, p. 195; M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, tran. R. Livingstone, p. 33

[180] The theory of Weber is still used in many recent publications, see for example, M. Castells, *La sociedad red*, *op. cit.* note 30, p. 40; C. Codron, *La surveillance diffuse : entre Droit et Norme*, Thesis, Université de Lille, June 15, 2018, p. 444; A.-L. Amilhat Szary, *Qu'est-ce qu'une frontière aujourd'hui ?*, *op. cit.* note 85, p. 59; C. Husson-Rochcongar, "La gouvernance d'Internet et les droits de l'homme," *op. cit.* note 105, p. 71; H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, pp. 187-212; M. Delmas-Marty, *Le relatif et l'universel*, *op. cit.* note 22, p. 209

[181] In that sense, the monopoly of legitimate coercion is still linked to the material components of statehood, with Weber recognizing that the "*idea of 'territory' is an essential defining feature*," M. Weber, *Le savant et le politique (1919)*, Union Générale d'Éditions, Le Monde en 10-18, 1963, p. 33. However, for this argumentation, this theory will be easier to apply to other entities than states, whose definitions of territory and population are unstable.

[182] J. Bodin, *Les six livres de la République*, *op. cit.* note 8, p. 103

bastion"[183] of sovereignty is supposed to be military force,[184] considering that it is the sovereign who can distinguish between friends and enemies.[185] This violence is exercised against aliens in the state's population. The second expression of sovereign violence is exercised against its own population. Bodin affirms that the strength of the sovereign "*lies in the coercion*"[186] applied to the population. This violence can affect both the body and the goods of the population, with the major violence available to the state being the death sentence.[187] To Weber, coercion equates to physical violence, as a restrictive definition of it. Relying on posterior works, an amplification of the meaning of violence, extended to coercion, can be drawn.

98. Coercion as physical violence. To Weber, physical violence[188] is the "*normal means of power*,"[189] necessary to avoid the disappearance of states,[190] due to the "*permanent struggle between clans or with generalized banditry*."[191] It is an enterprise of domination, in which dominators can effectively exert physical violence if necessary and in which dominated people agree to obey these dominators.[192] Afterward, this restrictive definition of coercion as physical violence was used by Kelsen, although with the term "coercion."[193] However, this thesis could be seen only as an *ultima ratio*: coercion is a broader concept.[194]

99. Weber and Kelsen: changing the interpretation. Another interpretation of Weber and Kelsen extends the definition of coercion. To Colliot-Thélène, Weber's writings broaden to "*the monopolization of the capacity to guarantee subjective rights, in other words, to make them exist*."[195] Such capacity is not limited to physical coercion. Similarly, Kelsen's theory could be widely interpreted not as "*the exclusive exercise of violence but as the exclusive right to prescribe or permit and therefore to prohibit*

[183] P. Bellanger, *La souveraineté numérique*, Stock, 2014, p. 14
[184] P. Bellanger, "De la souveraineté numérique," *op. cit.* note 6, p. 149. Beaud named that concept the military sovereignty, O. Beaud, *La puissance de l'Etat*, *op. cit.* note 16, p. 23
[185] D. Dyzenhaus, "Kelsen, Heller and Schmitt: Paradigms of Sovereignty Thought," *Theoretical Inquiries in Law*, 2015, vol. 16, no. 2, p. 341
[186] J. Bodin, *Les six livres de la République*, *op. cit.* note 8, p. 294
[187] *Ibid.* pp. 295-296
[188] M. Eabrasu, "Les états de la définition wébérienne de l'État," *op. cit.* note 179, p. 200
[189] M. Weber, *Le savant et le politique (1919)*, *op. cit.* note 181, p. 100
[190] M. Weber, *The vocation lectures*, *op. cit.* note 179, p. 33
[191] M. Eabrasu, "Les états de la définition wébérienne de l'État," *op. cit.* note 179, p. 199
[192] M. Weber, *Le savant et le politique (1919)*, *op. cit.* note 181, p. 101
[193] M. Troper, "Le monopole de la contrainte légitime," *Lignes*, Éditions Hazan, 1995, vol. n° 25, no. 2, p. 37
[194] C. Colliot-Thélène, "La fin du monopole de la violence légitime ?," *op. cit.* note 178, p. 19
[195] *Ibid.* p. 28

violence."[196] The state determines what is legal and what is not[197] and should be able to make its population obey such prescriptions through means other than physical coercion.[198] It is a "*combination of power mechanisms (coercion, assent, seduction, co-optation, etc.) involved in the exercise of authority*."[199] In that sense, Delmas-Marty recognizes the ultimate violence of the state through the privation of liberty by the institution of imprisonment and its coexistence with other "*more diffuse and less intense societal responses*."[200] In a global perspective, coercion means to influence persons to do or not do something or to do something against their will or even knowledge. In the end, an extensive signification is underlined: *"Everything that, in one way or another, coerces [the individual] can be qualified as violence*."[201]

100. On the contrary, Kant distinguishes between violence, which is limited to violence between individuals, and coercion, which is exerted by the state and is equivalent to the law.[202] Weber also relies on the notion of law linked to coercion, but through the notion of legitimacy: The particularity of the state's coercion is not coercion, but legitimacy.

B. From sociological to legal legitimacy

101. The question of the monopoly. At first glance, the most important part of the monopoly of legitimate coercion is the word "monopoly." In that sense, the objective of the state would be to remain the one and only entity to exercise coercion. Sovereignty, through the monopoly of coercion, is then closely linked to a process of peacemaking.[203] Such a perspective referred to Bodin's historical context.[204] However,

---

[196] M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 40
[197] Conseil d'État (ed.), *Droit comparé et territorialité du droit*, *op. cit.* note 6, p. 219, 11th conference, intervention of Denys de Béchillon
[198] Even Weber acknowledged it: "*Violence is, of course, not the normal or the only means available to the state*," M. Weber, *The vocation lectures*, *op. cit.* note 179, p. 33
[199] J.A. Agnew, *Globalization and sovereignty*, *op. cit.* note 12, p. 147
[200] M. Delmas-Marty, *Le flou du droit: du code pénal aux droits de l'homme*, Presses universitaires de France, Les Voies du droit, 1st ed., 1986, p. 132. On a broad understanding of the law from coercion to incitement, see P.-E. Berthier, "Les incitations légales," *Semaine sociale Lamy*, June 8, 2015, no. 1680 supplément, p. 36
[201] C. Colliot-Thélène, "Violence et contrainte," *Lignes*, Éditions Hazan, 1995, vol. n° 25, no. 2, p. 264
[202] *Ibid.* pp. 269-270. Coercion as law can be divided into three categories: "*Its agents sometimes subject individuals to noncommunicative direct coercion (coercive acts); its laws subject individuals to noncommunicative legal coercion (in authorizing coercive acts); and its laws subject individuals to communicative legal coercion (in threatening punitive harms)*," A. Abizadeh, "Democratic Legitimacy and State Coercion: A Reply to David Miller," *Political Theory*, 2010, vol. 38, no. 1, p. 123
[203] M. Massé, "La souveraineté pénale," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 1999, p. 905
[204] See *supra* 46.

it is a simplistic perspective. When a state employs coercion, it is done sometimes to repress or to prevent the violence of other entities, either foreign states or its own population.[205] There is no monopoly on coercion; even states cannot be deemed to be failing because other entities exercise coercion or because they allow coercion from other entities.[206] When questioning who is sovereign, the point is not to determine whether someone is monopolizing coercion but to understand who can exercise it.[207] Weber considers that states are effectively sovereigns because their coercion is legitimate while non-state coercion is not.[208]

102. Weber's theory. According to Weber, there are three grounds to organize[209] and, therefore, to legitimize coercion.[210] First, traditional legitimacy is based on "*custom, sanctified by a validity that extends back into the mists of time and is perpetuated by habit*."[211] Second, there is the charismatic legitimacy which rests on "*the authority of the extraordinary, personal gift of grace or charisma, that is, the wholly personal devotion to, and a personal trust in, the revelations, heroism, or other leadership qualities of an individual*."[212] Finally, legal legitimacy relies on "*belief in the validity of legal statutes and practical 'competence' based on rational rules […] based on a person's willingness to carry out statutory duties obediently*."[213] It is that final legitimacy that retains the interest of legal thinkers, particulaly Kelsen.

103. Kelsen's theory. Kelsen equates a state with its legal order and the monopoly of coercion. The word "legitimacy" is not explicit because it is included within the word "monopoly." Kelsen's theory of legitimacy is the legal translation, through the principle of legality, of the sociological legal legitimacy of Weber.[214] The state's legal order monopolizes coercion in the sense that it creates a framework to legally legitimize

---

[205] M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 40
[206] M. Eabrasu, "Les états de la définition wébérienne de l'État," *op. cit.* note 179, p. 198
[207] *Ibid.* p. 200
[208] *Ibid.* p. 202
[209] For Troper, violence "*becomes legitimate precisely when it is organized. It can then be called "coercion"*," M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 37
[210] Weber himself underlines that it is just a theory of legitimacy, and that in practice, acceptance of the coercion of one entity is more "*the product of interests of the most varied kinds, but chiefly of hope and fear*," M. Weber, *The vocation lectures*, *op. cit.* note 179, p. 34
[211] *Ibid.*. Weber gives the examples of patriarchs and patrimonial rulers.
[212] *Ibid.*, Weber gives the examples of "*prophets or - in the political sphere - the elected warlord or the ruler chosen by popular vote, the great demagogue, and the leaders of political parties*."
[213] *Ibid.*, Weber gives the examples of "*the modern "servant of the state" and all those agents of power who resemble him in this respect*."
[214] A sociological legitimacy would describe "*the adherence and loyalty of certain individuals to an organization*," and a normative legitimacy, to provide "*reasons why an organization would be legitimate*," M. Eabrasu, "Les états de la définition wébérienne de l'État," *op. cit.* note 179, p. 206

norms.[215] As a characteristic of the state, sovereignty means to be, "*the unique source of law and the only one entitled to use the means of coercion*."[216] A state's legitimacy comes from legal coercion through the creation of rules (coercion in its large sense) and from the possibility to exercise material coercion if needed (coercion in its restrictive sense) within the framework of the law.[217] To summarize, from Weber to Kelsen, "*The state is that political form which acts in the legal form*."[218]

104. Legitimacy and the rule of law. From this definition was created the concept of the "rule of law."[219] Through the restrictive sense of coercion, the principle of the rule of law means that the "*state's deployment of physical force and its threats of punitive harms against persons are legitimate only if carried out according to public, general, impartially applied, standing laws*."[220] Chevallier adds a practical definition to this formal one. Laws will be applied only through jurisdictional control and, if needed, sanctions. Therefore, he considers that the rule of law implies the "*development of a legal democracy in which the judge appears as the keystone*."[221] However, the rule of law relies not only on the formal creation of law and its material application but also on specific values.[222] It is a standard based on fundamental rights, democratic

[215] M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 36. Such theory is well spread among legal practitioners and thinkers. Even when theorizing legal pluralism, Merry considers that "*It is essential to see state law as fundamentally different in that it exercises the coercive power of the state and monopolizes the symbolic power associated with state authority. But, in many ways, it ideologically shapes other normative orders as well as provides an inescapable framework for their practice*," S.E. Merry, "Legal Pluralism," *Law & Society Review*, 1988, vol. 22, no. 5, p. 879

[216] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, p. 12

[217] *Ibid.* pp. 22-23

[218] M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 43. See also, on the link between internal sovereignty and the place of the law, see *infra* 325.

[219] Which is then a "*pleosnam to Kelsen*," since he did not consider norms outside the state as law, M. Delmas-Marty, *Le relatif et l'universel*, *op. cit.* note 22, p. 32. For a global definition of the rule of law: The "*expression, translated from the German Rechts-staat, used to characterize a state in which all political and administrative authorities, central and local, act in effective conformity with the laws in force and in which all individuals benefit equally from public liberties and procedural and jurisdictional guarantees*," S. Guinchard et al., *Lexique des termes juridiques*, *op. cit.* note 10, p. 453

[220] A. Abizadeh, "Democratic Legitimacy and State Coercion," *op. cit.* note 202, p. 121

[221] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 5, p. 232. Delmas-Marty criticizes this procedural conception of the rule of law, highlighting that the English concept and the French concept (Etat de droit) do not bear the exact same signification, M. Delmas-Marty, *Le pluralisme ordonné*, Éditions du Seuil, Les forces imaginantes du droit no. 2, 2004, p. 78

[222] This evolution of the concept of the rule of law, from formal standards to axiological ones including democracy and fundamental rights, is well developed in J. Chevallier, *L'État de droit*, LGDJ, Clefs, 6th ed., 2017. The author highly criticizes the formal perspective, which is self-legitimizing. By considering axiological and standards norms to define the rule of law, it allows for a more dynamic perspective (in particular thanks to the constant evolution of supranational and national case law). In that sense, it equates with external legitimacy, which is "*compliance with extra-systemic standards or values*," in opposition to internal legitimacy (legitimation by applying the rules set by the system), M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 193, p. 38; J. Chevallier, *L'État de droit*, pp. 41-44. Those values can be attached to the global system, or to each decision taken by the system. In his

legitimacy,[223] and judicial guarantees.[224] However, this concept is then linked to a specific type of government and a specific conception of law within Occidental cultures. To Delmas-Marty, it is not possible to apply such standards globally.[225] Legitimacy, like the state's material elements, is also variable.

105. No definition of sovereignty is absolute; it is a variable concept, with multiple components, including legitimate coercion. However, the latter concept offers an appropriate frame for a legal analysis, particularly for the fight against human trafficking, through the acme of internal legitimate coercion—criminal law—which is meant to prevent conflicts and criminality.

C. Criminal law as the acme of coercion

106. Right to punish. Criminal law, as the main exercise of the extreme form of the state's legitimate violence, rests on two objectives: a right to punish and a duty to protect. Its first objective is to punish offenders. In that sense, some authors rely on the right to punish as the acme of sovereignty.[226] This perspective was explicitly recognized in 1882 by the French *Cour de Cassation:*[227] "*The right to punish emanates from the right of sovereignty*."[228] As "*an overriding principle*,"[229] criminal sovereignty is legitimized "*by the continued use of violence by individuals or groups not authorized*

thesis, Barraud relies on such values as democracy and fundamental rights, linked to the rule of law, but also on structural criteria, like the binding force of the norms, and the level of legal security they create through their accessibility and durability, B. Barraud, *Le renouvellement des sources du droit - Illustrations en droit de la communication par internet*, Thesis, Université d'Aix Marseille, July 1, 2016

[223] Although, Codron ends up considering that democracy may no longer be one of the principles of the rule of law, replaced by the "*fluctuating interests of the Nation*," through consumption and production, due to the development of capitalist and liberal states, C. Codron, *La surveillance diffuse*, *op. cit.* note 180, ¶¶ 595-598

[224] M. Delmas-Marty, *La refondation des pouvoirs*, Éditions du Seuil, Les forces imaginantes du droit no. 3, 2007, pp. 104-105. Barraud lists "*democracy, legal security, equality before the law, the existence of mechanisms to ensure that the authorities comply with the rules in force, transparency, separation of powers, functions and authorities, independence of judges*," B. Barraud, *Le renouvellement des sources du droit*, *op. cit.* note 222, p. 226

[225] M. Delmas-Marty, *La refondation des pouvoirs*, *op. cit.* note 224, p. 106

[226] M. Delmas-Marty, *Le pluralisme ordonné*, *op. cit.* note 221, p. 123

[227] O. Cahn, "Les interactions normatives entre les régimes de common law et de droit romano-germanique," *in* Société française pour le droit international, M. Ubéda-Saillard (eds.), *La souveraineté pénale de l'État au XXI*ème *siècle*, Éditions Pedone, 2018, p. 79; M. Massé, "La souveraineté pénale," *op. cit.* note 203, p. 905

[228] P. Beauvais, "Les mutations de la souveraineté pénale," *in* Collectif (ed.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 72

[229] L. de Carbonnières, "Le droit pénal, expression de l'autorité du souverain : *imperium* ou *jurisdictio*," *in* Société française pour le droit international, M. Ubéda-Saillard (eds.), *La souveraineté pénale de l'État au XXI*ème *siècle*, Éditions Pedone, 2018, p. 47

by the state,"[230] to maintain a peaceful public order. In achieving that goal, it is the only legal discipline in which sanctions will restrain fundamental rights through the privation of life or death or, today in European countries,[231] of liberty through imprisonment.

107. Right to investigate. However, punishing offenders is an ideal outcome for criminal law. Considering criminal sovereignty as a mere right to punish is restrictive and does not take into account the entire criminal process. On the one hand, criminal law determines a state's jurisdiction to start a criminal investigation. In that sense, legitimate coercion is linked to and defines the material component of the territory.[232] The principle of territoriality in criminal law determines in the first place the crimes that the state can prosecute.[233] On the other hand, coercion is applied not only after conviction through criminal sanctions but also is used at every stage of the prosecution process, when realizing acts of investigation against the consent of people or without their knowledge. In that perspective, sovereignty and coercion, in a large sense, are extended "*to all acts of investigation, including those that do not infringe any fundamental right*."[234] Therefore, the sovereign state establishes not only its own powers of coercion to prosecute and punish offenders but also its material and territorial limits.[235]

108. Duty to protect. However, understanding criminal law only through that lens is like considering only one side of the coin. As already mentioned, sovereignty is based primarily on population, which the state has the obligation to protect.[236] Most laws are meant to protect persons, either through their physical and mental integrity or through their properties.[237] In Europe, offenses are no longer seen primarily as an

[230] C. Colliot-Thélène, "La fin du monopole de la violence légitime ?," *op. cit.* note 178, p. 7
[231] Article 2.1 of the CPHR provides an exception to allow the death penalty. However, its 6th Protocol (1983) abolished the death penalty (Article 1), with an exception in times of war (Article 2). Both conventions have been ratified by 46 countries (the CPHR has also been ratified by the EU). The 13th Protocol (2002) suppresses the exception in times of war (Article 2). It has been ratified by 44 countries (Azerbaijan and Russia did not ratify this protocol).
[232] H. Donnedieu de Vabres, *Les principes modernes du droit pénal international*, Editions Panthéon-Assas, 2005, pp. 3-7
[233] H. Ruiz Fabri, "Immatériel, territorialité et État," *op. cit.* note 3, p. 194; see *infra* Part 1. Title 1. Chapter 2. Section 1. .
[234] M. Lasalle, "Souverainetés et responsabilités dans la collecte internationale de preuves - L'exemple de l'accès aux données bancaires en matière pénale," *in* Société française pour le droit international, M. Ubéda-Saillard (eds.), *La souveraineté pénale de l'État au XXIème siècle*, Éditions Pedone, 2018, p. 277
[235] P. Beauvais, "Les mutations de la souveraineté pénale," *op. cit.* note 228, p. 73
[236] See *supra* 61 and followings.
[237] In Spain, the study of criminal law usually relies on the values protected by the offenses, most of them relying on fundamental rights.

attack on the state but as an attack on the individual; in fact, additional rights have been given to victims over time.[238] The victims are taken into consideration not only for their protection during the process, but also as part of it:, to start an investigation, to interact during the stages of the criminal process, and to ask for reparation at its end.[239]

109. The monopoly of legitimate coercion can be interpreted in a restrictive way, meaning the exercise of physical violence. However, due to the wide variety of means in the hands of the state to control its territory, its population, and its government as well as to make use of its sovereignty, "coercion" should be understood as a broader concept. As the digital world expands, the state can develop a new way to exercise coercion: digital legitimate coercion.

II. Defining digital legitimate coercion

110. Avoiding technological solutionism. As a preliminary remark, it must be underlined that digital legitimate coercion will not replace classical means of coercion. Digital legitimate coercion is an additional layer of coercion,[240] in the same way that digital sovereignty is a new layer of sovereignty, creating new challenges, but not erasing the primary questions around the classical concept of sovereignty. In that sense, "*technology solutionism*"[241] should be avoided as well as "*fetishizing tech*."[242] First, avoiding this solutionism supposes to escape "Internet-centrism," as the core of

[238] See for example, S. Tadrous, *La place de la victime dans le procès pénal*, Thesis, Université Montpellier I, December 1, 2014; G. Beaussonie, "L'installation de la victime dans le procès pénal," *Actualité juridique Pénal*, Dalloz, 2015, p. 526. These evolutions are linked to the extension of human rights through the interpretation of the right to a due process by the ECHR, and by the EU legal framework, in particular the directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime. It is particularly interesting to see the evolution of the victim's place within time. Those recent changes seem to make the process look more like inquisitor processes back in the Middle Ages, J.-A. Wemmers, K. Cyr, "Gender and Victims' Expectations Regarding Their Role in the Criminal Justice System: Towards Victim-Centred Prosecutorial Policies," *in* H. Kury, S. Redo, E. Shea (eds.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, p. 235

[239] On the contrary, in the US, the victims should file a civil suit to ask for reparation.

[240] To compare, digital legitimate coercion can be abbreviated as "DLC." DLC also means "downloadable content," which is an additional part of a main videogame: it does not replace the basic software but adds more content, usually additional gameplay.

[241] E. Morozov, *To save everything, click here: the folly of technological solutionism*, PublicAffairs, 1st ed., 2013

[242] M. Broussard, *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018, p. 194. To make a parallel with the distinction between vanilla and kinky sexuality or fetishes, classical means to solve problems are needed, from "vanilla" solutions, paper-based or human-based, to "hard" solutions relying on all-technological tools. There is a wide spectrum of analysis between those two extremes. It is quite surprising to advocate for such diversity in the tech sector when a wide part of the spectrum of sexuality is still stigmatized, especially "non-conventional" practices.

all contemporary problems but also solutions, and "*to learn how to engage in narrow, empirically grounded arguments about the individual technologies and platforms that compose 'the Internet.'*"[243] The Internet is a diverse movement with multiple components. Second, as an additional layer of sovereignty, problems derived from the Internet and new technologies can be solved by non-digital means of coercion. This understanding is important when fighting against human trafficking. The relationships of this phenomenon with new technologies are a trendy topic. Technologies add new opportunities, but do not erase the classical *modus operandi* of both traffickers and those stopping the traffic. Recruitment continues to take place through physical human-to-human interactions, exploitation does not always need the Internet, and money laundering still relies mainly on cash. From the state's perspective, "*Human trafficking as a technological challenge […] does not offer a holistic approach*."[244] All of the elements dedicated to fight against cyber trafficking presented in this thesis are not enough to repress human trafficking in general. The state must rely on a wide variety of techniques to prosecute traffickers and to protect their victims.[245]

111. Digital versus virtual. Digital coercion is not virtual. According to the Cambridge Dictionary, "virtual" means "*not existing in the physical world*" or "*not involving people physically*." By contrast, "digital" implies "*using or relating to digital signals and computer technology*." Violence and coercion exercised through a digital means are not virtual. Consider the consequences of cyberstalking, cyber harassment, and cyber trafficking: The physical and mental effects of these crimes are tangible for victims and the money earned from the victims' exploitation is real. Investigating through the Internet to identify victims and offer them physical protection or to imprison traffickers are real consequences. Accordingly, if such illegitimate coercion is real and has impacts on the physical layer of the world, then the digital legitimate coercion of the state is real as well. Because this coercion is digital, not virtual, it allows the state to control information, people, and the economy and, therefore, to exercise its sovereignty.

112. Strict digital coercion. What is digital legitimate coercion? This concept is

[243] E. Morozov, *To save everything, click here*, *op. cit.* note 241, p. 68
[244] I. Chen, C. Tortosa, "The Use of Digital Evidence in Human Trafficking Investigations," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 124
[245] In that sense, see M. Graw Leary, "Fighting Fire with Fire: Technology in Child Sex Trafficking," *Duke Journal of Gender Law & Policy*, 2014, vol. 21, p. 318; S. Milivojević, H. Moore, M. Segrave, "Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology," *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 19-25

understood through a tertiary division. First, there is the restrictive interpretation of digital coercion. It is digital coercion in a digital environment, directly exercised by the state. If the state enters an online account to search for information without the consent of the account holder, the action (coercion) of the state and its main and direct consequences take place digitally.

113. State non-digital coercion *versus* digital behavior. Second, a broader concept of digital coercion implies interaction with non-digital coercion tools. This second approach can be divided into two parts. On the one hand, state-level non-digital coercion can respond to digital behavior. The state can exercise non-digital coercion to trigger a specific behavior in the digital environment. Regulating the conservation of data is not digital; it is a new legal obligation applied to digital intermediaries. In the end, it will change the behavior of these intermediaries regarding data retention, whether for a longer or shorter time. Alternatively, a digital behavior can trigger non-digital coercion from the state. Seizing the phone of a trafficker can prevent them from contacting their victims. In this case, the state is not acting in the digital space, but its action will trigger changes in this space.

114. State digital coercion *versus* non-digital behavior. On the other hand, the state can exercise digital coercion to trigger a behavior in the real world (non-digital behavior). By blocking or controlling information online, the state can prevent people from questioning certain historical facts or political positions; although this is an extreme example, it is done in China. Online campaigns to raise awareness about human trafficking, gender-based violence, or cyber harassment seek to offer the victims an incentive to reach out for help. Likewise, a physical behavior can trigger a digital response from the state. The passage of time can trigger the deletion of data (especially criminal data) processed by the state, and threats to a witness or victim can lead to the use of digital tools such as video conferencing.

115. Consequently, the concept of legitimate coercion evolves to adapt the fight against cyber trafficking. Relying on the concept of (digital) legitimate coercion highlights the central role of the state in the repression of the phenomenon, as it threatens its sovereignty.

§2. Applying digital legitimate coercion to face cyber trafficking

116. To protect the state's material elements, its (digital) legitimate coercion seems

to be an appropriate tool to repress (cyber) human trafficking. The role of the state, through its powers of classical and digital coercion, is highlighted by both the strategies developed to fight against trafficking (I) and its international obligations (II).

I. Digital legitimate coercion in strategies to repress human trafficking

117. Fight against trafficking: main approaches and global strategy. The repression of trafficking rests on two main strategies or approaches. The first is focused on trafficking as a "*criminal justice issue*," focusing on "*intelligence gathering, dismantling criminal groups, and arresting and prosecuting traffickers*."[246] It is the main approach of the international convention on trafficking. The Palermo Protocol focuses on criminal repression measures,[247] border control,[248] and international cooperation

[246] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 152, p. 27. However, it seems that both approaches are conflated by Aronowitz. To reduce a criminal issue such as human trafficking, it is not necessary to call for border control and immigration restrictions.

[247] On the contrary, the text contains only three articles on victims' protection, which, in their wording, do not impose strong obligations, S. Scarpa, "UN Palermo Trafficking Protocol Eighteen Years On: A Critique," *op. cit.* note 122, p. 635; J. Jones, "Is It Time to Open a Conversation About a New United Nations Treaty to Fight Human Trafficking," *op. cit.* note 167, p. 1808. The same limitation was criticized regarding the EU Council Framework Decision of 19 July 2002 on combating trafficking in human beings. It had only one article related to the protection of victims, Article 7. See S.H. Krieg, "Trafficking in Human Beings: The EU Approach between Border Control, Law Enforcement and Human Rights," *European Law Journal*, 2009, vol. 15, no. 6, pp. 775-790; A. Gallagher, *The international law of human trafficking*, *op. cit.* note 130, p. 96

[248] In particular, part of this criminal approach is called a "*border security approach*," J. Todres, "The Private Sector's Pivotal Role in Combating Human Trafficking," *California Law Review Circuit*, 2012, vol. 3, pp. 79-99. Trafficking is seen as a transnational threat that does not respect the conditions established by the state for entering and staying on its territory. Therefore, a way to reduce human trafficking could be to increase border control, as part of a "*security and sovereign model, that involves the control of immigrant populations and leads to a repressive spiral*," M. Delmas-Marty, *Résister, responsabiliser, anticiper*, *op. cit.* note 13, p. 21. However, this border control approach has been criticized because of the insistence on passing measures to globally limit migrations, K. Alden Dinan, "Globalization and national sovereignty," *op. cit.* note 138, p. 67. Berman considers that "*Discourses of sex-trafficking redefine and relocate these assaults on sovereignty within a gendered and racialized frame […] that authorizes the state to reinstate sovereign borders*," J. Berman, "(Un)Popular Strangers and Crises (Un)Bounded," *op. cit.* note 110, p. 63. Indeed, "*The higher the barriers of entry to an attractive target country are, the more complex becomes the methods and morality of human smuggling*," increasing the violence of traffickers and smugglers against victims and making investigations harder as illegal flows tend to use more elaborated processes, R. Väyrynen, *Illegal Immigration, Human Trafficking, and Organized Crime*, *op. cit.* note 153, p. 8. See also, R. Pati, "Human Trafficking: An Issue of Human and National Security," *op. cit.* note 1, p. 28; L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 320. To some authors, this strategy of states and its consequences are not even surprising as they "*allow states to have an official anti-immigrant/anti-human mobility policy, at the same time that their economies' demand for low cost labor is fulfilled*," K.E. Bravo, "Interrogating the State's Role in Human Trafficking," *op. cit.* note 162, p. 28. In this perspective, states benefit from trafficking, W. van Schendel, "Spaces of Engagement How Borderlands, Illegal Flows, and Territorial States Interlock," *in* W. van Schendel, I. Abraham (eds.), *Illicit flows and criminal things: states, borders, and the other side of globalization*, Indiana University Press, Tracking globalization, 2005, p. 60

between states.[249] Consequently, it highlights criminal law as the optimum form of legitimate coercion of the state to repress human trafficking. However, prosecuting traffickers is not the only approach. As a result of criticisms of the criminal approach, voices have been raised to strengthen the repression of trafficking, which is seen as a violation of human rights.[250] Because "*people are the beneficiaries of national security policies*,"[251] "*the state has a duty to redress the wrong*."[252] One of those "wrongs" is human trafficking, which endangers the basic fundamental rights of individuals as victims, as explained earlier.[253] Therefore, the European framework[254] increasingly focuses on protecting the rights of victims.[255] The legitimate coercion of the state then materializes through measures of assistance, and legal rights offered to the victims. This division traditionally considers the role of the state's legitimate coercion to repress trafficking. This binary is to be found and developed in the classical 3P strategy established by the United Nations General Assembly: prevent, protect, and

[249] Articles 10 to 13 of the Palermo Protocol

[250] A. Aronowitz, *Human trafficking, human misery*, *op. cit.* note 152, pp. 27-28. As underlined Shelley, "*What is the purpose of government if not to protect the lives of its citizens?*," L. Shelley, *Human trafficking A global perspective*, *op. cit.* note 35, p. 320

[251] R. Pati, "Human Trafficking: An Issue of Human and National Security," *op. cit.* note 1, p. 28

[252] R. Pati, "States' Positive Obligations with Respect to Human Trafficking: The European Court of Human Rights Breaks New Ground in Rantsev v. Cyprus and Russia," *Boston University International Law Review*, 2011, vol. 29, p. 134

[253] See *supra* 67 and followings.

[254] However, at the national level, it is sometimes still necessary that the victim participate in the criminal process to have access to their rights as a trafficked victim. See for example, Article 425-1 of the Code de l'entrée et du séjour des étrangers et du droit d'asile (France), regarding the emission of a temporary residence permit, which requires the foreigner victim to file a complaint or to testify against the offender. The same criticism is made of the United States legal framework, J.E. Halley et al., "From the International to the Local Feminist Legal Responses to Rape, Prostitution/Sex Work and Sex Trafficking: Four Studies in Contemporary Governance Feminism," *Harvard Women's Law Journal*, 2006, vol. 29, no. 2, p. 389

[255] The first text of the EU on human trafficking only integrated one article on the protection of victims (Article 7 of the Council Framework Decision 2002/629/JHA). Afterwards, two other instruments were passed to create new rights for victims: the directive 2004/81/EC of 29 April 2004 on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration, who cooperate with the competent authorities, and the directive 2009/52/EC of the European Parliament and of the Council of 18 June 2009 providing for minimum standards on sanctions and measures against employers of illegally staying third-country nationals. The directive 2011/36/EU that replaced the framework decision provides eight articles on the protection of victims (Articles 8, 11-17). Nowadays, trafficked victims can also rely on provisions passed due to the directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime. The Warsaw Convention integrates the protection of victims in its Articles 10 to 17.

prosecute.[256] Later, "partnerships"[257] were added to comprise the 4P strategy.[258] The three elements of this strategy have been developed by the literature to include digitally supported actions of the state.

118. Protection. The protection of trafficked victims occurs both within and outside the criminal procedure. Prior to the criminal process, hotlines can support the identification of victims,[259] and some of these hotlines are operated by the state.[260] During the criminal process, once the victims are identified, tools of "digital procedure" can help protect them. Video conferencing is regularly mentioned, allowing victims to avoid contact with their offenders.[261] A tape-recorded interview[262] avoids the need for multiple interviews requiring victims to repeat the descriptions of abuse. New

[256] General Assembly, "Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons," UN, July 30, 2010, A/RES/64/293; reaffirmed by the General Assembly, "Resolution 72/1. Political declaration on the implementation of the United Nations Global Plan of Action to Combat Trafficking in Persons," UN, September 27, 2017, p. 1, A/RES/72/1

[257] See *infra* 245.

[258] To adapt this strategy to the introduction of new technologies, Musto and boyd offer a 4A strategy: "*Awareness and visibility of particular online sites assumed to promote trafficking, […] amassment of data by law enforcement to pursue anti-trafficking investigations, […] augmentation of traditional surveillance techniques and tools, and […] advancement of collaborative arrangements and technological innovation in the form of automated or algorithmic techniques*", J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *Social Politics*, 2014, vol. 21, no. 3, p. 463; see also S. Milivojević, "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, p. 36. Given the various possibilities suggested by the literature to use new technologies when fighting against human trafficking, this approach seems too restrictive.

[259] Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, "Final Report," Committee for Equality between Women and Men, Council of Europe, September 16, 2003, pp. 72-73, EG-S-NT (2002) 9 rev.; A. Sykiotou, "Cyber trafficking: recruiting victims of human trafficking through the net," *in* N.E. Kourakēs, C.D. Spinellis (eds.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017, p. 1573. "*Mobile devices and SMS technologies may also enable survivors of human trafficking to more readily reach out to service providers and seek help*," Department of State, "Trafficking in persons report," US, June 2013, p. 14. The Crimestoppers number was very useful during the operation Pentameter (United Kingdom), UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," Austria Center Vienna, UNODC, UN, February 2008, p. 21

[260] For example, PHAROS in France, Inspection générale des affaires sociales, Inspection générale de l'administration, Inspection générale de la justice, "Evaluation de la loi du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées," France, December 2019, pp. 9, 40-41; or the hotline run by the unit specialized on human trafficking, in collaboration with the computer crime unit, in Belgium, Special Rapporteur on the sale of children, child prostitution and child pornography, "Report on the sale of children, child prostitution and child pornography," Commission on Human Rights, Economic and Social Council, UN, December 23, 2004, p. 17, E/CN.4/2005/78

[261] UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," *op. cit.* note 259, p. 25; K. Guilbert, "Chasing shadows: can technology save the slaves it snared?," *Reuters*, June 21, 2018, online https://www.reuters.com/article/us-technology-trafficking-fight-insight-idUSKBN1JH005 (retrieved on March 18, 2021); Department of State, "Trafficking in persons report," US, June 2021, p. 23. The latter document underlines the importance of this tool during the COVID pandemic.

[262] European Institute for Gender Equality, "Gender-specific measures in anti-trafficking actions Report," EU, 2018, p. 54

technologies can also help to reduce language barriers, for example, by facilitating access to an interpreter,[263] providing the victim with classes,[264] or facilitating access to mental health assistance.[265] The protection of the victim can also rely on the restriction of the movement of the trafficker by means other than imprisonment, such as mechanisms of surveillance relying on new technologies,[266] such as an electronic bracelet. Finally, the victims could more easily receive compensation if the process was completed online, even after their repatriation.

119. Prosecution. Prosecuting offenders usually implies the identification of victims. For law enforcement authorities, cyber trafficking offers new sources of evidence and the means to identify victims. Monitoring the Internet is mentioned regularly.[267] Such monitoring can rely not only on human means but also on technological tools, such as facial recognition technology[268] and, more generally, artificial intelligence.[269] These tools are particularly useful for data mining[270] and for quickly highlighting patterns or "red flags" of human trafficking.[271] Identification of

[263] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020, p. 44; Spotlight Initiative, "Mobile women and mobile phones Women migrant workers' use of information and communication technologies in ASEAN," EU, ILO, 2019, pp. 40-41

[264] European Union Agency For Fundamental Rights, "Protecting migrant workers from exploitation in the EU: workers' perspectives," EU, 2019, p. 21

[265] A.A. Vujanovic et al., "Applying Telemental Health Services for Adults Experiencing Trafficking," *Public Health Rep*, SAGE Publications Inc, July 1, 2022, vol. 137, no. 1_suppl, pp. 17S-22S

[266] d. boyd et al., *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the US*, Microsoft Research Connections, December 2011, p. 9

[267] A. Sykiotou, *Trafficking in human beings: Internet recruitment - Misuse of the Internet for the recruitment of victims of trafficking in human beings*, Council of Europe, 2007, p. 99; J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *op. cit.* note 258, p. 467; M. Graw Leary, "Fighting Fire with Fire," *op. cit.* note 245, p. 314; E. Heil, A. Nichols, "Hot spot trafficking: a theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States," *Contemporary Justice Review*, Routledge, October 2, 2014, vol. 17, no. 4, p. 423

[268] Inter-agency coordination group against trafficking in persons, *Human trafficking and technology: trends, challenges and opportunities*, Issue Brief, no. 7, UN, 2019, p. 4; S. Raets, J. Janssens, "Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business," *European Journal on Criminal Policy and Research*, October 26, 2019, p. 14. Although such kind of technology is mainly mentioned when considering child pornography. See for example, the Stop Child Abuse – Trace an Object campaign launched by Europol, Europol, "Internet organised crime threat assessment," EU, 2018, p. 31

[269] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 263, p. 44. On those artificial intelligence tools, see *infra* Part 2. Title 1. Chapter 2. Section 2. .

[270] J. Anil Kumar, "The impact of human trafficking in ASEAN: Singapore as a case-study," *Asian Journal of International Law*, Research Collection School Of Law, 2018, vol. 8, no. 1, p. 223; UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, UN, May 2015, p. 47

[271] R. Konrad, A. Trapp, T. Palmbach, "Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications," *European Journal of Operational*

victims can also be done through other technologies, such as satellite images to locate areas of exploitation,[272] or drones to "*track illegal cannabis farms*."[273] The law provides law enforcement authorities with a wide range of investigation investigatory techniques linked to new technologies: geotagging, interception of communications,[274] digital forensics,[275] or entrapment.[276] When traffickers rely on digital financial solutions, it allows law enforcement authorities to deepen a financial investigation.[277] Finally, new technologies improve cooperation and foster the creation of mutual tools like such as databases, including Europol's Analytical Work File Phoenix database dedicated to human trafficking.[278] Each of these techniques allows the procurement of additional evidence that allows prosecutors to avoid relying exclusively or almost exclusively on the victims' testimonies.[279]

120. Prevention. Finally, technologies foster "*prevention or education initiatives*."[280]

Research, June 1, 2017, vol. 259, no. 2, p. 2; J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1704; A. Beduschi, "The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law," *Georgetown Journal of International Law*, 2018, vol. 49, no. 3, p. 1008. To some authors, such tools are meant to prevent human trafficking, see for example, G.A. Sarfaty, "Can Big Data Revolutionize International Human Rights Law," *University of Pennsylvania Journal of International Law*, 2017, vol. 39, no. 1, p. 85. However, when considering the advertisement of victims, the exploitation is usually already taking place. However, the definition of trafficking does not require an accumulation of acts and can be characterized since the recruitment.

[272] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 263, p. 10

[273] F. Gerry QC, J. Muraszkiewicz, N. Vavoula, "The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns," *Computer Law & Security Review*, April 2016, vol. 32, no. 2, p. 214

[274] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *op. cit.* note 258, p. 469

[275] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, *op. cit.* note 270, p. 46

[276] F. Kurz, "Prosecution of trafficking in human beings in civil law systems The example of Belgium," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 231

[277] Special Rapporteur on contemporary forms of slavery, including its causes and consequences, "Current and emerging forms of slavery - Report," Human Rights Council, General Assembly, UN, July 25, 2019, ¶ 59, A/HRC/42/44; H. Watson, A. Donovan, "Role of technology in human trafficking," *TRACE*, October 2015, p. 9; Inspection générale des affaires sociales, Inspection générale de l'administration, Inspection générale de la justice, *Evaluation de la loi du 13 avril 2016*, *op. cit.* note 260, p. 39;

[278] J.-M. Souvira, "La traite des êtres humains et l'exploitation sexuelle," *Cahiers de la sécurité et de la justice*, INHESJ, September 2009, no. 9, p. 112

[279] I. Chen, C. Tortosa, "The Use of Digital Evidence in Human Trafficking Investigations," *op. cit.* note 244, p. 123; J. Musto, "The Limits and Possibilities of Data-Driven Anti-trafficking Efforts," *Georgia State University Law Review*, May 1, 2020, vol. 36, no. 4, p. 1158

[280] d. boyd et al., *Human Trafficking and Technology*, *op. cit.* note 266, p. 4; S. Yu, "Human Trafficking and the Internet," *in* M. Palmiotto (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 70

Awareness-raising campaigns[281] can benefit from the Internet, reaching a wider audience[282], and focusing on human trafficking or on the dangers of the Internet, especially for young people.[283] For example, since cyber trafficking runs through intermediaries,[284] raising awareness or regulating these sectors is also an option. Information websites on working and migration regulation can raise awareness among potential victims, making them less vulnerable.[285] Regarding migration, new technologies offer additional ways of creating better secured identity documents[286] and verification machines.[287] New technologies also offer tools to create remote training, accessible to a wider audience of professionals who work with trafficked victims.[288]. In general, obtaining more information on human trafficking through new technology helps combat the crime thanks to better knowledge and intelligence.[289]

121. Each approach to fighting against human trafficking has been developed to

[281] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 263, p. 8; A. Sykiotou, "Cyber trafficking," *op. cit.* note 259, p. 1571; C. Bouchoux et al., *Rapport d'information sur les femmes et les mineur-e-s victimes de la traite des êtres humains*, no. 448, Sénat, France, March 9, 2016, p. 66

[282] Europol, "Intelligence Notification 15/2014 Trafficking in human beings and the internet," EU, October 2014, p. 2; T. Guberek, R. Silva, *"Human Rights and Technology": Mapping the Landscape to Support Grantmaking*, PRIMA, Ford Foundation, August 2014, p. 21

[283] D. Dushi, "Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo," *International Review of Law, Computers & Technology*, January 2, 2018, vol. 32, no. 1, p. 96

[284] For example, marriage agencies, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *Final Report*, *op. cit.* note 259, p. 56; Committee of ministers, "Recommendation no. R (91)11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults," Council of Europe, September 9, 1991, p. 3; adoption agencies, *Ibid.* p. 3; or recruitment agencies, M. Latonero et al., *Technology and Labor Trafficking in a Network Society - General Overview, Emerging Innovations, and Philippines Case Study*, USC Annenberg - USC University of Southern California, February 2015, p. 23

[285] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 263, p. 8

[286] M. Chawki, *La traite des êtres humains à l'ère numérique*, Éditions de Saint-Amans, 2010, p. 295; Global programme against trafficking in human beings, "Toolkit to Combat Trafficking in Persons," UNODC, UN, 2008, p. 201

[287] UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," *op. cit.* note 259, p. 18. Blockchain is also mentioned to facilitate the process of migration and make it more secure, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 263, p. 44; K. Guilbert, "Chasing shadows," *op. cit.* note 261

[288] Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *Final Report*, *op. cit.* note 259, pp. 66, 72, 83; D.M. Hughes, "Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies," *SAGE Open*, December 18, 2014, vol. 4, no. 4, p. 4

[289] F. Gerry QC, J. Muraszkiewicz, N. Vavoula, "The role of technology in the fight against human trafficking," *op. cit.* note 273, p. 213; G. Rankin, N. Kinsella, "Human Trafficking – The Importance of

share best practices and to spread ideas for how an extension of the digital legitimate coercion of states could enhance the repression of cyber trafficking. Therefore, the state remains at the center of the evolution of strategies. Furthermore, the need to exercise such digital coercion by the state is increasingly recognized by the legal framework.

II. Digital legitimate coercion in the state's international obligations

122. Supranational texts. First, states are the unique holders of obligations under supranational instruments regarding trafficking. The articles of the three major instruments to combat against trafficking[290] rely on obligations directly meant for states and their legitimate coercion. This is obvious considering the structure of international public law.[291] However, treaties have not included many references to the use of new technologies to repress human trafficking.[292] Generally, they mention "measures," which are technologically neutral and allow the state to adapt its tools to respond to the evolution of the traffic.[293] As attention regarding the links between human trafficking and new technologies rose in the 2000s,[294] it was not surprising that the Palermo conventions may have made no or few references to the latter.[295] Nevertheless, this situation led to more questioning within the Council of Europe framework, since it commissioned studies on those links before the adoption of the Warsaw Convention.[296]

Knowledge Information Exchange," *in* B. Akhgar, S. Yates (eds.), *Intelligence Management*, Springer London, Advanced Information and Knowledge Processing, 2011, p. 172

[290] The Palermo Protocol, the Warsaw Convention and the Directive 2011/36/EU. It is explicitly clear the latter since the first paragraph of its preamble highlights the central role of the Union and member states.

[291] On the links between sovereignty and international relations, see *infra* Part 1. Title 2. Chapter 2. .

[292] For instance, the EU 2011 directive also underlines the use of communication technologies for interviews, to protect the victims, Articles 10.3.b and 15.5.b. Its preamble (Paragraph 15) highlights the need to have "*access to the investigative tools used in organized crime or other serious crime cases. Such tools could include the interception of communications, covert surveillance including electronic surveillance, the monitoring of bank accounts and other financial investigations*."

[293] For example, in the Palermo protocol: "*other measures*" for prevention (Article 9), "*other appropriate measures*" for border control (Article 11), or "*available means*" for control of documents (Article 12). Similarly, the Warsaw Convention is very general in its provisions.

[294] For a historical list of references to such links in international organizations, see *infra* 268 to 270.

[295] The Palermo Convention mentions video conferencing for testimonies as a means to protect witnesses, Article 24.2.b, for developing law enforcement authorities' cooperation, Article 27.3, for technical assistance, Article 29.1.h, and the use of "*special investigative techniques, such as electronic or other forms of surveillance and undercover operations*," Article 20.1.

[296] D. Hughes, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation. Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation*, Committee for Equality between Women and Men, Council of Europe, November 2001; D. Hughes, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *The Impact of the Use of New Communications and*

It should be mentioned that the proposal to amend the Directive 2011/36/EU emphasizes that online trafficking processes should be equally prosecuted and convicted,[297] but the proposal does not modify the definition of the offense nor provide for measures to address the specific challenges of prosecuting cyber trafficking.

123. Case law: positive obligations. Second, the case law of the ECHR also considers the state as the first actor meant to repress trafficking.[298] The ECHR extended the CPHR to this phenomenon through its Article 4[299] in the Rantsev case.[300] In the Siliadin case, the ECHR first extended this article to include positive obligations for states "*to adopt criminal-law provisions which penalize the practices referred to in Article 4 and to apply them in practice*."[301] Then, the Rantsev case clarified the scope of states' positive obligations regarding trafficking in particular. These obligations are not limited to the criminalization of the phenomenon, but also include "*measures to prevent trafficking and to protect victims*."[302] Those positive obligations are divided into three parts: putting in place an appropriate legal and regulatory framework, adopting operational measures for both protection and criminalization, and checking that those

Information Technologies on Trafficking in Human Beings for Sexual Exploitation A Study of the Users, Committee for Equality between Women and Men, Council of Europe, May 2001; Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *Final Report*, *op. cit.* note 259

[297] Article 1.2, European Commission, Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, December 19, 2022, COM(2022) 732 final

[298] For a review of the ECHR cases regarding human trafficking, see V. Stoyanova, "European Court of Human Rights and the Right Not to Be Subjected to Slavery, Servitude, Forced Labor, and Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1393-1407; R. Pati, "States' Positive Obligations with Respect to Human Trafficking," *op. cit.* note 252, pp. 79-142

[299] It prohibits the use of slavery, servitude, forced, or compulsory labor.

[300] ECHR, *Rantsev*, *op. cit.* note 46, ¶ 282, reaffirmed in ECHR, *M. and Others v. Italy and Bulgaria*, July 31, 2012, no. 40020/03; ECHR, *L.E. v. Greece*, January 21, 2016, no. 71545/12

[301] ECHR, *Siliadin*, *op. cit.* note 45, ¶ 89. Positive obligations deriving from an article redacted in a negative way have already been recognized for Articles 3 and 8, in a rape case: "*The Court considers that States have a positive obligation […] to enact criminal-law provisions effectively punishing rape and to apply them in practice through effective investigation and prosecution*," ECHR, *M.C. v. Bulgary*, December 4, 2003, no. 39272/98, ¶ 153

[302] ECHR, *Rantsev*, *op. cit.* note 46, ¶ 285; reaffirmed in ECHR, *Zoletic*, *op. cit.* note 71, ¶ 180. Those positive obligations regarding victims' protection should be independent from the criminal process, since, "*(Potential) victims need support even before the offense of human trafficking is formally established*," ECHR, *J. and others v. Austria*, January 17, 2017, no. 58216/12, ¶ 115. Recently, the ECHR found that when a state prosecutes a potential or identified victim of human trafficking, it does not fulfill its positive obligation to adopt operational measures to protect victims of trafficking, ECHR, *V.C.L. and A.N. v. the United Kingdom*, February 16, 2021, 77587/12 and 74603/12. However, the court limits the scope of those positive obligations, which will not exist generally in an abstract way, but only when "*The State authorities were aware, or ought to have been aware, of circumstances giving rise to a credible suspicion that an identified individual had been, or was at real and immediate risk of being, trafficked or exploited*," ECHR, *Rantsev*, *op. cit.* note 46, ¶ 286. Such limitation avoids imposing "*an impossible or disproportionate burden on the authorities*," *Ibid.* ¶ 287

measures are effective.[303]

124. Case law: digital obligations. The ECHR developed states' positive obligations to investigate human trafficking to include a digital investigation, in the case of S.M. v. Croatia.[304] *Via* Facebook, a man contacted and befriended a woman who was looking for a job, then quickly forced her to provide sexual services, through psychological pressure and physical violence.[305] When the woman succeeded in leaving and filing a criminal complaint, an investigation was opened for procuring prostitution and rape.[306] However, the court acquitted the man, on the grounds that those services were not forced, as the prosecutors could not prove coercion.[307] As a result, the woman filed a complaint with the ECHR, alleging that "*the domestic authorities had failed effectively to apply the relevant criminal-law mechanisms concerning her allegations of human trafficking*."[308] Indeed, the court considers that "*there was* prima facie *evidence that she had been subjected to treatment contrary to Article 4 of the Convention*."[309] The court underlines various failures in the investigatory process, rendering it ineffective and triggering a violation of Article 4.[310] In particular, "*The prosecuting authorities never sought to inspect the applicant's or T.M.'s Facebook accounts and, thus, to ascertain the nature of their first contact and further exchanges*."[311] Consequently, when investigating trafficking, the state has an obligation to search for digital evidence. Although it is an obligation of means and not of results,[312] the ECHR creates a new standard to make ensure that the coercion applied by the state to repress human trafficking evolves with the crime.

125. National framework. Finally, the French national framework provides

---

[303] ECHR, *L.E. v. Greece*, *op. cit.* note 300, ¶¶ 70-85; ECHR, *Chowdury*, *op. cit.* note 71, ¶¶ 105-127. As the court underlined, "*The first two aspects of the positive obligations can be denoted as substantive, whereas the third aspect designates the States' (positive) procedural obligation*," ECHR, *V.C.L. and A.N. v. the United Kingdom*, *op. cit.* note 302, ¶ 156. Reaffirmed in ECHR, *S.M. v. Croatia*, June 25, 2020, no. 60561/14, ¶ 306; ECHR, *Zoletic*, *op. cit.* note 71, ¶ 182

[304] ECHR, *S.M. v. Croatia*, *op. cit.* note 303

[305] Those services were advertised online. When she managed to leave him, he contacted her again through Facebook with threats against her family. The woman also limited her exploitation by deactivating the advertisement when her exploiter was not around, *Ibid.* ¶¶ 11-17. She also learned that she was not the only "girlfriend" of this man in this situation and that the others were suffering also revenge porn from him, *Ibid.* ¶ 31

[306] ECHR, *S.M. v. Croatia*, *op. cit.* note 303, ¶¶ 18-20

[307] *Ibid.* ¶ 78

[308] *Ibid.* ¶ 240

[309] *Ibid.* ¶ 332

[310] *Ibid.* ¶¶ 343-347

[311] *Ibid.* ¶ 337

[312] *Ibid.* ¶ 315

examples of how to consider the cyber evolution of trafficking or exploitation offenses in its criminal code.[313] The sanction for trafficking is increased "*when the person has been put in contact with the perpetrator through the use of an electronic communication network for the dissemination of messages to a non-specific public*."[314] However, this aggravating circumstance is limited to the first part of the trafficking process, the recruitment, through a message sent to a wide public, excluding the possibility of direct private messaging. It should be highlighted that the code considers a similar aggravating circumstance for pimping, one of the exploitation offenses of trafficking.[315] On the contrary, offenses[316] criminalizing other types of exploitation do not consider the cyber components of trafficking. Differently, the Spanish project for a comprehensive law against human trafficking considers cyber trafficking by focusing on preventing the online recruitment of victims, on cooperation with digital actors and on the deletion of online content.[317]

126. Conclusion of the section. An abstract way to define sovereignty is to rely on the concept of the monopoly of the legitimate use of physical violence. This theory ends up extending to the use of legitimate coercion, especially through the state's legal

[313] Regarding the general criminal systems, it can be highlighted that, in 2001, before the creation of the human trafficking offense, a circular on procuring prostitution already mentioned the use of video conferencing for victims whose identities are protected, Ministère de la Justice, Circulaire de lutte contre le proxénétisme, France, December 18, 2001, see Articles 706-58 and 706-61 of the Code de procédure penal. Consequently, a circular on criminal policy regarding human trafficking recognized, on the one hand, the very specific phenomenon of cyber prostitution and, on the other hand, the need to investigate the Internet and financial flows to disrupt the economic side of the traffic, Ministère de la Justice, Circulaire de politique pénale en matière de lutte contre la traite des êtres humains, France, January 22, 2015. The circular regarding the law that created the offense of human trafficking does not mention any link with cyber trafficking or coercion, except for the aggravating circumstance, Ministère de la Justice, Circulaire de présentation des dispositions de droit pénal de la loi n° 2003-239 du 18 mars pour la sécurité intérieure et de la loi n° 2003-88 du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xénophobe, France, February 3, 2003

[314] Article 225-4-2.I.3° of the Code pénal. Neither Spain (Article 177bis, and Article 22 regarding general aggravating circumstances) nor Romania (Articles 210-214, Article 75 regarding general aggravating circumstances) consider a similar aggravating circumstance. However, it could be noted that it is an aggravating circumstance in Spain for the offense of criminal organizations and groups, Article 570 bis.2.c.

[315] Article 225-7.10° of the Code pénal: pimping is aggravated when committed "*through the use of an electronic communication network for the dissemination of messages to a non-specified public*." It might include all kinds of pimping, from recruitment to exploitation, but is still limited to messaging to a non-defined audience. Ollard criticizes the lack of harmonization of these "*digital aggravating circumstances*" all over the Code pénal, R. Ollard, "Un an de droit pénal du numérique (Octobre 2021 – Octobre 2022)," *Droit pénal*, LexisNexis, December 2022, no. 12, ¶ 8

[316] See, for instance, aggravating circumstances for slavery, Code pénal, art 224-1 C; for forced labor and servitude, art 225-15; for forced begging, art 225-12-6.

[317] C. Guisasola Lerma, "Prevención y represión penal del delito de trata: una aproximación al anteproyecto de Ley Orgánica integral contra la trata y la explotación," *Revista Española de Empresas y Derechos Humanos*, July 2023, no. 1, p. 55

framework, and then to digital means of coercion. The state remains the first and only actor to exercise coercion through criminal law, with prosecution and conviction on one side, and protection on the other. By theorizing digital legitimate coercion, states obtain new opportunities to exercise their powers and to reaffirm their sovereignty. Not all the components of these new means of coercion are digital, underscoring the interactions between cyberspace and the real world. As traffickers take advantage of the opportunities offered by new technologies, the state remains the primary actor in combatting cyber trafficking. Its digital coercion powers can be applied to all sides of the strategy to repress trafficking: the prosecution of offenders, the protection of victims, and the prevention of the phenomenon. The role of the sovereign state in fighting against cyber trafficking is increasingly recognized within the international framework. Treaties are mainly technology-neutral, but the case law of the ECHR has evolved with the new *modus operandi* of offenders. This creates new positive obligations for the state to consider the cyber parts of the offense in complying with the supranational human rights framework.

127. Conclusion of chapter. Sovereignty, equated with the concept of a state, is usually defined through three material components: population, territory, and government. However, these concepts are variable, both in their legal definition and when facing social phenomena such as globalization and digitalization. Although sovereign states will not seem to disappear with globalization or digitalization, all of their elements are modified because of it, and these changes introduce new vulnerabilities and create further opportunities to commit human trafficking. Thus, their definition depends on states, not on sovereignty. Setting aside these criticisms of the theory of the state, human trafficking appears to be one of the threats to its material components. Population was presented as the first element of a state; however, human trafficking was mainly, in its origin, taken into account only in its transnational *modus operandi*, therefore focusing on territory. This highlights the different priorities of a criminal approach or a human rights approach. Human trafficking, especially when facilitated by new technology, violates the fundamental rights of victims. The means of for those violations are diverse, and the consequences might be amplified due to new technologies, although comprehensive studies are still lacking. When trafficking is transnational, it hinders the control of the state over its territory. This challenge increases when processes are facilitated by services in cyberspace, which is not

delimited by national borders. Linked to corruption, money laundering, and criminal organizations, trafficking negatively affects governments. As states' sovereignty is threatened by trafficking, sovereignty also appears to be the basis of its repression. Indeed, the legitimate coercion of the state seems to be at the center of the fight against this traffic. The broad notion of coercion is legitimized within the state on various bases; this monopoly leads states to be the only bearers of international obligations to repress trafficking. Despite being a "*global crime*" that requires a "*global justice*" response,[318] the main solutions still rest in the hands of states. Their obligations are broader by the inclusion of a new digital layer of coercion, to adapt their response to the evolution of the phenomenon. This extension of their powers of coercion and, thus, of sovereignty, can be developed through specific examples of criminal procedure law.

[318] M. Delmas-Marty, *Le relatif et l'universel*, *op. cit.* note 22, p. 42

Chapter 2. The extension of the state's sovereignty to face cyber human trafficking

128. When "*states have seldom adequate capabilities to fully enforce restrictions on criminal activities, […] their sovereignty is incomplete*."[1] Criminal law remains the acme of legitimate coercion and, thus, of sovereignty: Coercion must adapt to criminal realities. As a result, many criminal legislative changes were designed to strengthen digital coercion to protect states' sovereignty from new crimes. States might consider extending these new tools of digital legitimate coercion to cyber human trafficking, which is hindering their sovereignty. States rest first on the extension of their competence to prosecute and convict offenders, modifying the classical definition of the principle of territoriality (Section 1). However, the determination of sovereignty through jurisdiction is not enough. The state also develops its digital legitimate coercion through digital investigative techniques, to effectively obtain evidence against offenders (Section 2).

Section 1. Cyber human trafficking: a potential extension of the geographical scope of digital legitimate coercion

129. Principle of territoriality. The state will determine the offenses that will be prosecuted within the limits of its sovereignty through the rules on jurisdiction. The principle of territoriality provides that states should prosecute only offenses committed in their territory. This principle is recognized in the international instruments against trafficking[2] and in the studied national frameworks.[3] Therefore, an offense of trafficking can be prosecuted in the country in which the acts, means, or exploitation take place.

---

[1] R. Väyrynen, *Illegal Immigration, Human Trafficking, and Organized Crime*, no. DP2003-72, World Institute for Development Economic Research, WIDER Working Paper Series, 2003, p. 4

[2] Article 15.1 of the Palermo Convention, Article 31.1.a of the Warsaw Convention and Article 10.1.a of Directive 2011/36/EU

[3] In France, this principle is clearly recognized since "*The offense is deemed to have been committed in the territory of the Republic if one of its constitutive acts took place in that territory*," Article 113-2 of the Code pénal. In Spain, similarly, the Ley Orgánica 6/1985 del Poder Judicial considers the territorial application of the criminal law at Article 23.1. In particular, the Spanish definition of human trafficking is criticized due to the unnecessary specification that the offense can occur "*on Spanish territory, or from Spain, or in transit or to Spain*." See, for instance, P. Lloria García, "El delito de trata de seres humanos y la necesidad de creación de una ley integral," *Estudios Penales y Criminológicos*, June 22, 2019, vol. 39, p. 378. It is necessary for the victim to be physically present in Spain at some point during the process, M. Cabanes Ferrando, *La trata de seres humanos: concepto desde el marco normativo: una aproximación al delito*, J.M. Bosch Editor, 2022, p. 203. In Romania, the principle is enshrined at Article 8.1 of the Codul penal.

However, when the constitutive acts are committed online, is this part of a national territory? Where is the recruitment of a victim located when it happens on Facebook? To what territory is the online advertisement of a victim's kidney linked?[4] Where does threatening a victim via a web-based message application to force them into exploitation take place?

130. Defining cyberspace. Regarding cyber trafficking, certain material elements take place in cyberspace. What is cyberspace?[5] There are few definitions of it. Post considers that it exists "*everywhere, nowhere, and only on the Net*."[6] It is integrated into the various layers of digitalization,[7] and it can be understood as a "*space for the circulation of information flows and signs via teleinformatics networks, notably the Internet and all information systems*."[8] It is considered open, since it accepts "*almost any kind of computer or network to join in one universal network-of-networks*"; minimalist, as it requires "*very little of the computers that wanted to join*"; neutral, as it

[4] This topic is of particular importance regarding online exploitation: the consequences of the exploitation will be global (for instance, forced sexual livestreaming), while the servers hosting the data may be located outside of a state's borders, G. Geoffroy, *Rapport d'information sur la prostitution en France*, no. 3334, Assemblée Nationale, France, April 13, 2011, p. 52

[5] Originally, the word comes from the science fiction novel Neuromancer, written by William Gibson and published in 1984, P. Trudel, "La lex electronica," *in* C.-A. Morand (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no. 46, 2001, p. 221. The novelist defined its creation as a "*new informational space made of connected computer and brain networks*," P. Musso, "Le Web : nouveau territoire et vieux concepts," *Annales des Mines - Réalités industrielles*, ESKA, November 2010, vol. 2010/4, no. 4, p. 80. Such creations influenced well-known masterpieces such as the Wachowski sisters' films Matrix.

[6] D.G. Post, "Governing Cyberspace," *Wayne Law Review*, 1996, vol. 43, no. 1, p. 160

[7] "*The first layer […] is formed by a circuit of electronic impulses. The second layer […] is based on an electronic network, but it connects specific places, with well-defined social, cultural, physical and functional characteristics. The third important layer of the space of flows refers to [its] spatial organization*." According to this division, cyberspace would be the second layer, M. Castells, *La sociedad red*, Alianza Editorial SA, La era de la información: economía, sociedad y cultura, June 30, 2005, vol. 1, pp. 488-492. Bratton proposed six layers. "*First, the* Earth *layer provides a physical foundation […] The* Cloud *layer [offers] the vast server archipelagos behind the scenes and behind the surface that provide ubiquitous computational services […] The* City *layer […] comprises the environment of discontinuous megacities and meganetworks that situate human settlement and mobility in the combination of physical and virtual envelopes […] the* Address *layer examines massively granular universal addressing systems […] The* Interface *layer describes the projective, perceptual cinematic, semiotic layer on a given instrumental landscape, including the frames, subtitles, navigable maps, pixelated hallucinations, and augmented realities through which local signification and significance are programmed […] At the top […] is the most culturally complex layer, the* User," B.H. Bratton, *The stack: on software and sovereignty*, MIT Press, Software studies, 2015, pp. 121-123. Depending on how cyberspace is defined, it could correspond to either the cloud, the city, or the interface layers.

[8] P. Musso, "Le Web," *op. cit.* note 5, p. 75. The American Department of Defense gave a longer definition in 2008: "*A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*," X. Raufer, *Cyber-criminologie*, CNRS Éditions, 2015, p. 19

regards "*every other type of early application [as] the same*."[9] Cyberspace is also interconnected,[10] dematerialized, decentralized, and offers highly customized services.[11]

131. Dividing cyberspace. Cyberspace can be separated from the physical world; indeed, "*Physical location and physical space are becoming both indeterminate and functionally irrelevant*."[12] However, on the one hand, virtual interactions directly interfere with real people and have real consequences, especially regarding human trafficking:[13] Cyberspace is only "*blurring boundaries between the virtual and the real*."[14] On the other hand, cyberspace does not have borders like those in the physical space, but it can be divided depending on technical rules, especially regarding domain names;[15] the content accessible depending on the localization of the Internet Protocol (IP) address;[16] or the community of users in a specific space;[17] for example, taking into account the language used.[18] It is the idea of Lessig when he considers, "z*oning the net*."[19] Although there are "*no territorially based boundaries*,"[20] some scholars accept the idea of the "nationalization" of cyberspace.[21] In that sense, cyberspace can be "*an augmentation and a digital extension of the territory*."[22]

132. Thus, the classical notion of the state's territorial competence (or jurisdiction) evolves (§1). Moreover, the state relies on other criteria to avoid the difficulties linked to cyberspace (§2). However, the use of these grounds for jurisdiction can be doubtful, particularly considering the state's results in repressing human trafficking (§3).

---

[9] J.L. Goldsmith, T. Wu, *Who controls the Internet? Illusions of a borderless world*, Oxford University Press, 2006, p. 23

[10] It can be deemed as the major characteristic of cyberspace, D.G. Post, "Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace," *Journal of Online Law*, 1995, ¶ 13

[11] P. Trudel, "La lex electronica," *op. cit.* note 5, pp. 224-225

[12] D.G. Post, D.R. Johnson, "Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems," *Chicago-Kent Law Review*, 1998, vol. 73, no. 4, p. 1058

[13] See *supra* 112 to 115.

[14] K.F. Aas, "Beyond 'the desert of the real': crime control in a virtual(ised) reality," *in* Y. Jewkes (ed.), *Crime online*, Willan, 2007, p. 167

[15] J.L. Goldsmith, T. Wu, *Who controls the Internet?*, *op. cit.* note 9, p. 31

[16] *Ibid.* p. 55

[17] L. Lessig, "The Zones of Cyberspace," *Stanford Law Review*, May 1996, vol. 48, no. 5, p. 1406

[18] J.L. Goldsmith, T. Wu, *Who controls the Internet?*, *op. cit.* note 9, pp. 50-51

[19] L. Lessig, "Reading The Constitution in Cyberspace," *Emory Law Journal*, 1996, vol. 45, no. 3, p. 16

[20] D.G. Post, "Governing Cyberspace," *op. cit.* note 6, p. 160

[21] J.L. Goldsmith, T. Wu, *Who controls the Internet?*, *op. cit.* note 9, p. 6. One extreme example would be the control of part of cyberspace by China.

[22] P. Musso, "Le Web," *op. cit.* note 5, p. 75. As the territory extended to oceans and seas and then to atmospheric space with the development of technologies such as ships and airplanes, it could now be extended to cyberspace.

§1. Redefining territory

133. All of a state's criminal laws cannot be applied in global cyberspace. Indeed, "*a sovereign's jurisdiction […] necessarily extends only to events and transactions that bear some relationship to [its] physical territory.*"[23] Therefore, the state must define the criteria to link cyberspace, in which the constitutive acts of trafficking are committed, to its sovereign territory. In the absence of case law considering cyber human trafficking, this study relies on literature and potentially applicable norms. Indeed, multiple criteria have been drawn to establish connections to a territory, applied to cyberspace in particular to prosecute press liberty and intellectual property rights offenses in France and by the Court of Justice of the European Union (CJEU) (I). Finally, the French criminal code inserted an original[24] extension of territory to fit with the evolution of cyber offenses (II).

I. Linking cyberspace to national territory

134. Applicable theories. Various theories can delimit a sovereign jurisdiction in cyberspace. First, the theory of action establishes jurisdiction in the country in which the offense is committed.[25] For example, if the offender buys an airline tickets for the victim from a computer located in France, then France is competent. However, such localization is difficult to detect because offenders and technological tools can cross physical borders, and there are now techniques for faking a localization.[26] Second, there is the theory of ubiquity,[27] which recognizes the possibility of seeing an online element globally, independently from the origin of its emission. On the one hand, the theory of reception assumes a very broad interpretation of the concept of ubiquity.[28] As soon as an element is visible in the territory of a country, this country is competent. The information does not have to actively target a specific recipient. For example, an

[23] D.G. Post, "Governing Cyberspace," *op. cit.* note 6, p. 158
[24] Neither the Spanish Ley Orgánica del Poder Judicial nor the Romanian Codigul Penal contain any similar special grounds for competence.
[25] A. Huet, "Le droit pénal et internet," *Petites affiches*, November 10, 1999, no. 224, p. 40
[26] Like a Virtual Private Network (VPN) or a proxy, J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1694
[27] A. Huet, "Le droit pénal et internet," *op. cit.* note 25, p. 39
[28] D. Brach-Thiel, "La compétence des juridictions pénales françaises face aux infractions commises via Internet," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 39

advertisement for a foreign trafficked victim, on a foreign website, for services suggested in a foreign country, but visible on a computer located in France, could trigger the French competence. This example underlines that, if this interpretation facilitates the prosecution of crimes, it is also too broad.[29] Many countries would have jurisdiction for the same offense, confronting their different sovereignties and hindering the principle of *ne bis in idem*. On the other hand, the theory of ubiquity receives a restrictive interpretation. The focalization theory adds complementary criteria to ensure that the element is intended for people in a specific country. This theory uses various indicators:[30] language[31] or the country in which the products can be delivered. In the last example, if the victims were advertised for future exploitation in France, French jurisdiction would be confirmed. All of these theories were applied by the case law, particularly in France and by the CJEU.

135. CJEU case law. The case law of the CJEU can seem inconsistent at first, using both theories to determine the applicable jurisdiction. Usually at stake are Articles 5.3 and 15.1.c of Regulation 44/2001 of December 22, 2000, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, repealed and replaced by Articles 7.2 and 17.1.c of the Regulation 1215/2012 of December 12, 2012. First, the jurisdiction is set "*where the harmful event occurred or may occur*" for delict or quasi-delict torts. It supposes "*a particularly close connecting factor between the dispute and the courts of the place*":[32] It underlines the theory of focalization. Second and similarly, jurisdiction over consumer contracts supposes that "*the mere fact that an Internet site is accessible is not sufficient*."[33] However, to facilitate the reparation of torts, which is the closest topic to criminal law, the CJEU broadened its interpretation of the first jurisdiction rule by referring to the theory of reception. Courts

[29] J. Bossan, "Le droit pénal confronté à la diversité des intermédiaires de l'internet," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2013, ¶ 4

[30] *Faisceau d'indices* in French.

[31] English, French and Spanish are among the top ten languages used on the Internet, Miniwatts Marketing Group, "Top Ten Internet Languages in The World - Internet Statistics," *Internet World Stats*, January 31, 2020, online https://www.internetworldstats.com/stats7.htm (retrieved on September 22, 2021)

[32] CJEU, *Concurrence SARL v Samsung Electronics France SAS, Amazon Services Europe Sàrl*, December 21, 2016, C-618/15, ¶ 26; ECJ, *Handelskwekerij G. J. Bier B.V. v Mines de Potasse d'Alsace S.A. (preliminary ruling requested by the Gerechtshof of The Hague)*, November 30, 1976, C-21/76, ¶ 11

[33] Paragraph 24, preamble of the Regulation 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), referring to the Regulation 44/2001, CJEU, *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)*, December 7, 2010, C-585/08 and C-144/09, ¶¶ 92-94; CJEU, *L'Oréal SA and others v. eBay International AG*, July 12, 2011, C-324/09, ¶ 64

are competent when the website is accessible in their country. However, this interpretation is limited, since the "*court has jurisdiction only to determine the damage caused in the Member State within which it is located*."[34]

136. Criminal case law. Regarding the criteria applied to link cyberspace to territory, the French case law depends on the chambers of the *Cour de Cassation* and has evolved over time.[35] The criminal chamber did not have many opportunities to consider jurisdiction for online offenses,[36] and regarding offenses against press liberty, the court applied the theory of reception.[37] Tribunals followed this position for offenses committed in cyberspace. The major example is the Yahoo! case[38] regarding Nazi materials sold on this website.[39] However, the case law evolved in favor of the theory

[34] CJEU, *Pez Hejduk v EnergieAgentur.NRW GmbH*, January 22, 2015, C-441/13, ¶ 38; ECJ, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL, Chequepoint International Ltd and Presse Alliance SA*, March 7, 1995, C-68/93, ¶ 33; CJEU, *eDate Advertising GmbH v. X; and Olivier Martinez, Robert Martinez v. MGN Limited*, October 25, 2011, C-509/09 and C-161/10, ¶ 52; CJEU, *Peter Pinckney v. KDG Mediatech AG*, October 3, 2013, C- 170/12, ¶ 47; CJEU, *Gtflix Tv v. DR*, December 21, 2021, C- 251/20, ¶ 30

[35] D. Brach-Thiel, "La compétence des juridictions pénales françaises face aux infractions commises via Internet," *op. cit.* note 28, pp. 38-42; M. Kebir, "Compétence territoriale : accessibilité d'un site internet à l'origine d'un dommage," *Dalloz Actualité*, Dalloz, November 6, 2017. Outside the criminal field, the first civil chamber of the court seems to always rely on the theory of reception, especially in cases regarding intellectual property rights violations, Cour de Cassation, Chambre civile 1, December 9, 2003, no. 01-03225; Cour de Cassation, Chambre civile 1, January 22, 2014, no. 11-24019; Cour de Cassation, Chambre civile 1, January 22, 2014, no. 10-15890; Cour de Cassation, Chambre civile 1, January 22, 2014, no. 11-26822; Cour de Cassation, Chambre civile 1, October 18, 2017, no. 16-10428. Those decisions rely on the usual following argument: "*Accessibility, within the jurisdiction of the court hearing the case [...] is sufficient to retain the jurisdiction of that court*." On the contrary, the commercial chamber seems to always have been using the theory of focalization, requiring that the online websites would be intended for a French public, considering that "*The mere accessibility of an Internet site on French territory is not sufficient to retain the jurisdiction of French courts*," Cour de Cassation, Chambre commerciale, January 11, 2005, no. 02-18381; Cour de Cassation, Chambre commerciale, March 20, 2007, no. 04-19679; Cour de Cassation, Chambre commerciale, March 9, 2010, no. 08-16752; Cour de Cassation, Chambre commerciale, July 13, 2010, no. 06-20230; Cour de Cassation, Chambre commerciale, March 29, 2011, no. 10-12272; Cour de Cassation, Chambre commerciale, September 20, 2011, no. 10-16569; Cour de Cassation, Chambre commerciale, March 20, 2012, no. 11-10600; Cour de Cassation, Chambre commerciale, May 3, 2012, no. 11-10507; Cour de Cassation, Chambre commerciale, May 3, 2012, no. 11-10508; Cour de Cassation, Chambre commerciale, February 12, 2013, no. 11-25914; Cour de Cassation, Chambre commerciale, July 5, 2017, 14-16.737; Cour de Cassation, Chambre civile 1, June 15, 2022, no. 18-24850

[36] The criminal chamber applied the theory of action only once, Cour de Cassation, Chambre criminelle, December 8, 2009, no. 09-82120 and 09-82135

[37] The court always considered that those offenses could be prosecuted where they were published, then accessible, Cour de cassation, *Le juge et la mondialisation: dans la jurisprudence de la Cour de cassation - Etude annuelle 2017*, La Documentation Française, 2018, p. 198. It also applied this theory to other offenses, Cour de Cassation, Chambre criminelle, January 15, 2008, no. 07-86944.

[38] J. Francillon, "Le droit pénal face à la cyberdélinquance et à la cybercriminalité," *Revue Lamy Droit de l'immatériel*, April 1, 2012, no. 81, p. 6

[39] In accordance with the first judgment, the appeal court emphasized that the website allowed "*Internet users located in France, and in particular in the jurisdiction of the Tribunal de Grande Instance of Paris, to view on their computer screen the incriminated services and sites*," Cour d'appel de Paris, 11ème chambre, *Timothy K. et Yahoo! Inc v. Ministère public, Association Amicale des déportés d'Auschwitz et des Camps de Haute Silésie, et MRAP*, March 17, 2004; Tribunal de grande Instance de Paris,

of focalization, especially in cases of intellectual property rights offenses.[40] Since 2010, the court has required evidence that the concerned website "*was aiming at the French public audience*."[41] In 2016, this requirement was extended to press liberty offenses committed through cyberspace:[42] The publication should take place in France, and being accessible is not an act of publication. Therefore, the French territory seems to extend into cyberspace, but only if various clues link it to the physical sovereign territory. Applying this case law of the *Cour de Cassation*, cyber trafficking could be prosecuted as soon as it bears proximity to the sovereignty of the country.

137. Beyond the case law, a new and original article was introduced in the French Penal Code to address online jurisdiction.

II. Linking cyber offenses to territory: the French Penal Code

138. A new ground of competence. The limited criminal case law on jurisdiction came into question in 2016.[43] A new article, 113-2-1, provides that "*Any crime or misdemeanor [délit] carried out by means of an electronic communication network, when it is attempted or committed to the detriment of a natural person residing in the territory of the Republic or of a legal entity whose registered office is located in the territory of the Republic, is deemed to have been committed in the territory of the Republic*." Therefore, the legislation abandons the division between the theories of reception and focalization to use the notion of residence.[44] Although this article bestows wide competence to French jurisdictions in cyberspace, three criticisms

Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" v. Yahoo ! Inc. et Yahoo France, May 22, 2000, Ordonnance de référé

[40] Cour de Cassation, Chambre criminelle, September 9, 2008, no. 07-87281; Cour de Cassation, Chambre criminelle, December 14, 2010, no. 10-80088; Cour de Cassation, Chambre criminelle, November 29, 2011, no. 09-88250

[41] Cour de Cassation, Chambre criminelle, December 14, 2010, *op. cit.* note 40; confirmed by the commercial chamber: "*The mere accessibility of an Internet site on French territory is not sufficient to justify the jurisdiction of the French courts*," Cour de Cassation, Chambre commerciale, March 29, 2011, *op. cit.* note 35. See also Cour de Cassation, Chambre criminelle, November 29, 2011, *op. cit.* note 40

[42] Cour de Cassation, Chambre criminelle, July 12, 2016, no. 15-86645

[43] Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, see M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 127

[44] Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes - Rapport sur la cybercriminalité*, République française, February 2014, pp. 210-211. However, its tenth recommendation would have limited this ground of competence to misdemeanors punishable by imprisonment and used nationality criteria.

arise.[45]

139. Criticism: scope. Part of the literature interprets the scope of this article to be restricted to cybercrime offenses in a narrow sense,[46] for example, offenses against the confidentiality, integrity, and availability of computer data and systems.[47] On the contrary, Parizot argues that this provision has a wider purpose.[48] Indeed, in the explanatory memorandum of the law, this article was meant to strengthen the guarantees during the criminal procedure and to simplify its conduct. Moreover, relying on the definition of the "*by means of*" expression, it means "*using that method, instrument, or process*." Therefore, if human trafficking offenders use an electronic communication network to realize the material elements of the offense through cyberspace, human trafficking could be included within the scope of the article.

140. Criticism: actor. Second, the provision relies on the victim. It is coherent with the evolution of criminal procedure, which actively includes more and more victims.[49] However, the first objective of this procedure is to find and convict offenders. Thus, if the victim is not identified or is not residing in France, the French jurisdiction will not be competent on this ground. As a special exception to the principle of territoriality, does it mean that if the victim is does not reside in France, French jurisdictions will not be competent at all on the ground of the principle of territoriality? For example, if a person in a foreign country advertises a deceptive job in France to recruit people in this foreign country, and no victim is yet residing in France, then French jurisdictions will not be competent. This does not consider the theory of ubiquity.

141. Criticism: residence. Finally, the concept of residence[50] does not seem appropriate. On the one hand, it is not a common criminal code concept.[51] The criteria established by other grounds of competence are nationality, or, regarding terrorist

[45] As for June 2023, there has been no interpretation of the Cour de Cassation.
[46] See *infra* 296 for an explanation on the different categories of cybercrimes
[47] D. Brach-Thiel, "La compétence des juridictions pénales françaises face aux infractions commises via Internet," *op. cit.* note 28, p. 43
[48] R. Parizot, "Loi du 3 juin 2016 : aspects obscurs de droit pénal général (Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale)," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 376
[49] See *supra* 108.
[50] The residence is different from the domicile, the former being a matter of fact and the second a matter of law in the civil law culture, T. Debard, S. Guinchard, *Lexique des termes juridiques 2021-2022*, Dalloz, Lexiques, 29th ed., 2021, pp. 928-929
[51] Although it is used in the Code de procédure pénale, for example, for house arrest (articles 137 and following of the Code de procédure pénale)

offenses, the habitual residence.[52] This notion is also used in the European regulations on international private law,[53] but they do not define it.[54] For this reason, the CJEU linked the concepts of habitual residence and mere residence[55] to the "*permanent center of […] interests*."[56] While Article 113-2-1 does not use the adjective "habitual," scholars consider that the mere concept of residence should induce a notion of stability, both in civil law[57] and in international law.[58] Thus, an intangible definition is linked to intangible cyberspace. If the concept is interpreted as habitual residence, it challenges the French competence on cyber trafficking. Potential foreign victims can maintain the center of their interests, such as family, and property, in their country of origin. The habitual part is also difficult to apply to some victims when they move regularly within one country or at the transnational level.

142. Although linking cyberspace to the principle of territoriality has been challenging, the state can still expand its sovereign power of coercion to repress human trafficking through other bases of jurisdiction.

---

[52] Articles 113-13 and 113-14 of the Code pénal. On the former article, see D. Brach-Thiel, "Le nouvel article 113-13 du code pénal : contexte et analyse," *Actualité juridique Pénal*, Dalloz, 2013, p. 90; J. Alix, "Fallait-il étendre la compétence des juridictions pénales en matière terroriste ? (à propos de l'article 2 de la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme)," *Recueil Dalloz*, 2013, p. 518; T. Herran, "La nouvelle compétence française en matière de terrorisme - Réflexions sur l'article 113-13 du Code pénal," *Droit pénal*, April 2013, no. 4, p. étude 10. On the notion of habitual residence, see C. Pomart, "Enfin une définition pour la notion de résidence habituelle," *Revue Lamy Droit civil*, September 1, 2006, no. 30

[53] Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters; Regulation 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations, etc.

[54] E. Ralser, "Fascicule unique : Domicile et résidence dans les rapports internationaux - Articles 102 à 111," *JurisClasseur Civil Code*, LexisNexis, December 27, 2017, ¶ 41

[55] It has been very clear since the interpretation of Regulation n°1408/71 of the Council of 14 June 1971 on the application of social security schemes to employed persons and their families moving within the Community, when the CJEU considers that the "*concept of 'the Member State in which he resides' must be limited to the State where the worker, although occupied in another Member State, continues habitually to reside and where the habitual center of his interests is also situated*," ECJ, *Silvani Di Paolo v. Office National de l'Emploi*, February 17, 1977, C-76/76, ¶ 17

[56] ECJ, *Anciens Etablissements D. Angenieux fils aîné and Caisse primaire centrale d'assurance maladie de la région parisienne v. Willy Hakenberg*, July 12, 1973, C-13/37, ¶ 32. This definition has been reproduced in the French case law: "*Habitual residence, an autonomous concept in European law, is defined as the place where the person concerned has fixed, with the intention of giving it a stable character, the permanent or habitual center of his interests*," Cour de Cassation, Chambre civile 1, December 14, 2005, 05-10.951. It is similar to the national definition given in nationality law: "*For the purposes of nationality law, residence means an actual establishment of a stable and permanent nature coinciding with the center of the family ties and occupations of the person concerned*," Cour de Cassation, Chambre civile 1, February 11, 1997, no. 95-11674

[57] Y. Buffelan-Lanore, "Domicile, demeure et logement familial," *Répertoire de droit civil*, Dalloz, December 2019, ¶ 6

[58] E. Ralser, "Domicile et résidence dans les rapports internationaux," *op. cit.* note 54, ¶¶ 42-44

§2. Expanding the competence

143. To link the commission in cyberspace of material elements of human trafficking to states' jurisdiction, the principle of territoriality does not seem sufficient, so other grounds of competence were developed to expand states' digital coercion and sovereignty.[59] To begin, physical material elements of the offense can occur within a national territory: Annex jurisdiction allows criminal prosecution to be extended abroad or online, recognizing the transnational component of cyber trafficking (I). When trafficking is fully committed abroad, other grounds for extraterritorial jurisdiction facilitate the prosecution of human trafficking (II).

I. Brick-and-mortar offenses: the annex jurisdiction

144. Brick-and-mortar trafficking. E-commerce platforms are usually divided between brick-and-mortar companies and pure-player companies. The former refers to companies that have both a shopping website, and shops in the real world.[60] This dichotomy exists in cyber trafficking. For instance, a victim may be forced to stay on the street to look for "clients" while they are advertised online. A broader sense of the "brick-and-mortar" expression means that all cyber activities rely on physical infrastructure.[61] They are the "*physical foundations*"[62] of the Internet, used to power its infrastructure, to flow between continents, and to stock data.[63] Similarly, cyber trafficking always has material elements, in particular, offenders and victims.[64] Physical and digital elements are combined in brick-and-mortar trafficking.

145. Annex jurisdiction. Grounding jurisdiction on digital elements is difficult; it is

[59] This extension of criminal law outside the territory of the state was validated by the Permanent Court of International Justice, *Lotus*, September 7, 1927, no. 9, pp. 19-20
[60] For example: Ikea, H&M, Carrefour, etc.
[61] Regarding online commerce, they will usually have a physical space to locate the goods, or, if the goods are digital too, a place to produce them or take decisions about the company.
[62] N. Choucri, D.D. Clark, "Who controls cyberspace?," *Bulletin of the Atomic Scientists*, SAGE Publications, September 1, 2013, vol. 69, no. 5, p. 22. The three other layers are the following: "*The logical layer, which includes the Internet protocols, the World Wide Web, browsers, the domain-naming system, websites, and software that make use of the physical foundations; the information layer of encoded text, photos, videos, and other material that is stored, transmitted, and transformed in cyberspace; and, of course, the users who shape the cyberexperience and the nature of cyberspace itself by communicating, working with information, making decisions, and carrying out plans*."
[63] It also corresponds to the first layer of The Stack theorized by Bratton, meaning the Earth, B.H. Bratton, *The stack*, *op. cit.* note 7, pp. 134-179
[64] However, regarding sexual exploitation, some raise the rights of robots as victims, T. Daups, "Pour une charte constitutionnelle de la robotique et des nouvelles technologies," *Petites affiches*, Lextenso, October 6, 2017, no. 200, p. 7

easier based on physical elements. Once those are proved, jurisdiction can be extended. The procedure can be broadened to indivisible[65] or connected[66] offenses. On the one hand, indivisibility requires a variety of offenders for the same offense or a variety of offenses by the same offender.[67] The procedure can also extend to offenses with a "*mutual dependency relationship*."[68] For example, in the case of human trafficking, exploitation in France may be inextricably linked to recruitment in another country via online advertisement or the online threat of violence against the victim's victim's family overseas. On the other hand, this connection implies that offenses have been committed by several persons at the same time, or at different times and places but according to a defined purpose (for example, in an organized crime group), or by a relationship of cause and effect, when the purpose of certain offenses was to facilitate the execution of others or to ensure their impunity.[69] A stronger link is needed between offenses. There should be a direct cause-and-effect relationship between recruitment and exploitation: Those elements are committed for the same purpose, even if committed in different places and at different times.

146. Limits. These grounds for broad jurisdiction may allow a thorough examination of cyber trafficking. Nonetheless, they face some limits. First, the requirement for a variety of offenders[70] does not apply to most human trafficking cases: A wide range of actors are involved in the umbrella term "traffickers," including recruiters, transporters,

[65] Article 382.3 of the Code de procédure pénale. The Ley de Enjuiciamiento Criminal recognizes the same concept in its Article 17.1.

[66] Article 382.3 of the Code de procédure pénale linked to Article 203. The Codul de Procedură Penală does not seem to make a difference when considering joint cases. Article 43 gives the following examples: "*a) when two or more offenses were committed by the same person; b) when two or more persons participated in the commission of an offense; c) when there is a connection between two or more offenses and joinder of cases is required for a proper rendering of justice*."

[67] B. Bouloc, G. Stefani, G. Levasseur, *Procédure pénale*, Dalloz, Précis, 27th ed., 2020, p. 638

[68] É. Verny, *Procédure pénale*, Dalloz, Cours Dalloz, 7th ed., 2020, p. 123. Article 17.3 of the Ley de Enjuiciamiento Criminal seems to recognize a similar concept, but with more restrictions: "*Crimes that are not connected but have been committed by the same person and are analogous or related to each other when they fall under the jurisdiction of the same judicial body*." It only considers the situation of a variety of offenses by the same offenders.

[69] Article 203 of the Code de procédure pénale, see B. Bouloc, G. Stefani, G. Levasseur, *Procédure pénale*, *op. cit.* note 67, p. 637. Article 17.2 of the Ley de Enjuicimiento Criminal considers similarly the following examples: those committed by two or more persons together; by two or more persons in different places or times, if there has been a prior agreement to do so; as a means to perpetrate others or to facilitate their execution; to procure impunity for other crimes; or by several persons when injuries or reciprocal damages are caused.

[70] Article 203 of the Code de procédure pénale. On the contrary, Article 17.2 clearly considers other grounds than a variety of offenders.

hosts, controllers, and money launderers.[71] Not all of them might be qualified as offenders for the trafficking offense. Some cases of trafficking involve only one trafficker organizing the entire process; thus, it could be difficult to extend jurisdiction to digital material elements. Second, the requirement for a variety of offenses does not fit regarding human trafficking: Its different stages are still part of the same offense.[72] Arguing that the recruitment, transportation, and exploitation stages are different offenses hinders the fact that they are all rooted in the same reasons.

147. Examples. Despite these limits, French law enforcement authorities already seem to rely on the connection theory to extend to material elements from abroad. This theory considers the transnational component of trafficking, for instance, the recruitment of the victims in their country of origin.[73] A trafficking case that can be considered cyber trafficking that was prosecuted in Montpellier, included the material elements committed in Spain.[74] Thirty-three victims were identified in an organized sex tour operation in southern France, based on a telephone backbone installed in Barcelona.[75] However, this case appears to rely exclusively on a territorial basis: the exploitation in France.

148. These techniques may broaden jurisdiction to include cyber trafficking elements, regardless of where they were committed materially, as long as they are connected to or indivisible from physical material elements. However, as cybercrime evolves, traffickers discover new ways to exploit victims, and pure-player trafficking emerges.

II. Pure-player offenses: extraterritorial jurisdiction

149. Going extraterritorial. A pure-player cyber human trafficking case may have no material elements in a country but visible content accessible from it. Its repression can rely not on the extension of the territory but on the acknowledgment of

[71] See, for example, T. Spapens, “The business of trafficking in human beings,” *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, pp. 537-543

[72] In that regard, the Codul de Procedură Penală considers joint procedures in cases of “*continued offenses, of formal multiple offenses, or in any other cases when two or more material acts compose a single offense*.”

[73] Conversation with prosecutors from section F3 of the Tribunal Judiciaire of Paris

[74] Conversation with a prosecutor of the Tribunal Judiciaire of Montpellier

[75] Le Figaro, AFP, “Un réseau international de traite des êtres humains démantelé dans le sud de l’Europe,” *Le Figaro.fr*, March 5, 2021, online https://www.lefigaro.fr/faits-divers/un-reseau-international-de-traite-des-etres-humains-demantele-dans-le-sud-de-l-europe-20210305 (retrieved on April 19, 2021)

extraterritorial competence. The law does not intend to "nationalize" parts of cyberspace but designs rules of extraterritoriality through other links to its sovereignty. Supranational instruments and national laws recognize extraterritorial jurisdiction, including provisions facilitating its application for human trafficking.

150. Supranational texts. International texts offer extraterritorial grounds for jurisdiction, but those lists are not exhaustive.[76] The Palermo Convention and the Warsaw Convention[77] consider extraterritorial jurisdiction based on the nationality of the victim, the nationality of the offender (or their residence if they are a stateless person), the preparation of an organized criminal group for committing an offense within the territory of a state, or the presence of the offender in the territory of a state and the impossibility of extradition (principle of *aut dedere aut judicare*).[78] Regarding the nationality of the offender, the Warsaw Convention introduces the principle of dual criminality: The prosecution will be allowed, "*if the offense is punishable under criminal law where it was committed or if the offense is committed outside the territorial jurisdiction of any State*."[79] The Directive 2011/36/EU extends these grounds for extraterritorial jurisdiction[80] to the principle of the nationality of the victim to their habitual residence,[81] which creates a supplementary jurisdiction basis when the offense is "*committed for the benefit of a legal person established in its territory*."[82] Furthermore, to facilitate the prosecution of extraterritorial human trafficking facts, the directive allows for exceptions to the principle of dual criminality and the requirement to base the prosecution on a "*report made by the victim in the place where the offense was committed, or a denunciation from the State of the place where the offense was committed*."[83]

151. National translations. Consequently, national grounds for extraterritorial jurisdiction sometimes specifically consider account human trafficking. In France, the

[76] Article 15.6 of the Palermo Convention, complementing the Palermo protocol on human trafficking; and Article 31.5 of the Warsaw Convention
[77] Article 15 of the Palermo Convention; and Article 31 of the Warsaw Convention
[78] This principle obliges a state to prosecute an offense when refusing the extradition of the offender.
[79] Article 31.1.d of the Warsaw Convention
[80] The basis of the nationality of the offender is recalled at Article 10.1.b, and the residence of the offender is taken into account at Article 10.2.c. Regarding the principle *aut dedere aut judicare*, which is not recognized in the directive, within the framework of the European arrest warrant, cases for refusal of extradition are more limited, see Article 4 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA), and the principle of dual criminality is not required for human trafficking, Article 2.2.
[81] Article 10.2.a of Directive 2011/36/EU
[82] Article 10.2.b of Directive 2011/36/EU
[83] Article 10.3 of Directive 2011/36/EU

exceptions from the directive were indeed transposed.[84] However, the prosecution must rely on the request of the prosecutor, and the recognition of the principle of *aut dedere aut judicare*[85] is limited to certain grounds for refusal of extradition.[86] The Spanish legislation considers specific grounds for extraterritorial prosecution of trafficking.[87] The law eliminates the need for dual criminality, but it requires a request from the public prosecutor or the victim.[88] On the contrary, Romanian law does not consider specific provisions for jurisdiction over human trafficking. Dual criminality is not required if the sentencing provides a term longer than 10 years of imprisonment,[89] but it is not the case for human trafficking.[90] Extraterritorial prosecutions do not mention the need for a victim's report or a state's denunciation but require internal authorizations.[91] Finally, Romanian law considers the possibility of prosecuting an

[84] Non-application of dual criminality when the ground for jurisdiction is the nationality of the offender, Article 113-6 of the Code Pénal in relation with Article 225-4-8. Article 113-6 provides that the French nationality could have been acquired after the commission of the offense. Regarding the ground for jurisdiction on the basis of the nationality of the victim, Article 113-7 of the Code pénal requires misdemeanors prosecuted on this ground of jurisdiction to be punished by a sentence of imprisonment, which is the case for human trafficking (Article 225-4-1.I, seven years of imprisonment). This ground for extraterritorial competence is very close to the new Article 113-2-1, which is another criticism of the literature, D. Brach-Thiel, "La compétence des juridictions pénales françaises face aux infractions commises via Internet," *op. cit.* note 28, p. 45. The prosecution does not need the complaint of the victim or the denunciation of the state of commission, Article 225-4-8 of the Code pénal. It does not apply if the case is prosecuted within a jurisdiction with regional or national competence, like a juridiction interrégionale spécialisée (JIRS) or the Paris Juridiction nationale chargée de la lutte contre la criminalité organisée (JUNALCO), Article 113-8-1.

[85] Article 113-8-1 of the Code pénal

[86] The following grounds for refusal allow the principle of *aut dedere aut judicare* to be invoked: the sentence could be against the French public order, such as a death sentence; the offender was convicted by a court that did not ensure the fundamental guarantees of procedure and protection of the rights of the defense; the offense is political; and extradition could have serious consequences for the person, particularly due to their age or state of health.

[87] Article 23.4.m of the Ley Orgánica del Poder Judicial. They include the nationality or residence of the offender and the nationality or residence of the victim, but only if the offender is present in Spain. "*An analysis of these connection criteria allows us to point out that the legislator has opted to implement a principle of universal territorial jurisdiction based on the* iudex aprehensionis*, since it considers that Spanish courts may prosecute an offense of trafficking regardless of the place where the crime has occurred and the nationality of the victims, as long as the perpetrator is in Spanish territory*." All these requirements make "*it almost impossible for a Spanish court to hear a trafficking offense committed abroad, even if the victim is of Spanish nationality*," J.M. García-Martínez, "Trata de Seres Humanos y Jurisdicción Universal," *Revista Aranzadi de Derecho y Proceso Penal*, Autumn 2023, vol. 69

[88] Article 23.6 of the Ley Orgánica del Poder Judicial

[89] Regarding the nationality of the offender, Article 9 of the Codul de Procedură Penală. Dual criminal is not applicable when the offense "*was committed in a location that is not subject to any state's jurisdiction*," which is highly improbable regarding trafficking. The law recognized extensively the criteria of the nationality of the victim, Article 10 of the Codul de Procedură Penală.

[90] Article 210 of the Codul Penal. Article 12 of the Codul de Procedură Penală considers that the stipulations of those articles can evolve through the ratification of an international treaty. However, since the suppression of the dual criminality principle is not mandatory in supranational instruments on human trafficking, it still applies.

[91] The prosecution would need an "*authorization from the Chief Prosecutor of the Prosecutor's Office attached to the Court of Appeals in whose jurisdiction the first Prosecutor's Office is located that received*

offender when they are located in the territory, by application of the principle *aut dedere aut judicare* or for offenses "*the Romanian State has undertaken to repress on the basis of an international treaty*," which should include human trafficking.[92]

152. An application to human trafficking. As a result, states have other grounds for extraterritorial jurisdiction to prosecute human trafficking, particularly cyber trafficking materially committed outside their territory. However, it still needs a special connection with the sovereignty of the state: in general, the nationality of the trafficker or the victim. The applicability of these grounds is more or less eased by national legislation, depending on whether the country equates residence with nationality and on procedural criteria. The exception to the requirement of a victim report is particularly important in the framework of trafficking due to the limits regarding identification of victims.[93] Moreover, the exception to the dual criminality principle considered by the directive might be seen as unnecessary due to the existence of an international definition of trafficking. Nonetheless, the national transposition of this exception seems more than useful since national definitions are still not fully harmonized[94] and might highlight incompatible differences. For the victims, these grounds allow them to connect the prosecution and the source of reparation to their home country, to which they may return or live.

153. Cyber trafficking takes place in cyberspace, where it may not be possible to link the material elements of the offense to a sovereign territory. However, extraterritorial jurisdiction allows the states to extend their power of coercion to repress cases that trigger their duty to protect in other ways. Still, if the legal tools are multiple and ease the prosecution of human trafficking, are the states really going to use them?

§3. Extended jurisdiction for cyber trafficking: a real problem?

154. Hypothesis: proactive sovereignty. The objective of an extended jurisdiction is to consider the digital elements of trafficking or to establish jurisdiction for cases with no material element in the national territory but somehow linked to it. The delimitation

information about the violation, or, as the case may be, from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice" (jurisdiction based on the nationality of the offender), or "*from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice*" (jurisdiction based on the nationality of the victim).

[92] Article 11 of the Codul de Procedură Penală

[93] See *infra* 161.

[94] See *supra* 19.

of jurisdiction is key to determining the scope of a state's sovereignty and its powers of legitimate coercion. It is hypothesized that states have a proactive policy to repress human trafficking, especially cyber trafficking. This phenomenon would be seen in the offenses prioritized for prosecution, including through extended competence. However, the real priority given to trafficking challenges the application of the wide range of grounds for jurisdiction.

155. EU and national strategies. In strategic documents, the EU has focused recently on cyber trafficking, with the objective of "*tackling the digital business model of traffickers*."[95] However, the jurisdiction topic is considered only when trafficking is linked to an organized criminal group or a transnational process.[96] In France, Spain, and Romania, cyber trafficking is almost ignored,[97], although such an evolution can be explicitly recognized.[98] On the contrary, for instance, the French action plan is still at the delayed stage of "*putting human trafficking at the heart of the criminal policy of*

[95] European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," EU, April 14, 2021, p. 11, COM(2021) 171 final

[96] *Ibid.* p. 4; European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025," EU, April 14, 2021, p. 8, COM(2021) 170 final

[97] Except, in France, regarding the evolution of responsibilities of the digital sector for advertisements for sexual services, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, "2nd plan d'action national contre la traite des êtres humains 2019-2021," France, 2019, Measure 35. However, a slow evolution can be highlighted, for instance in the 2023-2027 action plan against illegal work (one form of exploitation after trafficking), which includes one measure to develop cyber investigations, Commission nationale de lutte contre le travail illégal, "Plan national de lutte contre le travail illégal (2023-2027)," Direction Générale du Travail, France, May 22, 2023, p. 13. In Spain, no specific actions are foreseen in the last action plan. Only a general measure is included to "*promote concrete actions to improve the detection of possible cases of human trafficking and exploitation through the use of new technologies*," Centro de inteligencia contra el terrorismo y el crimen organizado, "Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023," Secretaría de Estado de seguridad, Ministerio del Interior, Spain, January 2022, Measure 1.2.E. In Romania, no action is programmed to specifically take into account such evolution, Guvernul, "Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022," Romania, October 31, 2018, pp. 21-22. In any case, the role of new technologies is mainly recognized for prevention, through communication campaigns, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, *2nd plan d'action national contre la traite des êtres humains 2019-2021* actions 1 and 2; Ministerio de Sanidad, Servicios Sociales e Igualdad, "Plan integral de lucha contra la trata de mujeres y niñas con fines de explotación sexual 2015-2018," Spain, 2014 measure 21; Guvernul, *Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022*, p. 20

[98] Guvernul, *Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022*, *op. cit.* note 97, pp. 4-5; Centro de inteligencia contra el terrorismo y el crimen organizado, *Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023*, *op. cit.* note 97, p. 27

public prosecutors' offices."[99]

156. GRETA evaluations. Lately, the GRETA also considered the evolution of human trafficking through new technologies,[100] but its study of the evaluations does not seem to be a priority. Regarding jurisdiction where it is highly affected by digital material elements, it does not appear to be an important part of the evaluation. For instance, in the second evaluation round,[101] reports only generally explained extraterritorial rules. On the contrary, the GRETA monitors the evolution of investigative techniques available to prosecute human trafficking.[102]

157. Judicial results. As states continue to struggle to repress human trafficking as a material offense or sometimes as a brick-and-mortar offense, jurisdiction is not a topic of priority, even though it is a main component of the definition of sovereignty.[103]

---

[99] Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, *2nd plan d'action national contre la traite des êtres humains 2019-2021*, *op. cit.* note 97, Measure 34. This lack of priority given to human trafficking in France has been highlighted by the three years with no national strategy, CNCDH, "Avis sur le 2nd plan d'action national contre la traite des êtres humains (2019-2021)," France, December 1, 2019, ¶¶ 1, 7

[100] GRETA, "Table ronde sur la traite des êtres humains à l'ère du numérique," *Coe.int*, December 18, 2019, online https://www.coe.int/fr/web/anti-human-trafficking/news/-/asset_publisher/fX6ZWufj34JY/content/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age (retrieved on September 20, 2021); GRETA, "8th general report on GRETA's activities covering the period from 1 January to 31 December 2018," Council of Europe, 2019, p. 20; GRETA, "9th general report on GRETA's activities covering the period from 1 January to 31 December 2019," Council of Europe, 2020, ¶¶ 7, 8, 43; GRETA, "11th general report on GRETA's activities covering the period from 1 January to 31 December 2021," Council of Europe, 2022

[101] GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Spain - Second evaluation round," Council of Europe, 2018, ¶ 266; GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Romania - Second evaluation round," Council of Europe, 2016, ¶ 198; GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by France - Second evaluation round," Council of Europe, 2017, ¶ 285. The topic is not mentioned in the reports for the third round of evaluation.

[102] See *infra* Part 1. Title 1. Section 2. . N. Le Coz, "Les apports du droit européen et du Conseil de l'Europe à la lutte contre la traite des êtres humains," *in* B. Lavaud-Legendre (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 168, evaluation on the basis of the Committee of ministers, "Recommendation Rec(2005)10 on 'special investigation techniques' in relation to serious crimes including acts of terrorism," Council of Europe, April 20, 2005, p. 10

[103] It is also a topic of priority for human trafficking, in particular regarding sexual tourism harming minors. In this regard, Section F3 of the Paris Tribunal judiciaire noted that extraterritorial competence is indeed applied for sexual tourism against minors. Nevertheless, those cases are not prosecuted in France for human trafficking, but for infantile pornography (Articles 227-21-1 to 227-28-3 of the Code pénal) or rape (Articles 222-22 to 222-33-1 of the Code pénal). Interestingly, pornography is included in the list of kinds of exploitation in Spain, Article 177 bis.1.b of the Código Penal. In the United States, the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act was passed with this objective, K.D. Breckenridge, "Justice Beyond Borders: A Comparison of Australian and U.S. Child-Sex Tourism Laws," *Pacific Rim Law & Policy Journal*, 2004, vol. 13, p. 404; A. Fraley, "Child Sex Tourism Legislation Under the PROTECT Act: Does It Really Protect?," *St. John's Law Review*, 2005, vol. 79, no. 2, p. 444. Similarly, the Trafficking Victims Protection Act of the United States has been extended to include extraterritorial competence since 2008, M.Y. Mattar, "Interpreting Judicial

First, the investigations are mainly reactive[104] due to the discovery of evidence on the territory or to the complaints of victims.[105] Second, the results of the repression are still limited. Globally, the United States estimates that more than 115,000 victims were identified in 2022, while fewer than 5,600 exploiters were convicted.[106] In France, there were only 20 convictions in 2018 for human trafficking[107] while associations assisted almost 3,000 victims the same year.[108] In 2021, there were 24 convictions for trafficking in Spain while 1,626 persons were detected and assisted under the framework protocol for protection of victims of human trafficking, although assistance under this framework is limited to the assistance of trafficked victims trafficked for sexual exploitation.[109] Comparatively, in 2021, 505 victims were identified in Romania, and 175 people were definitively convicted of human trafficking.[110]

158. Conclusion of the section. Due to the difficulty of raising human trafficking as a political priority, jurisdiction does not seem to be questioned, although it is applied regarding cybercrimes. Jurisdiction is indeed a materialization of sovereignty by defining the scope of the exercise of coercion. Nevertheless, if countries would like to expand their competence to strengthen their action against cyber trafficking, they can rely on various grounds of competence, both as an extension of territory by linking cyberspace to the physical space of the state and by the application of extraterritorial

---

Interpretations of the Criminal Statutes of the Trafficking Victims Protection Act: Ten Years Later," *American University Journal of Gender Social Policy and Law*, 2011, vol. 19, no. 4, pp. 1290-1294

[104] Compared to proactive investigations, understood as an investigation where "*investigators decide when and where to launch the investigation, direct the investigation as they see fit, and control the investigation to its conclusion*," Global programme against trafficking in human beings, "Toolkit to Combat Trafficking in Persons," UNODC, UN, 2008, p. 178

[105] K. Mitchell, d. boyd, *Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement*, Crimes against Children Research Center, University of New Hampshire, November 2014; A. Farrell, C. Owens, J. McDevitt, "New laws but few cases: understanding the challenges to the investigation and prosecution of human trafficking cases," *Crime, Law and Social Change*, March 2014, vol. 61, no. 2, pp. 139-168. This is confirmed by French professionals, especially the OCRTEH and the OCLTI. The Section F3 of the Tribunal judiciaire of Paris confirmed the absence of the exercise of extraterritorial jurisdiction in their cases. Similarly in Belgium, see F. Kurz, "Prosecution of trafficking in human beings in civil law systems The example of Belgium," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 232

[106] Department of State, "Trafficking in persons report," US, June 2023, p. 77

[107] GRETA, "Evaluation Report - France - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, February 18, 2022, ¶ 105

[108] A. Sourd, A. Vacher, *La traite des êtres humains en France Profil des victimes suivies par les associations en 2018*, Troisième enquête annuelle, Observatoire national de la délinquance et des réponses pénales, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, 2019

[109] GRETA, "Evaluation Report - Spain - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, June 12, 2023, ¶ 114

[110] Agenţia Naţională Împotriva Traficului de Persoane, "Raport Anual privind fenomenul traficului de persoane în anul 2021," Romania, 2022, pp. 9, 22

grounds of competence. However, these tactics rely on an "*extensive interpretation, numerous exceptions and a partial dilution*"[111] of basic concepts, which would challenge tribunals in applying these rules and in introducing coherence between them. Once a state has jurisdiction to prosecute cyber trafficking, it can also rely on the extension of its means of coercion to secure prosecutions and fortify its sovereignty.

Section 2. Cyber human trafficking: a wide extension of the material scope of the state's digital legitimate coercion

159. After considering where cyber trafficking can be prosecuted, states must consider how to prosecute it. Law enforcement authorities need evidence to secure convictions and to officially recognize the status of trafficked victims among those identified. Given the evolution of the *modus operandi* of trafficking, the means of coercion will need to be extended to include new types of digital coercion (§1). Thus, the studied states will rely on similar investigative techniques, applicable to trafficking (§2).

§4. The need to extend investigative techniques to prosecute cyber trafficking

160. As the material elements of human trafficking take advantage of cyberspace and new technologies, they produce new sources of evidence. Underscoring the limits of classical trafficking investigations, based on victims' testimonies (I), new opportunities arise by using new technologies to secure prosecutions, thus making use of extended means of digital coercion by the sovereign state (II).

I. The limits of classical investigative techniques

161. Identifying victims. Traditionally, investigations into human trafficking rely heavily on victims' testimonies,[112] particularly to demonstrate the coercive nature of the offense.[113] Consequently, law enforcement authorities should first identify the

[111] M. Van de Kerchove, "Eclatement et recomposition du droit pénal," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000, p. 8
[112] A. Farrell, C. Owens, J. McDevitt, "New laws but few cases," *op. cit.* note 105, p. 158; K. Bales, S. Lize, "Investigating Human Trafficking," *FBI Law Enforcement Bulletin*, April 2007, vol. 76, no. 4, p. 26
[113] A. Farrell, B. Kane, "Criminal Justice System Responses to Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 653

victims,[114] but, many obstacles limit this process.[115] One is the failure "*of local officials to prioritize the problem of human trafficking and inadequate training to prepare law enforcement and other first responders to identify cases*."[116] Additionally, lack of identification can be seen as a consequence of "*the hidden nature of the crime*."[117] Identification is further hindered by a lack of self-identification as victims, which can be due to numerous factors: "*no knowledge of their rights*"; the "*accept[ance of] exploitation, as a means to an end,*" which may be migration; or when the "*exploitation takes place within the setting of a relationship*."[118]

162. Obtaining testimonies. Once victims are identified, their participation in the criminal investigation is not automatic. According to INTERPOL, "*less than 0.5% of victims worldwide agree to testify*,"[119] and law enforcement authorities face many

[114] Moreover, "*The possibility for identification is frequently the only limit preventing further abuses*": The identification is needed for both aspects of criminal law, which are, the prosecution of offenders and the protection of victims, S. Howell, "Systemic Vulnerabilities on the Internet and the Exploitation of Women and Girls: Challenges and Prospects for Global Regulation," *in* H. Kury, S. Redo, E. Shea (eds.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, p. 588

[115] Regarding victims of trafficking for labor exploitation in Spain, Villacampa Estiarte summarizes various elements that challenge obtaining testimonies: the fear to file a complaint against the offender, the fear to be deported due to an undocumented situation, not speaking the language, the lack of self-identification, the lack of cooperation with law enforcement authorities, and the difficulty to check the identity of the victims, C. Villacampa Estiarte, "Dificultades en la persecución penal de la trata de seres humanos para explotación laboral," *Indret: Revista para el Análisis del Derecho*, Universitat Pompeu Fabra, 2022, no. 2, p. 182

[116] A. Farrell, "Improving Law Enforcement Identification and Response to Human Trafficking," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 185

[117] A. Farrell, C. Owens, J. McDevitt, "New laws but few cases," *op. cit.* note 105, p. 158

[118] M. van Meeteren, J. Hiah, "Self-Identification of Victimization of Labor Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1608-1609. Indeed, "*Complex relationships that frequently exist between victims and the perpetrators of human trafficking […] fuel the underreporting of the crime*," M. van der Watt, "A Complex Systems Stratagem to Combating Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 765. In that respect, the lover boy method could be mentioned, which consists of the trafficker making the victim fall in love with him, A. Lavorgna, *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*, Thesis, University of Trento, December 2013, p. 121; Department of State, "Trafficking in persons report," US, June 2019, p. 200; B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures – Quelles réalités sociales et juridiques ?*, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020, p. 26; F. Bovenkerk, M. van San, "Loverboys in the Amsterdam Red Light District: A realist approach to the study of a moral panic," *Crime, Media, Culture: An International Journal*, August 2011, vol. 7, no. 2, pp. 185-199

[119] L. Trautman, M. Moeller, "The Role of the Border and Border Policies in Efforts to Combat Human Trafficking: A Case Study of the Cascadia Region of the US-Canada Border," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 994

obstacles to obtaining victims' testimony.[120] One is the personal nature of the victimization and the trauma it causes.[121]. A first solution is to make ensure that "*the victim gains continued presence and begins accessing care and protection*."[122] This practical topic raises the complementarity of the crime control approach and the human rights approach.[123] Additionally, poor "*relationships between potential human trafficking victims and the police*"[124] limit the likelihood of victims testifying. Indeed, victims fear the police, often because traffickers lie "*about police brutality and deportation*,"[125] asserting that what the victims are doing is illegal.[126] To foster trust and comfort, law enforcement authorities should also consider that victims "*may be more willing to talk to someone of the same gender*" or to someone fluent in their language.[127] MoreoverArticle 26 of the Warsaw Convention considers that states can "*provide for the possibility of not imposing penalties on victims for their involvement in unlawful activities, to the extent that they have been compelled to do so*," which is a

[120] The United States' guide for law enforcement authorities investigating human trafficking outlines at least seventeen reasons why victims may refuse to testify: "*• Threaten victims with arrest or deportation • Threaten to harm or kill family in the victim's homeland • Use debt and other fines in order to create an insurmountable "peonage" situation in which the victim must work off a debt or face punishment. […] • Move victims from location to location or trading them from one establishment to another resulting in a situation where victims may not know which town or state they are in and are less able to locate assistance • Create a dependency using tactics of psychological and emotional abuse in much the same way a batterer behaves toward their intimate partner in a dynamic of domestic violence • Dictate or restrict movement • Isolate victims who do not speak English […] • Confiscate papers and legal documents • Misrepresent U.S. laws and consequences for entering the country illegally • May not perceive themselves as victims because they do not know their rights • Feel shame about the type of work they were made to do • Feel ashamed to admit victimization […] • Believe that any debts are their obligation to repay (some may have even signed a contract) • Fear law enforcement because of their illegal status […] • View their situation as temporary […] • Mistrust law enforcement because officers in their home country may be corrupt and even directly involved in the trafficking trade • Choose to remain in the situation rather than reporting the crime to keep family safe from retribution*," Department of Justice, International Association of Chiefs of Police, "The crime of human trafficking - A Law Enforcement Guide to Identification and Investigation," US, January 1, 2007, pp. 9-10

[121] M. Graw Leary, "Fighting Fire with Fire: Technology in Child Sex Trafficking," *Duke Journal of Gender Law & Policy*, 2014, vol. 21, pp. 291-292. "*Females from some cultures may be reluctant to seek assistance in these cases because of the shame and stigmatization that might come from disclosing their experience. […] Males from some cultures, particularly those with a very rigid concept of masculinity, may not want to admit their victimization*," K. Bales, S. Lize, "Investigating Human Trafficking," *op. cit.* note 112, p. 29

[122] K. Bales, S. Lize, "Investigating Human Trafficking," *op. cit.* note 112, p. 26

[123] K. Bruckmüller, S. Schumann, "Crime Control versus Social Work Approaches in the Context of the '3P' Paradigm - Prevention, Protection, Prosecution," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 124

[124] A. Farrell, "Improving Law Enforcement Identification and Response to Human Trafficking," *op. cit.* note 116, p. 185

[125] K. Bales, S. Lize, "Investigating Human Trafficking," *op. cit.* note 112, p. 27

[126] Especially since law enforcement authorities may prosecute victims instead of assisting them, for instance, due to a lack of training.

[127] K. Bales, S. Lize, "Investigating Human Trafficking," *op. cit.* note 112, p. 29

legal protection against the prosecution of trafficked victims. Although it is not a mandatory provision, the Directive 2011/36/EU made it compulsory.[128] Finally, fear of retaliation from their traffickers can prevent victims from testifying.[129] One solution to this problem could be witness protection.[130]

163. Limited use of testimonies. Even when victims are identified and are willing to testify, they will not always offer information that is vital for the criminal prosecution. First, "*Victims may not have sufficient information about criminal networks*."[131] Regarding cyber trafficking, victims may not know the real name of their trafficker; their phone number, if they communicate through a tool that does not require it; or their address. However, even if the victim provides evidence, the credibility of their testimony can be questioned.[132] Doubts regarding their statement can result from the original lack of self-identification, the original voluntary migration, or a drug addiction.[133] This is usually a result of stereotypes or a lack of training of law enforcement authorities.

164. Since the primary source of evidence for the prosecution of human trafficking

---

[128] Article 8 of Directive 2011/36/EU. It is still possible to object that this provision is not completely mandatory, as it is limited by the expression "*in accordance with the basic principles of their legal systems*." This principle is recognized specifically for human trafficking at Article 177 bis.11 of the Código penal and Article 20 of the Lege privind prevenirea și combaterea traficului de personae (although for only a limited list of offenses). The principle of non-punishment of persons who committed offenses under constraint is generally recognized at Articles 23-25 of the Codul penal (regarding physical and moral constraints) and at Article 122-2 of the Code pénal ("*A person who has acted under the influence of force or coercion which they could not resist is not criminally liable*").

[129] M. Graw Leary, "Fighting Fire with Fire," *op. cit.* note 121, pp. 291-292

[130] Article 28 of the Warsaw Convention and Article 12.3 of the EU directive. Regarding national frameworks: France: Articles 706-57 to 706-63 of the Code de procédure pénale; Romania: Lege 682/2002 privind protecția martorilor, Articles 125-130 of the Codul de Procedură Penală and Articles 26 and 27 of the Lege privind prevenirea și combaterea traficului de personae; Spain: Ley Orgánica 19/1994 de protección a testigos y peritos en causas criminals and Articles 19 to 26 of the Ley 4/2015 del Estatuto de la víctima del delito.

[131] A. Farrell, B. Kane, "Criminal Justice System Responses to Human Trafficking," *op. cit.* note 113, p. 647

[132] A. Herz, "Human Trafficking and Police Investigations," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 131. In particular, in Spain, the Tribunal Supremo developed criteria to test the credibility of testimonies of victims of gender-based violence that might be applied to victims of trafficking, despite their possible contradiction with the consequences of the victims' trauma. Those are: the relationship with the offender, the confirmation of the facts by other proofs, and the consistency of the testimony prolonged in time, repeatedly expressed, and set out without ambiguity or contradiction, M. Ibáñez Solaz, "Algunas consideraciones sobre la prueba en los delitos de violencia de género," *in* E. Martínez García (ed.), *La prevencion y erradicación de la violencia de género: un estudio multidisplinar y forense*, Aranzadi, 2012, p. 450; A. Planchadell Gargallo, "Investigación y enjuiciamiento del delito de trata: aspectos procesales desde la jurisprudencia," *in* C. Villacampa Estiarte, A. Planchadell Gargallo (eds.), *La trata de seres humanos tras un decenio de su incriminación: ¿es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, 2022, pp. 876-879

[133] A. Farrell, C. Owens, J. McDevitt, "New laws but few cases," *op. cit.* note 105, p. 160

is difficult to obtain and sometimes fails to convince judges, investigations should not rely only on the testimonies of victims.[134] It is internationally agreed that "*investigations and prosecutions [should be conducted] without relying solely and exclusively on witness testimony*."[135] As cyber trafficking creates new tracks,[136] it offers new opportunities to exercise digital coercion and facilitate the repression of the offense.

II. The advantages of digital investigative techniques

165. Defining digital investigative techniques. To begin with, what is a "digital investigative technique"?[137] Roussel defines it as any act of investigation aimed at obtaining data,[138] which can be defined as the "*representation of information for automatic processing*."[139] Data is a broadly interpreted concept, "*regardless of the nature or content of the information, and the technical format of presentation*."[140] Automatic processing is also widely broadly interpreted.[141] Within digital investigative techniques, Roussel distinguishes between invasive and non-invasive techniques. The latter means to "*extract data that is the property of the administration*,"[142] for example,

---

[134] It is even considered in Article 9.2 of the Directive 2011/36/EU, and Article 27.1 of the Warsaw Convention. It has been underlined by the EU, see European Commission, "Report on the progress made in the fight against trafficking in human beings as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims," EU, May 19, 2016, p. 12, COM(2016) 267 final

[135] OSCE, "Decision No. 557: OSCE Action Plan to Combat Trafficking in Human Beings," July 24, 2003, p. 3, PC.DEC/557

[136] In particular, Bowen cites, along with experts and material evidence, "*mobile phone downloads, cell site analysis, and downloads from personal computers belonging to the suspect, forensic evidence to link suspects to victims, evidence from closed-circuit television (CCTV), and police surveillance evidence*," P. Bowen, "Prosecution of cases of human trafficking in a common law system," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 215

[137] The Council of Europe relies on a more limited concept: special investigative techniques, which are also used in national frameworks, Committee of ministers, *Recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism*, *op. cit.* note 102. Because, for example, Article 9.4 of the EU directive does not specify investigative techniques, the term "digital investigative techniques" will be used instead.

[138] B. Roussel, *Les investigations numériques en procédure pénale*, Thesis, Université de Bordeaux, July 7, 2020, ¶ 211

[139] European Commission for the Efficiency of Justice, "European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment," Council of Europe, December 4, 2018, p. 70

[140] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data," EU, June 20, 2007, p. 28

[141] Processing is defined by Article 4.2 of the GDPR and Article 3.2 of the Law Enforcement Directive as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*." Automatic processing is defined by Convention n°108 of the Council of Europe. Regarding digital investigative techniques, they are not limited to obtaining personal data but all kinds of data.

[142] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 138, ¶ 214

an inquiry in an open-access database or one operated by an administration. On the contrary, invasive digital investigative techniques "*are at the meeting point of coercive and intrusive measures, for which the judicial authorities carry out strong and active actions in their search for elements*."[143] These are, for instance, data searches, in a physical space such as a house or in cyberspace such as by accessing a Facebook account. As they represent the core of digital legitimate coercion in criminal procedure law and, thus, of sovereignty, this study is limited to invasive digital investigative techniques.

166. Categories of digital investigative techniques. A line can be drawn between strictly digital techniques and broadly technological techniques.[144] The former takes place in the digital space, with or without a connection to cyberspace. For example, when local data are examined on a computer, one does not always enter cyberspace. Conversely, accessing a cloud save of WhatsApp conversations implies entering cyberspace. Technological techniques can include non-digital strategies such as geotagging through localization by satellites, or wiretapping through offline microphones. However, as these techniques often rely on digital automated processing and are meant to obtain data, they are included in this study.

167. Categories of data. Data, notably from phones,[145] are thus called "*evidentiary gold mines*."[146] Data can be divided into two types: content data and metadata. In general, content data is what is searched for; it is defined as "*any data in a digital format, such as text, voice, videos, images, and sound*."[147] The data can be all of the

[143] *Ibid.* ¶ 215

[144] Second, such techniques can also be divided between all-digital techniques and physical and digital techniques. One example is the implementation of malware on a computer or phone. If malware can be installed remotely, such as via email, the technology would be entirely digital. On the contrary, if the law enforcement agents must have access to the device, by arresting the owner or entering a physical space (a house, for instance), then the technique would be both physical and digital.

[145] M. Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Center on Communication Leadership & Policy, University of Southern California, November 2012, p. 28; D.M. Hughes, "Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies," *SAGE Open*, December 18, 2014, vol. 4, no. 4, p. 6

[146] Department of State, "Trafficking in persons report," US, June 2013, p. 14. See also R. Leary, J. Thomas, "How Complexity Theory is Changing the Role of Analysis in Law Enforcement and National Security," *in* B. Akhgar, S. Yates (eds.), *Intelligence Management*, Springer London, Advanced Information and Knowledge Processing, 2011, pp. 65-66. It is especially useful when it includes the "*record of all transactions and communications*," D.M. Hughes, "Trafficking in Human Beings in the European Union," *op. cit.* note 145, p. 6

[147] Article 3.12 of the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (the E-evidence regulation) and Article 4.3.b of the European Commission, Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of

short message service (SMS) communications between a victim and their trafficker, considered the "*golden evidence*."[148] Additionally, law enforcement authorities can extract metadata, understood as "*data processed in an electronic communications network for the purposes of transmitting, distributing, or exchanging electronic communications content*."[149] Therefore, using the SMS example, metadata would be the time of sending and reception of a communication. Metadata can also be important in relation to pictures, that "*often contain[ing] identifying information such as who owns the file*."[150] There are various categories of metadata. Identification data refers to "*data requested for the sole purpose of identifying the user, [meaning Internet Protocol (IP)] addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information*."[151] These data are not likely to constitute major evidence in cyber trafficking investigations, but they are needed to access other data, especially content data. For instance, access data are needed to access a Facebook account.[152] Another important type of metadata is localization data, defined as "*any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment*."[153] Geotagging is often seen as a useful digital investigative technique to investigate cyber trafficking.[154]

168. Avoiding technological solutionism. The objective of these techniques is to obtain a different type of evidence, especially when prosecuting cyber trafficking. The

personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), January 10, 2017, COM(2017) 10 final

[148] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *Social Politics*, 2014, vol. 21, no. 3, p. 472

[149] Article 4.3.c of the Proposal for a regulation on Privacy and Electronic Communications

[150] J. Middleton, "From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 474

[151] Article 3.10 of the E-evidence regulation

[152] S. Raets, J. Janssens, "Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business," *European Journal on Criminal Policy and Research*, October 26, 2019, p. 12

[153] Article 2.c of the directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal dataand the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[154] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *op. cit.* note 148, p. 469; T. Guberek, R. Silva, *"Human Rights and Technology": Mapping the Landscape to Support Grantmaking*, PRIMA, Ford Foundation, August 2014, p. 24; R. Konrad, A. Trapp, T. Palmbach, "Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications," *European Journal of Operational Research*, June 1, 2017, vol. 259, no. 2, p. 14. For example, "*Thailand has turned to satellites to tackle forced labor among fishermen in its lucrative seafood industry*," K. Guilbert, "Chasing shadows: can technology save the slaves it snared?," *Reuters*, June 21, 2018, online https://www.reuters.com/article/us-technology-trafficking-fight-insight-idUSKBN1JH005 (retrieved on March 18, 2021)

ultimate goal is to place less pressure on victims;[155] law enforcement will no longer rely solely on victims' testimonies.[156] However, a warning is needed against technological solutionism. This philosophy "*would postulate the existence of a technical solution to any problem*,."[157] bBut technology is not "*always the solution*."[158] Focusing solely on prosecuting traffickers and downplaying the importance of victims' testimonies to the point where identifying them is not a priority undermines the state's sovereignty by impeding this duty to protect.[159] Both sides of the criminal law objectives should always be considered. Classical and digital investigative techniques are complementary, with the proportion of each depending on the circumstances of each case. All digital evidence always aims, in the end, at "*offline operations*."[160]

169. Thus, digital investigative techniques appear to be of particular interest to prosecuting trafficking and fostering the protection of victims. These general considerations should be complemented by specific explanations of some legally available digital investigative techniques in national frameworks.

§5. The extension of digital investigative techniques to cyber trafficking prosecutions

170. To exercise their sovereignty, each state provides a list of investigative techniques, including digital ones. Because criminal law and criminal procedure law are the pinnacle of sovereignty, they are primarily national in nature, employing the

[155] J. Musto, "The Limits and Possibilities of Data-Driven Anti-trafficking Efforts," *Georgia State University Law Review*, May 1, 2020, vol. 36, no. 4, p. 1158

[156] A. Farrell, C. Owens, J. McDevitt, "New laws but few cases," *op. cit.* note 105, p. 158. This priority has been explicitly underlined by the OCLTI. For example, they want to develop observations using 360° cameras to better understand and record housing conditions and eventually, in a few years, be able to return to the scene via a virtual reality headset. By avoiding multiple hearings, it is possible to better elicit the empathy of those who witness the scene while minimizing the impact on the victims. Another example could be the mandatory recording of the hearings of minors for human trafficking, Article 706-52 of the Code de procédure pénale.

[157] Y. Meneceur, *L'intelligence artificielle en procès: Plaidoyer pour une réglementation internationale et européenne*, Bruylant, 2020, p. 2. It is what Pierre Ducassé called "*technophilia*." He also considered two other approaches to technology. The second one is "*anti-technicism*," with a traditional distrust to technology; the third one is "*indifference*," considering technology as neutral and insignificant for questioning the world's problems.

[158] M. Broussard, *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018, pp. 7-8

[159] I. Chen, C. Tortosa, "The Use of Digital Evidence in Human Trafficking Investigations," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 123. Part of the healing process for victims can actually include their participation in criminal proceedings and expressing what happened to them (although it should always remain voluntary).

[160] S. Yu, "Human Trafficking and the Internet," *in* M. Palmiotto (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, pp. 69-70

most harmful forms of coercion to fundamental rights. However, criminal procedure laws usually include similar investigative techniques, even if the regimes differ (II). Indeed, despite criminal procedure law being one of the last legal disciplines to be open to supranational harmonization,[161] the realities of technical capacities shape digital investigative techniques, and all of these techniques are available to investigate human trafficking (I).

I. Digital investigative techniques: wide applicability to cyber human trafficking cases

171. Techniques available for any offenses. Some digital investigative techniques are available for the investigation of any offense, and these strategies includes one of the most common investigative techniques, digital search and seizure, which is widely available in France,[162] Spain,[163] and Romania.[164] Additionally, in Spain, geotagging can be applied to the investigation of any offense,[165] while in France, geotagging is similarly widely applicable when direct localization is obtained through the victim's equipment.[166] Lastly, in Romania, the interception of the victim's communications is available to investigate any offense when requested by the victim.[167] Therefore, all of these digital techniques are applicable to the investigation of cyber human trafficking cases.

172. Techniques considering a threshold. Other investigatory methods establish a threshold to limit the investigation to offenses with a certain level of seriousness. As such, in France[168] and Spain,[169] various techniques—especially the interception of

[161] L. Arroyo Zapatero, "Quelle méthode pour une harmonisation pénale ?," *Revue Européenne du Droit*, Groupe d'études géopolitiques, 2021, vol. 2, no. 1, p. 8
[162] During the investigation for flagrancy, Articles 56 and following of the Code de procédure pénale; the preliminary investigation, Articles 76 and following; and the judicial information, Articles 92 and following
[163] Articles 588 sexies a to c, of the Ley de Enjuiciamiento Criminal, in relation to Articles 545 to 578, in the absence of specific provision
[164] Article 168 of the Codul de Procedură Penală, in the absence of specific provision
[165] As long as the measure is necessary and proportionated, Article 588 quinquies b of the Ley de Enjuiciamiento Criminal. Similarly, recording of images in public spaces, Article 588 quinquies a. As this technique is not regulated in France due to the lack of interference with privacy, it is also open to the investigation of any offense, Cour de Cassation, Chambre criminelle, April 6, 2022, no. 21-84092; Cour de Cassation, Chambre criminelle, May 7, 2019, no. 18-85596
[166] Article 230-44 of the Code de procédure pénale
[167] Article 140.9 of the Codul de Procedură Penală
[168] Interceptions of communications, Article 100 of the Code de procédure pénale. Geotagging, Article 230-32. Recording of images in public places by means of airborne devices, Article 230-47.
[169] Interceptions of communications, Article 588 ter a of the Ley de Enjuiciamiento Criminal, in relation to Article 579.1.1°. This section covers the use of technical devices (such as an IMSI-catcher) to identify terminals by capturing device or component identification codes, Article 588 ter l. However, the scope of this latter technique is not explicitly stated. Image and voice recording, Article 588 quater b.2.a.1°.

communications—are limited to offenses punishable by at least three years of imprisonment. Although this threshold has been criticized for being low,[170] it allows for the use of these approaches in the investigation of cyber human trafficking cases in both countries.[171]

173. Techniques limited to specific circumstances. Other digital investigative techniques are applicable to the investigation of offenses committed under certain circumstances. In the French and Spanish frameworks, two main categories of circumstances are the commission of an offense through electronic communications or the commission of an offense within a criminal organized group. The first circumstance is particularly important for the applicability of cyber infiltration in France and of legal hacking and secret remote searches in Spain, which would be the case for cyber human trafficking.[172] The second circumstance is almost unnecessary to reach, as cyber trafficking fits in the main scope of the studied techniques.[173]

174. Techniques considering human trafficking. In Romania, all electronic surveillance techniques[174] and infiltration[175] are limited to a list of offenses, including human trafficking. In France, special investigation methods[176] are similarly limited to a

Cyber infiltration, Article 282 bis.6 in relation to Article 588 ter a y 549.1.1°. Human trafficking committed by a criminal organized group is explicitly considered in the latter, Article 282 bis.4.c, but the offense falls within the main scope.

[170] J. Vegas Torres, "Las medidas de investigación tecnológica," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017; F. Bueno de Mata, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, Aranzadi derecho penal no. 1151, Primera edición, 2019, 2019, p. 67. It has also been criticized from its lack of harmonization, in Spain, with the thresholds of the Código penal, R. Bellido Penadés, *La captación de comunicaciones orales directas y de imágenes y su uso en el proceso penal (propuestas de reforma)*, Tirant lo Blanch, 2020, p. 100. It could further be criticized for not being harmonized for techniques with a different level of impact on privacy, from instance, no difference is made between the recording of image and voice in Spain, *Ibid.* p. 146.

[171] In France, the maximum sentence is seven years of imprisonment, Article 225-4-1 of the Code pénal. In Spain, between five to eight years of imprisonment, Article 177 bis of the Código penal.

[172] Article 230-46 of the Code de procédure pénale and Article 588 septies a.1 of the Ley de Enjuiciamiento Criminal. This category is also used in the scope of interception of communications (Article 100 of the Code de procédure pénale and Article 588 ter a of the Ley de Enjuiciamiento Criminal)

[173] Except for legal hacking and secret remote searches in Spain, for which both circumstances could be equally used, Article 588 septies a.1 of the Ley de Enjuiciamiento Criminal.

[174] Interception of communication, access to a computer system, image and sound recording, geotagging, Article 139.2 of the Codul de Procedură Penală

[175] Articles 148.1.a and 150.1.a of the Codul de Procedură Penală

[176] Interception of communication authorized outside a judicial information, Article 706-95 of the Code de procédure pénale; remote access to electronic correspondence, Articles 706-95-1 and 706-95-2; IMSI-catcher, image and voice recording, and legal hacking, Article 706-95-11

list of offenses,[177] which includes human trafficking in its aggravated forms,[178] such as when the victim was in contact with the trafficker through the use of an electronic communication network for the dissemination of messages to a non-specified public[179] or when the trafficking was committed by an organized group.[180]

175. All digital investigative techniques studied are applicable to human trafficking, particularly when facilitated by new technologies and committed partially online. These scopes face an obvious lack of harmonization in the French and Spanish frameworks. In particular, the French code is revised quite frequently to consider the evolution of techniques,[181] while the Spanish code was developed through comprehensive and global reforms[182] and the Romanian framework rests on a harmonized regulation.[183]

---

[177] Part of the doctrine criticizes the lack of harmonization of all those techniques to prosecute organized crime, M. Quéméner, "Fascicule 20 : La preuve numérique dans un cadre pénal - Articles 427 à 457," *JurisClasseur Procédure pénale*, LexisNexis, April 18, 2019, ¶ 80

[178] Aggravated circumstances include: when there are multiple victims, is from abroad or has recently arrived in France, when the victim is exposed to an immediate risk of death or injury likely to result in permanent mutilation or disability, when the victim suffer a long incapacity of work due to the level of violence, when the trafficker is a person that is supposed to repress human trafficking or is part of law enforcement authorities, when the offense has placed the victim in a serious material or psychological situation (Article 225-4-2 of the Code pénal); when trafficking is accompanied with acts of torture (Article 225-4-4 of the Code pénal).

[179] Article 225-4-2.3° of the Code pénal

[180] Article 225-4-3 of the Code pénal

[181] Loi n° 91-646 relative au secret des correspondances émises par la voie des télécommunications ; Loi n° 2003-239 pour la sécurité intérieure ; Loi n° 2004-204 portant adaptation de la justice aux évolutions de la criminalité ; Loi n° 2007-297 relative à la prévention de la délinquance ; Loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure ; Loi n° 2014-372 relative à la géolocalisation ; Loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme ; Loi n° 2016-731 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale ; Loi n° 2019-222 de programmation 2018-2022 et de réforme pour la justice; Loi n° 2022-52 relative à la responsabilité pénale et à la sécurité intérieure ; Loi n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur

[182] On the contrary, in Spain, all the techniques have been updated through the Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Such reform has been motivated in particular by the Decision 145/2014 of the Tribunal constitucional, which underlined the lack of detailed legislation on those kinds of techniques, Tribunal Constitucional, September 22, 2014, no. 145/2014; F. Otamendi Zozaya, *Las últimas reformas de la ley de enjuiciamento criminal una visión práctica tras un año de vigencia*, Dykinson, 2017, p. 23

[183] Despite various reforms: Lege nr. 281/2003 privind modificarea şi completarea Codului de procedura penală şi a unor legi speciale, Lege nr. 356/2006 pentru modificarea şi completarea Codului de procedură penală, precum şi pentru modificarea altor legi, Lege nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale, Lege nr. 75/2016 privind aprobarea Ordonanţei de urgenţă a Guvernului nr. 82/2014 pentru modificarea şi completarea Legii nr. 135/2010 privind Codul de procedură penală, Ordonanţă de urgenţă nr. 18/2016 pentru modificarea şi completarea Legii nr. 286/2009 privind Codul penal, Legii nr. 135/2010 privind Codul de procedură penală, precum şi pentru completarea art. 31 alin. (1) din Legea nr. 304/2004 privind organizarea judiciară, and Lege nr. 219/2021 pentru modificarea și completarea Legii nr. 104/2008 privind prevenirea și combaterea producerii și traficului ilicit de substanțe dopante cu grad mare de risc

Nevertheless, all of these techniques are available to investigate cyber trafficking by looking for different types of evidence.

II. Digital investigative techniques: similarities and small differences

176. While all three countries studied use the same digital investigative techniques, in general, their methodology for regulation is different. The French techniques methods are outlined in the code, depending on the stage of investigation[184] and on the circumstances. On the contrary, in Spain, investigative techniques are included in the same Title VIII and all rely on a common regime,[185] which develops principles to frame the application of these techniques.[186] Similarly, in Romania, the code regulates

[184] The French investigation is divided into three parts. Each part allows different actors to act within the investigation or to control it and the regime of the investigative techniques depends on such division. First, the investigation of flagrancy opens the possibility to realize the first observations and acts by the police officers, under the control of the public prosecutor, for a duration of eight days, see Article 12 and 53 of the Code de procédure pénale. Second, the preliminary investigation is run by the police, acting under the supervision of the public prosecutor, Article 75. As the public prosecutor is not an independent and impartial judge, ECHR, *Moulin v. France*, November 23, 2010, no. 37104/06, ¶¶ 55-59, some investigative techniques should rely on the authorization of the judge of liberties and custody. Finally, the judicial information (the instruction in a strict sense) is mandatory for crimes and optional for misdemeanors, Article 79. 94% of trafficking cases went to instruction between 2016 and 2020, Service statistique ministériel de la sécurité intérieure, "La traite et l'exploitation des êtres humains depuis 2016 : une approche par les données administratives," *Interstats*, October 2022, no. 49, p. 10

[185] Articles 588 bis a to 588 bis k of the Ley de Enjuiciamiento Criminal. Such harmonization is quite limited, as each technique specifies, for example, its duration and scope.

[186] Article 588 bis a of the Ley de Enjuiciamiento Criminal. The principle of specialty "*presupposes that the measure is related to the investigation of a specific offense*," M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015," *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario "Escorial-María Cristina," 2019, no. 52, pp. 183-184. Consequently, "*technological research measures of a prospective nature that would amount to a blank authorization*" are prohibited, I. López-Barajas Perea, "Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley," *Revista de Derecho Político*, Universidad Nacional de Educacion a Distancia (UNED), 2017, no. 98, p. 106. The suitability of the measure "*will serve to define the objective and subjective scope and duration of the measure by virtue of its usefulness*." The principles of exceptionality and necessity limit the use of technological measures when "*other less serious measures for the fundamental rights of the investigated or accused person and equally useful for the clarification of the facts*" are not possible. Finally, the proportionality of the measure implies that "*the sacrifice of the rights affected must not be greater than the benefit resulting from its adoption for the public interest or third parties*," R. Serra Cristóbal, "La vigilancia de datos y de comunicaciones digitales en la lucha por la seguridad nacional: especial referencia a las previsiones legislativa de España," *in* F. Flores Giménez, C. Ramón Chornet (eds.), *Análisis de los riesgos y amenazas para la seguridad*, Tirant lo Blanch, Derechos humanos, 1st ed., 2017, pp. 126-128. As for the principle of proportionality, in its strict sense, it considers in particular the seriousness of the punishable acts, depending on the penalty, "*the nature of the crime, the social relevance of the facts and the technological field of production*," I. López-Barajas Perea, "Garantías constitucionales en la investigación tecnológica del delito," p. 105; J.J. López Ortega, "La utilización de medios técnicos de observación y vigilancia en el proceso penal," *in* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 318; M. Cedeño Hernán, "Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017

all electronic surveillance techniques through a common regime.[187] Despite these different methodologies, digital investigative techniques can be divided between those one implemented with the knowledge of the concerned person (A) and those implemented without it (B).

A. An investigative technique known to the concerned person: digital searches

177. Digital data in material search. Searches were originally designed to look for material objects such as documents, but with the evolution of new technologies, there is now access to digital information. In general, digital searches must comply with the general regime of searches, and, as a consequence, the affected person will usually know about this technique. Two categories of digital searches can be implemented. First, the law considers the search of digital data during a physical search. In particular, it involves searching a set of "*components that have the ability to write, retain, and subsequently retrieve or read data on a storage medium*."[188] They can be divided into three categories: magnetic devices, such as a hard disk; optical devices, such as a digital versatile disc (DVD); or solid-state memory devices, such as a universal serial bus (USB) flash drive.[189] Therefore, if a computer is found during the search in the house of the trafficker, authorities can extend their search to the data accessible from it In France, police officers can "*access, through a digital system located on the location of the search, data relevant to the ongoing investigation and stored in that system or in another digital system, provided that such data is accessible from or available to the original system*."[190] French law does not require a specific authorization. On the contrary, in Spain, the authorization should explicitly mention that the judge also authorizes the registry of electronic devices.[191] A complementary authorization is required to access the digital data,[192] and another authorization—or one explicitly mentioned in the original one—is required to access any data available from the device but not stored in it.[193] Thus, the authorization only to register and seize the device does

[187] Articles 138 and following of the Codul de Procedură Penală
[188] Fiscalía General del Estado, Circular 5/2019 sobre sobre registro de dispositivos y equipos informáticos, el 6 de marzo de 2019, p. 30164
[189] *Ibid.*
[190] Article 57¶1 of the Code de procédure pénale
[191] Article 588 sexies a.1 of the Ley de Enjuiciamiento Criminal
[192] Article 588 sexies c of the Ley de Enjuiciamiento Criminal
[193] Article 588 sexies c.3 of the Ley de Enjuiciamiento Criminal

not allow access to the data.[194] Similarly, in Romania, computer searches are based on a specific authorization that should be extended to any further accessible system.[195]

178. Digital search. The second situation is a computer search within the office of law enforcement authorities. A trafficked victim interviewed at a police facility can be willing to enter the access code for their Facebook account, which displays all conversations with the trafficker. In France, the code provides the possibility to "*access, through a digital system located in a police or gendarmerie [...] unit, data relevant to the current investigation and stored in another digital system, if [these data are] accessible from the initial system*."[196] In both situations, the French practice rests on a *droit de suite*, (right to follow), meaning that "*all the branches of this system, including those located abroad, would then be subject to the same consultation procedures as the one located in France*."[197] Similarly, in Spain, the code considers digital searches to be outside the scope of a material search,[198] such as obtaining devices outside the home (e.g., seizing a defendant's phone) or accessing "*telematic data repositories*" (e.g., obtaining codes to access a Facebook account). As in the prior regime, an authorization is required to access the data. On the contrary, the Romanian articles do not seem to take into account the possibility of remote searches.

179. Because of the breadth of their scope, digital searches are an important tool for gathering evidence in a cyber human trafficking case. However, they still require the knowledge of the affected person, which can limit their effectiveness. Therefore, the codes develop a wide variety of secret digital investigative techniques, that are useful in cyber human trafficking cases.

---

[194] This double authorization consolidates the previous jurisprudence, which had developed after a change in case law, given that before 2010, the authorization to search a home was interpreted in an extensive manner "*to include the seizure of all computer media that could be found inside the home*," I. López-Barajas Perea, "Garantías constitucionales en la investigación tecnológica del delito," *op. cit.* note 186, p. 116

[195] Articles 168 and 168^1 of the Codul de Procedură Penală. The translation of the code should not be interpreted as limited to computer devices, but rather to any device that uses computing ("*sistem informatic*"). See Article 138.4, defining a computer system as "*any device or set of devices interconnected or in a functional relationship, one or more of which ensures the automatic processing of data, by means of a computer program*."

[196] Article 57¶2 of the Code de procédure pénale. The Cour de Cassation considers that finding access codes during a physical search and making use of them afterwards outside the regime of this search is an illegal search, not a simple investigation, Cour de Cassation, Chambre criminelle, November 6, 2013, no. 12-87130.

[197] R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, Thesis, Université de Lorraine, 2016, pp. 308-309

[198] Article 588 sexies b of the Ley de Enjuiciamiento Criminal

B. Secret digital investigative techniques

180. The following digital investigative techniques studied are implemented without the knowledge of the affected person. The most commonly used technique, usually the first one regulated by the criminal procedure codes, is the interception of communications (1); another technique specifically mentioned to investigate cyber trafficking is cyber infiltration (2); and other techniques could be useful to investigate cyber trafficking cases (3).

1. The original digital investigative technique: interception of communications

181. Defining "communications." The interception of communications is one of the most widely used investigative techniques. However, its regulation implies specific guarantees, since it involves a violation of the secrecy of communications, which is constitutionally protected in Spain.[199] In this framework, communication is defined as "*the process of transmission of expressions of meaning through any set of sounds, signals, or signs*."[200] What does "communications" mean in practice? Classically, it meant oral telephone conversations, but today, various types of communications can be intercepted:[201] content data, such as SMS, but also a wide range of metadata, including IP addresses or websites consulted.[202] In Spain, the extension of the technique to those other types of data requires an explicit mention in its

[199] Tribunal Constitucional, November 29, 1984, no. 114/1984; E. Frígols i Brines, "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías," *in* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 37-92

[200] Tribunal Constitucional, October 9, 2006, no. 281/2006; A.I. Vargas Gallego, "Algunos apuntes sobre la interceptación de las comunicaciones telefónicas," *Revista de Jurisprudencia El Derecho*, December 16, 2020, no. 8

[201] In France, see Article R40-46.1° of the Code de procédure pénale: "*a) Identity (name, married name, surname, forenames) of the natural person issuing or receiving the electronic communication, nickname, alias, date and place of birth, sex, parentage, family situation, nationality; b) Names, business name, legal representatives and managers of the legal entity issuing or receiving the electronic communication, as well as the registration numbers in the Trade and Companies Register; c) Address or any other information that allows the identification of the domicile, place or establishment; d) Identification elements of the link and data on the communication tools used; e) Telephone number (fixed and mobile, personal and professional); f) E-mail address or data relating to the services requested or used; g) Technical data relating to the location of the communication and of the terminal equipment; h) Data on the traffic of the communications of the intercepted link; i) Content of the intercepted electronic communications and related information; j) Data for billing and payment purposes*." In Spain, see Articles 588 ter b.2 and 588 ter d.2. b a d of the Ley de Enjuiciamiento Criminal. See also J.J. Fernández Rodríguez, "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente," *Revista Española de Derecho Constitucional*, December 14, 2016, no. 108, pp. 93-122.

[202] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 138, p. 187

authorization.[203] Therefore, the interception of communications through an identified device linked to (potential) human trafficking cases can provide a large amount of data, both on the offender(s) and the victim(s).

182. National regime. In France and Spain,[204] the regulation of intercepting communications was approved following condemnations by the ECHR.[205] The French framework regulates the "*interception of correspondence sent by electronic communications*." The latter concept is defined as the "*emission, transmission, or reception of signs, signals, writings, images or sounds by wire, wireless, optical, or other electromagnetic means*."[206] The technique is mainly limited to judicial information,[207] but a more flexible regime is applicable to the investigation of aggravated forms of trafficking[208], such as an extension of the duration.[209] The Spanish framework considers telephone and telematic communications, which has been criticized as an unnecessary specification given the rapid evolution of the means of communication.[210] However, telematic communications benefit from a broad interpretation, including "*communications involving computer software*,"[211] for instance, through WhatsApp. In Romania, the technique is broadly defined as the "*interception, access, monitoring, collection, or recording of communications made by telephone, computer systems, or by any other means of communication*."[212]

183. The extension of communication interceptions. This technique can be complemented by the use of a device to collect technical connection data and intercept

---

[203] Article 588 ter b.2 of the Ley de Enjuiciamiento Criminal defines electronic traffic or associated data as "*all data generated as a consequence of the conduction of the communication through an electronic communications network, of its availability to the user, as well as of the provision of an information society service or telematics communication of a similar nature*," and Article 588 ter d.2

[204] In Spain, the interception of communications is one of "*the most effective measures in the investigation against trafficking*," A. Planchadell Gargallo, "Investigación y enjuiciamiento del delito de trata," *op. cit.* note 132, p. 858

[205] ECHR, *Kruslin v. France*, April 24, 1990, no. 11801/85; ECHR, *Prado Bugallo v. Spain*, February 18, 2003, no. 58496/00. In France, it took a year before the first version of the interception regulation was approved, Loi n°91-646 relative au secret des correspondances émises par la voie des communications électroniques; while it took until 2015 in Spain to pass a sufficient regulation of these, Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. In particular, the Tribunal Supremo broadly criticized this shortcoming, stating that it was "*necessary to remedy [it] with the utmost urgency*," Tribunal Supremo. Sala Segunda, de lo Penal, November 26, 2014, no. 850/2014

[206] Article L32 of the Code des postes et des communications électroniques

[207] Articles 100 to 100-8 of the Code de procédure pénale

[208] Article 706-95 of the Code de procédure pénale

[209] Article 100-2 of the Code de procédure pénale

[210], E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019, p. 292

[211] F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, p. 65

[212] Article 138.2 of the Codul de Procedură Penală

correspondence,[213] in particular, an international mobile subscriber identity (IMSI) catcher.[214] Given the use of prepaid subscriber identity module (SIM) cards[215] for mobile phones by the traffickers or the victims, which do not provide as much data as phones with a permanent contract, this technique is especially useful for "*unidentified phones, acquired under a false identity or use the phones of their entourage*."[216] In Spain, this technique is not independent but is used as a means to obtain the necessary data to realize an interception of communication. Law enforcement authorities have the power to use any device to identify "*codes or technical labels of the telecommunication device or any of its components, such as the IMSI*[217] *or [international mobile equipment identity] IMEI*[218] *numbering, and, in general, […] the communication equipment used or the card used to access the telecommunication network*."[219] Such a technique does not require any authorization, but its use must be indicated when the authorities then seek to implement an interception of communications before the judge.[220] In France, the code considers obtaining more data than those envisaged under the Spanish concept: The code allows not only the "*identification of a terminal equipment or the subscription number of its user, as well as data relating to the location of a terminal equipment used*" but also the direct interception of communications between the identified devices. Given the breadth of the concept, judicial authorization is always required.[221] No similar technique is

[213] Article 706-95-20 of the Code de procédure pénale. This investigative technique is closely linked to the interception of communications, as the identification of the device is probably needed to implement an interception of communications afterwards. Therefore, the detailed regime of the latter technique is applicable, articles 100-3 to 100-7. The Spanish regulation of this device is included in the chapter on the interception of communications, article 588 ter l of the Ley de Enjuiciamiento Criminal.
[214] In a specific area (a few kilometers), this device will reroute all correspondence (both content and metadata) of all the phones used, to identify a specific one, through the identification or localization of the device, or the subscription number of the user, M. Quéméner, "La preuve numérique dans un cadre pénal," *op. cit.* note 177, ¶ 74; T. Meindl, "Fascicule 20 : Procédure applicable à la criminalité et la délinquance organisées – Poursuite. Instruction. Jugement. Assistants spécialisés – Dispositions dérogatoires de procédure – Articles 706-73 à 706-106," *JurisClasseur Procédure pénale*, LexisNexis, January 31, 2020, ¶ 63
[215] See, for example, J. Middleton, "From the Street Corner to the Digital World," *op. cit.* note 150, p. 472; D. Barney, "Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking," *Pepperdine Law Review*, 2018, vol. 45, no. 4, p. 760
[216] J.-M. Brigant, "Mesures d'investigation face au défi numérique en droit français," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 239
[217] International Mobile Subscriber Identity, included in each SIM card
[218] International Mobile Equipment Identity, used to connect a phone to the Internet
[219] Article 588 ter l.1 of the Ley de Enjuiciamiento Criminal
[220] Article 588 ter l.2 of the Ley de Enjuiciamiento Criminal
[221] Article 706-95-12 of the Code de procédure pénale

regulated by the Romanian criminal procedure code.

184. The interception of communications already allows law enforcement authorities to obtain a wide range of digital evidence. However, new approaches have been developed alongside the evolution of offenses and techniques.

2. A digital investigative technique meant for cyber human trafficking: cyber infiltration

185. Importance of cyber infiltration. Cyber infiltration is often mentioned as a digital investigative technique useful to repress cyber trafficking, especially in cases involving minors.[222] It supposes the use of false online identities to look for digital evidence. These identities can be used to make contact with traffickers or victims, to "*confirm their identities or intents through digital communication technologies*,"[223] by using the identity of a potential victim or "client." In the United States, "*nearly one-quarter to one-third of sex trafficking cases are currently uncovered through Internet searches and sting operations*."[224] Online infiltration can extend to automatic responses or artificial intelligence assuming a determined identity,[225] what is called an "automated honey trap," especially to target sex buyers,[226] and to fake websites or advertisements[227] published by law enforcement authorities. For example, in France, online investigation by using a pseudonym[228] was created in 2007[229] for specific offenses only, including human trafficking.

186. Infiltration versus cyber infiltration. Cyber infiltration should be

[222] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020, p. 46. It is often mentioned regarding minor pornography, UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, UN, May 2015, p. 47; D. Dushi, "Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo," *International Review of Law, Computers & Technology*, January 2, 2018, vol. 32, no. 1, p. 96; K.J. Mitchell et al., "Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization," *Journal of Adolescent Health*, August 2010, vol. 47, no. 2, p. 185

[223] M. Graw Leary, "Fighting Fire with Fire," *op. cit.* note 121, pp. 314-315

[224] E. Heil, A. Nichols, "Hot spot trafficking: a theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States," *Contemporary Justice Review*, Routledge, October 2, 2014, vol. 17, no. 4, p. 423

[225] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *op. cit.* note 148, p. 468

[226] J. Musto, "The Limits and Possibilities," *op. cit.* note 155, p. 1163

[227] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *op. cit.* note 148, p. 468

[228] "*The pseudonym is a fictitious name freely chosen by a person to hide from the public his/her true personality in the exercise of a particular activity*," Cour de Cassation, Chambre civile 1, February 23, 1965, no. 62-13427

[229] Loi n°2007-297, Article 35, creating Article 706-35-1 of the Code de procédure pénale

distinguished from classical infiltration and Internet monitoring. It differs from the former concept, which defined as the technique in which the agent enters "*under an assumed identity in [an] organizational network for the investigation and repression of the offenses committed, the prevention of those to be committed, as well as the ascertainment of all relevant information about the specific criminal organization infiltrated in order to reach its total disarticulation*."[230] Therefore, classical infiltration is limited to prosecutions of organized offenses. Cyber infiltration is a "*more flexible version*"[231] of this concept and, therefore, has advantages,[232] but the powers of cyber agents are much more limited than those of infiltrated agents, due to online possibilities.[233] Therefore, Quéméner considers that the term "cyber infiltration" for such a technique is "*an abuse of language, legally erroneous*."[234] In Spain, however, cyber infiltration is regulated alongside classical infiltration.[235] Nonetheless, the concept of cyber infiltration does not fully refer to infiltration regulation. In particular, there is no mention of the "*protection of the agent's real name*," the implementation of other techniques affecting fundamental rights, or the exemption of the agent from liability for their actions when they qualify as offenses.[236] Similar shortcomings can be highlighted in the French regulation. In Romania, the code does not regulate cyber infiltration and considers only general provisions for infiltration.[237]

187. Internet watch *versus* cyber infiltration. An investigative technique used

[230] R. Zafra Espinosa de los Monteros, *El policía infiltrado: los presupuestos jurídicos en el proceso penal español*, Tirant lo Blanch, 2010, p. 65

[231] M. Quéméner, "Fascicule 1110 : Infiltrations numériques," *JurisClasseur Communication*, LexisNexis, July 3, 2019, ¶ 6

[232] It "*is easier to pretend to be someone else and maintain the false identity for longer [due to the absence of physical contact;] the agent has room to delay or postpone his responses and thus be able to think about the most appropriate response at any given moment [;] this option entails less personal sacrifice for the undercover police officer, who can continue with his normal life [;] it involves almost no risk to his life and physical integrity[;] The work costs less to the state coffers and is more effective, since the same police officer may be carrying out several monitoring operations at the same time, even communicating simultaneously with a wide variety of criminals[; and] there is less danger of the agent becoming corrupted either by establishing personal relations with the person under investigation beyond what is permitted or by becoming involved as one more in the activities of the persons under investigation*," M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017

[233] However, as techniques advance and more images and audio files are exchanged, the distinction between cyber infiltration and infiltration is likely to blur, resulting in a large scale of infiltration methods, more or less digital.

[234] M. Quéméner, "Infiltrations numériques," *op. cit.* note 231, ¶ 17

[235] Article 282 bis of the Ley de Enjuiciamiento Criminal

[236] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* note 210, pp. 525-526

[237] Article 138.1.g and h of the Codul de Procedură Penală. The latter is meant for the conduct of any transaction, for example, linked to a person suspected to be a victim of trafficking, Article 138.11

daily is Internet watching, the mere surveillance of Internet public spaces.[238] Such surveillance is useful for proactive investigations. It could be the surveillance of new posts from a determined Facebook account that does not require creating an account on the website, for example, if the person is suspected to be a trafficked victim or a trafficker. However, the boundary with cyber infiltration can be subtle. An account is required to access certain spaces, therefore, the use of a false identity is required, even if no interaction is conducted.[239] A Facebook account would be necessary to be added to a private group, for example, sharing job offers that are designed to be fraudulent, meant to recruit victims for trafficking. The agent could collect the interesting data only without having any direct interaction with another person. However, both the French and Spanish frameworks are based on the ability to participate in communication exchanges and do not differentiate from Internet watching.[240]

188. **Powers of the infiltrated agent.** In France, the powers of cyber-infiltrated agents are significantly limited by law: They can "*1° Participate in electronic exchanges […]; 2° Extract or keep by this means data on persons likely to be the perpetrators of these offenses and any evidence; 3° Acquire any content, product, substance, sample, or service or transmit any content*[241] *in response to an express request. The operation is authorized by the public prosecutor or investigating judge hearing the case; 4° After authorization by the public prosecutor or investigating judge hearing the case, with a view to the acquisition, transmission or sale by persons likely to be the perpetrators [...], make legal or financial means available to these persons, as well as means of transport, deposit, accommodation, storage and telecommunications*." Depending on what type of role the agent uses, they can contact or be contacted by traffickers through

[238] Therefore, in Spain, it has been explicitly decided that data left openly on the Internet are not protected by the secrecy of communications, thus no judicial authorization is required, Tribunal Supremo. Sala Segunda, de lo Penal, May 9, 2008, no. 236/2008; Tribunal Supremo. Sala Segunda, de lo Penal, May 28, 2008, no. 292/2008; E. Velasco Nuñez, "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías," *Revista de Jurisprudencia*, February 1, 2011, no. 4, p. 6; E. Velasco Núñez, "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica," *Diario La Ley*, November 4, 2013, no. 8183

[239] M. Quéméner, "Infiltrations numériques," *op. cit.* note 231, ¶ 20

[240] The legislation could have explicitly mentioned the possibility of acting in open channels with a false identity, without the need for judicial authorization, as validated by the Tribunal Supremo, Tribunal Supremo. Sala Segunda, de lo Penal, July 5, 2007, no. 767/2007; Tribunal Supremo. Sala Segunda, de lo Penal, July 14, 2010, no. 752/2010; F. Alba Cladera, G. García Martínez, "Blanqueo de capitales y agente encubierto en internet," *in* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 192

[241] However, considering Article D47-9 of the Code de procédure pénale, it seems that the code only provides a legal framework for the transmission of child pornography material.

an electronic communication means; gather electronic evidence against them; or, upon authorization, use the role of a "client" to buy trafficked victims' services or victims directly. In Spain, by contrast, the powers of agents are viewed more broadly: The technique is intended to investigate an offense by assuming a false "*identity in communications maintained in closed communication channels*," those not being defined.[242] A complementary authorization is needed to "*exchange or send illicit files by reason of their content and analyze the results of the algorithms applied for the identification of such illicit files*."[243] As in France, no specification is made regarding those illicit files, which is highly criticized in the literature.[244] This is a very important limitation to adapt this technique to an investigation of cyber trafficking.

189. Secret investigative techniques provide for the broad technique of interception of communications and the particularly useful technique of cyber infiltration to investigate cyber trafficking. Along with the development of new technologies, legislators adopted new techniques to improve prosecutions.

3. A complementary wide range of digital investigative techniques

190. The studied criminal procedure codes offer a wide range of other digital

[242] C. de Jorge Pérez, "El escondite virtual y el nuevo agente encubierto," *in* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 249. The literature defines them as "*those characterized by the communicator's express will to exclude third parties from the communication process*," B. Rizo Gómez, "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica," *in* J.M. Asencio Mellado, M. Fernández López (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1st ed., 2017, p. 103

[243] Article 282 bis.6¶ 1 of the Ley de Enjuiciamiento Criminal. This last point allows the use of algorithms and databases on child pornography, which make it possible to identify images to highlight the similarities of the images, European Commission, "Commission Staff working document - Impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse," EU, May 11, 2022, pp. 71-72, SWD(2022) 209 final; B. Rizo Gómez, "La infiltración policial en internet," *op. cit.* note 242, p. 119. This technique is used in France, even if not considered by the code, Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes - Rapport sur la cybercriminalité*, *op. cit.* note 44, pp. 37-38. The literature considers that the actions provided for in the Spanish code should be extended, in particular to include the possibility of opening bank accounts and disposing of money, F. Alba Cladera, G. García Martínez, "Blanqueo de capitales y agente encubierto en internet," *op. cit.* note 240, p. 197

[244] F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, p. 118; M.L. Villamarín López, "La nueva figura del agente encubierto online en la lucha contra la pornografía infantil," *op. cit.* note 232; C. de Jorge Pérez, "El escondite virtual y el nuevo agente encubierto," *op. cit.* note 242, p. 251; F. Bueno de Mata, "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting,'" *in* F. Bueno de Mata et al. (eds.), *Cambio de paradigma en la prevención y erradicación de la violencia de género*, Editorial Comares, Estudios de Derecho constitucional, 2017, p. 13

investigative techniques that could be useful to investigate cyber trafficking. These can be divided between broadly technological investigative techniques, particularly geotagging and voice and image recording (a), and strict digital investigative techniques, especially remote secret access to correspondence and legal hacking (b).

a. Technological investigative techniques

191. Geotagging. Geotagging is defined as "*an automated protocol that locates any moving object both in a specific physical space and at a specific time and point in time*."[245] It can obtain past location data or real-time location, for instance, on the basis of a phone system.[246] Only real-time geotagging is examined here, since the obtaining of past location data requires information requests to private companies.[247] Real-time geotagging can be based mainly on Bluetooth technology (very short-range radio frequency), on radio frequency, on satellite-based positioning systems, or on the global positioning system of the satellite network.[248] This technique could be particularly useful for cases where victims often move, or, for example, are advertised for sex tours, to determine whether the geotagging of a phone number corresponds to the cities advertised. In France,[249] the code considers two ways to implement geotagging:[250] First, law enforcement authorities can track a person's location, or second, they can use a beacon on an object, for example, a car.[251] In Romania, the code similarly

[245] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* note 210, p. 471
[246] F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, pp. 142-143. Regarding the former option, it depends on the retention of data by the operators involved, L. Vallés Causada, "Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 60-61
[247] See, for instance, Article 230-32 of the Code de procédure pénale. When location data is obtained afterwards, law enforcement authorities must rely on Article 588 ter j of the Ley de Enjuiciamiento Criminal when it is linked to phone data, or on Article 588 sexies a when it is linked to a GPS device. In France, it will be considered a request for data, covered by Articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 or 99-4 of the Code de procédure pénale.
[248] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* note 210, pp. 472-473
[249] Originally, law enforcement authorities used the provisions on requisitions for geotagging, within the flagrancy or preliminary investigation, or those for interception of communications, within the judicial information. The first case has been considered illegal due to the absence of the control of a judge, Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81949; Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81945. On the contrary, the use of the technique within the judicial information has been considered legal, Cour de Cassation, Chambre criminelle, January 14, 2014, no. 13-84909. Consequently, the legislator regulated particularly the geotagging through the Loi n° 2014-372.
[250] Its regime is more flexible (in particular its duration) when investigating organized crime, including aggravated trafficking, Article 230-33 of the Code de procédure pénale.
[251] The code provides a detailed regime to install and uninstall the technical device, Articles 230-34 to 230-36 of the Code de procédure pénale. The lack of coherence between investigation and instruction

considers real-time geotagging of both persons and objects.[252] In Spain, the code does not specify the ways of implementing the technique,[253] but the *Tribunal Supremo* considers that the "*tracking and location of objects, without being able to know the location data of any specific identified person, does not affect the fundamental right to personal privacy*."[254] Thus, it falls outside the scope of geotagging and does not require authorization.

192. Sound and image recording. The second technological investigative technique considered by criminal procedure codes is sound and image recordings.[255] If a car, a hotel lobby, or a company's office is likely to be where traffickers talk about and negotiate their traffic or transport and exploit victims, such technology will allow investigators to record and save their words and scenes. In France, this technique is limited to the investigation of organized crime, including aggravated trafficking. It considers the recording of "*words spoken by one or more persons in a private or confidential setting, in private or public places or vehicles, or the image of one or more persons in a private place*."[256] The Spanish code regulates the recording of sounds as

---

has been criticized in the literature, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 138, p. 167

[252] Article 138.7 of the Codul de Procedură Penală

[253] Articles 588 quinquies b and 588 quinquies c of the Ley de Enjuiciamiento Criminal. Prior to the 2015 reform, it was a very flexible measure because it did not require judicial authorization: the Tribunal Supremo determined that object tracking did not violate the right to privacy, Tribunal Supremo. Sala Segunda, de lo Penal, June 22, 2007, no. 562/2007; J.J. López Ortega, "La utilización de medios técnicos de observación y vigilancia en el proceso penal," *op. cit.* note 186, p. 266; A. Melón Muñoz (ed.), *Procesal penal 2021*, Francis Lefebvre, Memento práctico, 2020, ¶ 1782.3. Since the reform, the high court has recognized a right not to be located, J.C. Ortiz Pradillo, "Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal," *Diario La Ley*, Wolters Kluwer, 2021, no. 9955, pp. 1-2; J.R. Agustina, "Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales: análisis jurisprudencial comparado en relación con el derecho a la intimidad," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2013, no. 102, p. 4

[254] Tribunal Supremo. Sala Segunda, de lo Penal, July 7, 2016, no. 610/2016; Fiscalía General del Estado, Circular 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, March 6, 2019, pp. 30156-30157

[255] This differs from the interception of communications, in which "*the sound is captured through the intercepted telephone or telematic means of communication*," Fiscalía General del Estado, Circular 3/2019 sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, March 6, 2019, p. 30125. However, the national legislations appear to only contemplate device placement and make no mention of "*smart devices that make up the so-called internet of things such as the use of devices like Amazon's Alexa*," F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, p. 100. In such a case, the communication is not transmitted through a device but rather listened to through it, so interception of communications could not be applied. However, such devices are implemented by private companies; the most appropriate technological due diligence would probably be a request for data release. This type of collaboration is already requested in the United States, M. Burke, "Amazon's Alexa may have witnessed alleged Florida murder, authorities say," *NBC News*, November 2, 2019, online https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 (retrieved on October 12, 2022)

[256] Articles 706-96 to 706-98 of the Code de procédure pénale

the main technique,[257] and the recording of images must be explicitly authorized as an additional measure.[258] This technique is limited to communications with the suspected offender, "*on public highways or other open spaces, in their home, or in any other enclosed places*."[259] Thus, the technique is further limited to communications when it

[257] Article 588 quater a.3 of the Ley de Enjuiciamiento Criminal. This technique was considered "*one of the most relevant novelties*" of the 2015 reform, M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal," *op. cit.* note 186, p. 196. Indeed, the technique, not regulated, was validated by the Tribunal Supremo before being denegated by the Tribunal Constitucional due to its lack of legal basis, J. Vegas Torres, "Las medidas de investigación tecnológica," *op. cit.* note 170; Tribunal Constitucional, September 22, 2014, *op. cit.* note 182. Image recording is only incidental since, in the protection of fundamental rights at the constitutional level in the Spanish legal system, the right to image "*is not an object of specific and autonomous criminal protection but is protected through the rights to honor and privacy*," C. Juanatey Dorado, A. Doval Pais, "Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes," *in* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 132

[258] Images are not protected in a direct and restrictive manner as communications since their secrecy is not affected (Article 18.3 of the Constitución Española). Thus, since 1998, case law has authorized "*the filming of allegedly criminal scenes occurring in public spaces or on public roads*," Fiscalía General del Estado, Circular 4/2019, *op. cit.* note 254, p. 30139. Thus, nowadays, another technique is provided, more generally, for the recording of images in public spaces, focused on the suspected person, and only for the following purposes: to "*facilitate their identification, to locate the instruments or effects of the offense, or to obtain relevant data for the clarification of the facts*." This technique is applicable to any offense and does not require any authorization, Article 588 quinquies a of the Ley de Enjuiciamiento Criminal. It can be extended to third parties when it is necessary for the "*usefulness of the surveillance*" (for example, when the person under investigation meets third parties). This concept has been criticized as decreasing the protection of the proportionality principle, E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización. Cuando la práctica forense no puede esperar," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 124. On the contrary, in France, there is no specific legal concept. The Cour de cassation validated image recording of persons in public spaces, based on the general norms on prosecutors' powers, Article 41 del Code de procédure pénale and Cour de Cassation, Chambre criminelle, December 8, 2020, no. 20-83885; S. Fucini, "Vidéosurveillance sur la voie publique durant l'enquête : conditions d'autorisation," *Dalloz Actualité*, Dalloz, January 6, 2021, and instruction judges' powers, Article 81 and Cour de Cassation, Chambre criminelle, December 11, 2018, no. 18-82365; S. Fucini, "Vidéosurveillance sur la voie publique durant l'enquête : conditions de réalisation," *Dalloz Actualité*, Dalloz, January 18, 2019, but also by police officer, as the court deemed it does not violate the right to privacy, Cour de Cassation, Chambre criminelle, May 10, 2023, no. 22-86186. This last decision has been highly criticized, E. Dreyer, "Les OPJ peuvent filmer dans l'espace public sans limite ni contrôle judiciaire," *La Semaine Juridique Edition Générale*, LexisNexis, July 10, 2023, no. 27, p. 834 This technique differs from video surveillance systems. This concept is broadly defined as "*any continuous activity of observation or control of a space by technical means resulting in the recording of images that can be used in criminal proceedings*," A. Martínez Santos, "Las grabaciones obtenidas a través de sistemas de videovigilancia en el proceso penal: derechos fundamentales afectados y tipología de supuestos," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017. This continued use is regulated by specific legislation, and differs from the occasional recording of images captured for the needs of an investigation of a criminal act already committed.

[259] Article 588 quater a.1 of the Ley de Enjuiciamiento Criminal. Thus, this technique extends to "*measures of very different nature and scope*," M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 94. In Spain and France, high courts have studied the boundaries between recording in private settings and in public settings. The Tribunal Supremo set the following criteria: It depends on whether the interference is physical or virtual, Tribunal Supremo. Sala Segunda, de lo Penal, April 20, 2016, no. 329/2016. When

can "*be reasonably foreseen that [they] will provide essential data of evidential relevance for the clarification of the facts and the identification of the perpetrator*."[260] The Romanian code also considers, in electronic surveillance techniques,[261] the observation and recording of sounds and images (pictures and videos) .[262] Such surveillance can take place in both public and private spaces.

193. Use of drones. Finally, law enforcement authorities use drones as a technological investigative technique.[263] A drone is defined as "*a set of configurable elements that constitute a remotely piloted aircraft, its associated pilot stations, the required command and control links, and any other system elements that may be required, at any time during flight operation*."[264] This technique could be used to record images of evidence from the transportation process of trafficked victims or places of exploitation, such as agricultural fields or cannabis farms. In France, legislators created a new investigative technique in 2022[265] to consider these new technologies. It regulates the use of a technical device, "*by means of airborne cameras, […] for the purpose of capturing, fixing, transmitting, and recording, without their consent, the image of one or more persons in a public place*."[266] It should be emphasized that this concept is very narrow at the technological level; it would have been more interesting to approve a technologically neutral concept, including the regulation of image capture

---

the interference is physical, it does not affect fundamental rights since the person has not "*protected their privacy*." On the contrary, when the interference is virtual, devices are used to improve the agent's vision, which triggers a violation of the right to privacy (resulting in the need for judicial authorization). Consequently, this concept does not extend to the capture of images in private spaces from public places by means of devices (binoculars, ...), F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, p. 130. Similarly, the Cour de cassation indicated that the use of devices to obtain images inside a private place violates the fundamental right of privacy, Cour de Cassation, Chambre criminelle, March 21, 2007, no. 06-89444; H. Vlamynck, "Le point sur la captation de l'image et des paroles dans l'enquête de police," *Actualité juridique Pénal*, Dalloz, 2011, p. 574.

[260] Article 588 quater b.2.b of the Ley de Enjuiciamiento Criminal

[261] However, this measure, when implemented in private spaces, relies on a specific provision for its duration, with a maximum of 120 days, instead of six months, Article 144.3 of the Codul de Procedură Penală

[262] Article 138.6 of the Codul de Procedură Penală

[263] For an example of the use of a drone in a human trafficking investigation, see, infobae, "Trata de personas: un estudio de modelos webcam se convirtió en un infierno para jóvenes de la comunidad LGBT+ en Barranquilla," *Infobae*, November 23, 2022, online https://www.infobae.com/america/colombia/2022/11/23/trata-de-personas-un-estudio-de-modelos-webcam-se-convirtio-en-un-infierno-para-jovenes-de-la-comunidad-lgbt-en-barranquilla/ (retrieved on January 2, 2023)

[264] F. Bueno de Mata, "Peculiaridades probatorias del DRON como diligencia de investigación tecnológica," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 170

[265] Loi n° 2022-52 relative à la responsabilité pénale et à la sécurité intérieure, Article 16

[266] Article 230-47 of the Code de procédure pénale. See M. Bouchet, "Les drones face aux enjeux de droit pénal et de libertés fondamentales," *Dalloz IP/IT*, Dalloz, 2022, p. 299

in public places in general. If used to obtain other types of data or in other places, this concept will be abandoned in favor of image and voice recording or geotagging. In Spain, drones have been used since 2013,[267] but their regulation is still questioned.[268] In general, the technique of recording images in public places[269] seems appropriate for the evolution of technologies. However, as in France, when the use of a drone triggers the collection of sounds and images within a private space or location data, the useo f other techniques will be required. The use of drones is not particularly considered in the Romanian criminal procedure code.

194. Although these techniques can be useful to investigate human trafficking, they are not specifically appropriate to obtain evidence in cyber human trafficking cases. Thus, to adapt to cyberspace, legislators have introduced strict digital investigative techniques.

b. Strict digital investigative techniques

195. Access to electronic correspondence. Remote access to correspondence stored via electronic communications and accessible via a digital identifier is the first strict digital investigative technique[270] and is regulated in only a few countries in the EU.[271] This technique supposes the remote use of access codes—for example, a login and a password found during the investigation remotely— which means, for example, through the computer of law enforcement authorities.[272] Thus, if the authorities have found or can find the access code of the Facebook account of a trafficker, they can

[267] L. Donoso Abarca, "Legitimidad de los sistemas de videovigilancia activa como medida de investigación tecnológica," *in* F. Bueno de Mata, I. González Pulido, L. Bujosa Vadell (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, p. 251

[268] M. Alejandra Suárez, "Diligencias de investigación tecnológicas. La licitud de la actividad probatoria de un dron," *in* F. Bueno de la Mata, I. González Pulido, L.M. Bujosa Vadell (eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 393-403; F. Bueno de Mata, "Peculiaridades probatorias del DRON," *op. cit.* note 264, pp. 169-204

[269] Article 588 quinquies a of the Ley de Enjuiciamiento Criminal

[270] In that sense, this technique is very similar to remote searches, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 138, p. 123. However, such technique does not require the knowledge or consent of the person; on the contrary, it is implemented without their notification. Moreover, the search is limited to a very short period of time, while this kind of access is limited to the duration established in the authorization, but accessing the online space could potentially happen every day during this period, as a real surveillance measure. Similarly, this technique may appear similar to communication interception, but it is broader in that it allows not only to obtain communications done during the implementation of the technique, but also to have access to prior messages, drafts...

[271] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017

[272] T. Meindl, "Articles 706-73 à 706-106," *op. cit.* note 214, ¶ 56

check the conversations and potentially the number of victims, or of their Gmail account, to learn the next destination of the victim or the place of their arrival, if the tickets for transportation were bought online. This technique is explicitly considered by the French criminal procedure code.[273] The scope of this tool is quite large, extending to any type of communication, not only emails but also social networks or any other website.[274] The Spanish framework similarly includes the "*use of identification data and codes […] that allow, remotely and electronically, the remote examination, without the knowledge of the owner or user, of the contents of a computer, electronic device, electronic system, electronic mass data storage instrument, or database*."[275] The Romanian code offers a similar technique, although less detailed: access to a computer system. It supposes "*the entry into a computer system or means of storing computer data either directly or remotely […] through a network*,"[276] which could include electronic correspondence. Although the measure does not mention the need for access codes, this entry point must be mentioned in the authorization.[277]

196. Legal hacking. Lastly, criminal procedure codes can regulate the legal hacking of computer systems.[278] Regarding cyber trafficking, once a victim is identified

[273] Articles 706-95-1 to 706-95-3 of the Code de procédure pénale

[274] One question would be if it encompasses only correspondence in a restrictive sense, meaning, in the example of Facebook, messages sent through Messenger or any post or publication that must be connected to the account to be seen (for example, Facebook publications with restricted access). The law defines the notion of electronic mail (but not of electronic correspondence), as "*any message, in the form of text, voice, sound, or image, sent over a public communications network, stored on a network server or in the recipient's terminal equipment, until retrieved by the recipient*," Article 1.IV ¶5 of the Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. As the definition is broad, as long as correspondences are private, meaning, not to be seen without a specific code of access, this technique could extend to messages (in a restrictive sense) and publications.

[275] Article 588 septies a.1 of the Ley de Enjuiciamiento Criminal. It should be underlined that the authorization to enter such a space is limited to accessing the data. If needed, the judge should explicitly authorize the copy of data, Article 588 septies a.2.d. Similarly, as the authorization should specify the accessible device (or part of it), if the law enforcement authorities need access to another device (or another part of it), a complementary authorization is needed, Article 588 septies a.3. The Spanish literature considers that its use should be limited to when "*the police is unable to determine the physical location of such data*" to request a physical search of the devices, L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015," *op. cit.* note 271

[276] Article 138.3 of the Codul de Procedură Penală

[277] Article 140.5.g of the Codul de Procedură Penală

[278] Generally, a computer, but can include phone, tablet, server, etc., through the installation of a software, also known as a "*Trojan horse*," M.C. Rayón Ballesteros, "Medidas de investigación tecnológica en el proceso penal," *op. cit.* note 186, p. 201. The literature stresses the need to create a database on the existence of such software, to be able to "*differentiate the files or programs that have been sent by the police, from those that have been obtained by the suspect themselves, in an illicit way*," I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 166-167. Depending on the software, the installation can happen remotely, or access to the physical device may be needed, M. Quéméner, "La preuve numérique dans un cadre

but does not want to end their relationship with their exploiter, their phone could be hacked to obtain more evidence. Additionally, the hacking of the device of the trafficker could permit the gathering of valuable information at every stage and from every actor of the traffic. The French code considers digital data capture,[279] which permits access to four types of data. Originally,[280] the technique allowed authorities to see and collect data as they were displayed on the user's screen, through screen logger software, or as they were typed on the user's keyboard, through a key logger. In 2014,[281] this tool was extended to access audiovisual data when audiovisual peripherals were used, for example, the data from a webcam.[282] Finally, in 2016,[283] the technique was broadened to include the access of stored data, both content and metadata,[284] through what is known as a backdoor server.[285] In Spain, the code regulates access to electronic correspondence and legal hacking under the same concept.[286] However, the Spanish technique is more restrictive than the French one, as it considers only the access of stored data.[287]. In Romania, the code merely considers that access to a computer system or a data storage device can be implemented "*from a distance, through specialized programs*,"[288] without considering what those types of programs can do or what data they can obtain.

197. Conclusion of the section. To fight human trafficking with a cyber component, states' digital legitimate coercion can manifest in criminal procedure laws as the

---

pénal," *op. cit.* note 177, ¶¶ 68-69. The entrance into private spaces to install those softwares is not regulated in either the Spanish or Romanian frameworks. On the contrary, the French code regulates it, Article 706-102-5 of the Code de procédure pénale. The literature explains this failure as needed to not "*provide clues to criminals so that they can counter-program applications that detect these*," F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 170, p. 190. On its difference with searches, see O. Décima, "Du piratage informatique aux perquisitions et saisies numériques," *Actualité juridique Pénal*, Dalloz, 2017, p. 315

[279] Articles 706-102-1 to 706-102-5 of the Code de procédure pénale

[280] As introduced by the Loi n°2011-267, Article 36

[281] As modified by the Loi n°2014-1353, Article 21

[282] The Commission nationale de l'informatique et des libertés underlined that the agents can't activate and control those peripherals, CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale (demande d'avis n°18004354)*, September 26, 2019, no. 2019-119

[283] As modified by the Loi n°2016-731, Article 5

[284] M. Quéméner, "Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme," *Dalloz IP/IT*, 2016, p. 431

[285] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 138, pp. 199-200

[286] Articles 588 septies a to 588 septies c of the Ley de Enjuiciamiento Criminal

[287] As a result, the use of keyloggers or screenloggers was not permitted, F. Otamendi Zozaya, *Las últimas reformas de la ley de enjuiciamento criminal una visión práctica tras un año de vigencia*, *op. cit.* note 182, p. 144

[288] Article 138.3 of the Codul de Procedură Penală

pinnacle of their sovereignty, specifically through investigative techniques. The use of a variety of techniques to investigate trafficking is especially relevant to lessening the burden on the victims and the weight of their testimonies to secure a conviction. These techniques also search for new forms of evidence, scattered among various types of devices, when trafficking is facilitated by new technologies. Although the criminal procedure is a highly national aspect of sovereignty, states usually consider technically available techniques, assuming the constant evolution of the law to adapt to new technologies. Despite the absence of harmonized methodologies in the organization of criminal procedure codes, and although the Spanish and the Romanian codes seem to lack certain techniques—for example, cyber infiltration, full legal hacking, or the use of an IMSI catcher—the codes regulate the same digital investigative techniques. Thus, law enforcement authorities have a broad range of means to investigate cyber trafficking, including online and technical techniques.

198. Conclusion of the chapter. As human trafficking hinders states' sovereignty, especially when facilitated or committed through online and technological means, states must materialize their digital legitimate coercion to adapt their investigation to the phenomenon. When trafficking includes cyber elements, the connection to one jurisdiction meant to repress the offense is blurred. The principle of territoriality, at the core of the exercise of the state's coercion through criminal law, must adjust or new bases for extraterritorial jurisdiction must be found. Despite the evolution of the grounds of jurisdiction applicable to human trafficking, the phenomenon still lacks sufficient political priority to extend the state's capacity to prosecute outside of its borders to comprehensively combat cyber trafficking. Nevertheless, the applicability of legal tools to broaden jurisdiction could be seen as one solution to the repression of cyber trafficking. Consequently, the state's legitimate coercion is also broadened through multiple digital investigative techniques. More commonly, law enforcement authorities can rely on numerous investigative techniques to secure data and evidence, avoiding their reliance on the testimonies of victims. All of these techniques are applicable to human trafficking, particularly when it is facilitated online or is committed within an organized group. However, it appears that these techniques are not often

implemented, especially to repress trafficking.[289] Indeed, the broadness and effectiveness of these techniques can be widely discussed when considering the requirements of the ECHR and the practical limits of their implementation. Thus, the effectiveness of the sovereign powers of states is questioned.

[289] S. Petit-Leclair, "Eurojust et la lutte contre la traite des êtres humains," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 23. Legal practionners particularly mention interceptions of communications, although underlining its limits.

199. Conclusion of the title. The theory of sovereignty is connected to the framing of the state, and the mere offense of human trafficking threatens the protection of the elements that created these frames. In particular, the offense constitutes an attack on the population over which the state has control, triggering its duty to protect, even more so considering the violations derived from cyber trafficking. When transnational, especially when facilitated by services developed in cyberspace, the offense lessens the control of the state over its territory and borders. As an offense closely linked to corruption, organized criminal groups and money laundering, trafficking is a challenge to the protection of the state's government. Despite being threatened by (cyber) trafficking, sovereignty also provides a solution to the phenomenon. At its core, it legitimizes the state to exercise coercion, including in a new and complementary digital form. Digital legitimate coercion is translated into the realities of the state's actions to combat cyber trafficking, which is increasingly recognized in the legal frameworks. Thus, the sovereignty of the state is necessary to confront cyber trafficking. Diving into the details, this digital coercion provides various tools in the criminal law system. States mean to adapt their primary reaction to criminal offenses facilitated by new technologies as a materialization of their sovereignty, and this extension of sovereign powers is suitable to comprehensively support the repression of cyber trafficking. However, the broadening of the geographical scope of the state's coercion is hardly applied to the prosecution of trafficking due to a lack of political priority. Nevertheless, the investigation of this offense can rely on a wide range of digital investigative techniques that evolve with new technologies and adapt to the needs of law enforcement authorities when collecting evidence online. However, to comprehensively fight against cyber trafficking, the state cannot be studied as a closed system. In particular, the limits to the regulation and implementation of digital investigative techniques highlight the need to cooperate with other actors. As such, digital actors serve as adequate and necessary partners for the sovereign state to improve its repression of cyber human trafficking.

TITLE 2. DIGITAL ACTORS: COMPLEMENTING SOVEREIGNTY TO REPRESS CYBER TRAFFICKING

200. When the state is studied as a closed system, a consequence of its sovereignty that creates absolute power within its borders, it appears as the central actor in the repression of human trafficking, even when it is evolving through new technologies. Sovereignty is threatened by trafficking, but it also offers a solution to repress this criminal phenomenon: legitimate coercion. This coercion is extended through state criminal law to adapt the powers of law enforcement authorities to the new realities of cyberspace. Despite the law offering many new tools, state regulation cannot be studied as a closed system; its sovereignty is influenced today by supranational frameworks. Additionally, its sovereignty has always been influenced by the pragmatic possibilities for implementing its powers of coercion. An adequate perspective on the fight against cyber trafficking should consider both levels. Consequently, when the state's digital legitimate coercion faces challenges, it must be complemented by the cooperation of other entities (Chapter 1). Since digital actors appear central to the efficient repression of cyber trafficking, states can rely on old and new legal bases for cooperation. As these frameworks for cooperation evolve to consider the particularities of cyberspace, they also increasingly recognize autonomy for digital actors and extend their own types of sovereign powers (Chapter 2). From the acknowledgement of their material powers to technically rule cyberspace to their inclusion as addresses of supranational obligations, digital actors are core to the repression of cyber trafficking and, thus, complement the actions of the sovereign state.

Chapter 1. The necessity to complement the state's sovereignty to face cyber trafficking

201. The state "*develop[ed] more intrusive […] forms of law enforcement*"[1] to improve the repression of offenses evolving through new technologies, including human trafficking. The state's sovereignty remains based on the protection of its population and territory through the use of coercion, the pinnacle of which is criminal law. However, on the one hand, voices have been raised to draw attention to the violation of human rights in the implementation of these techniques. On the other hand, numerous practical difficulties remain to fully implement them. Thus, the state's heightened powers to exert digital coercion are limited (Section 1). These limits hinder the state's ability to effectively implement its sovereignty, by reducing the tools available to investigate and prosecute cyber human trafficking. Therefore, the national frameworks for coercion, developed by the states as primary sovereign actors, will must be complemented by the activities of other actors, particularly to effectively combat human trafficking (Section 2).

Section 1. Implementing the state's powers of coercion: from legal to practical limits

202. Although the state's powers have been extended through the new layer of digital legitimate coercion, these new opportunities to investigate cyber trafficking face various challenges. Insecurities in their implementation arise due to their confrontation with human rights and supranational frameworks (§1). Moreover, practical limits prevent law enforcement authorities from making full use of these techniques (§2).

§1. <u>The legal instability of the state's digital legitimate coercion powers</u>

203. Since 1994, international scholars have underlined that the state's new powers

[1] W. van Schendel, I. Abraham, "Introduction The Making of Illicitness," *in* W. van Schendel, I. Abraham (eds.), *Illicit flows and criminal things: states, borders, and the other side of globalization*, Indiana University Press, Tracking globalization, 2005, p. 4. Delmas-Marty names it the "*society of the permanent gaze*," M. Delmas-Marty, *Résister, responsabiliser, anticiper, ou, Comment humaniser la mondialisation*, Seuil, 2013, p. 84

must be "*balanced by adequate protection of human rights*."[2] However, the international framework to fight human trafficking strengthens criminal repression and states' powers. It pays little attention to the protection of the human rights of those being prosecuted[3] or the realities of prosecution. Indeed, despite the non-punishment principle, many trafficked victims are still prosecuted and convicted of other or similar offenses.[4] Thus, it is of utmost importance to determine the conformity of the state's digital investigation powers to the supranational human rights framework. The ECHR, in particular, developed extensive case law on investigative techniques,[5] which should be evaluated on both the bases of the right to privacy (I) and of a fair trial (II).

I. The state's digital legitimate coercion powers and the right to privacy

204. Interference with privacy. The ECHR developed a challenging case law on how to regulate investigative techniques, especially digital ones,[6] that interfere with Article 8 of the CPHR regarding the right to a private life, or privacy. The court expanded the concept of privacy to include any type of data obtained during an investigation,[7] as "*private life is a broad term not susceptible to exhaustive definition*."[8] Therefore, digital investigative techniques interfere with the right to a private life.

---

[2] Association internationale de droit pénal, "XV^{ème} congrès international de droit pénal (Rio de Janeiro, 4 – 10 septembre 1994)," *Revue internationale de droit pénal*, ERES, 2015, vol. 86, no. 2015/1, ¶¶ 16-19

[3] N. Boister, "Human rights protections in the suppression conventions," *Human Rights Law Review*, October 1, 2002, vol. 2, no. 2, pp. 199-227

[4] T. Harré, "Human Traffickers' Fair Trial Rights and Transnational Criminal Law," *Anti-Trafficking Review*, April 19, 2022, no. 18, pp. 159-173

[5] ECHR, *Klass and others v. Germany*, September 6, 1978, no. 5029/71; ECHR, *Malone v. the United Kingdom*, August 2, 1984, no. 8691/79

[6] Mostly interceptions of communications (both by the police and by the intelligence services, as long as they are secret) and geotagging. It must be underlined that the court considers that geotagging and, in general, localization data, are less harmful to the right of privacy in comparison with image or sound data, ECHR, *Uzun v. Germany*, September 2, 2010, no. 35623/05, ¶ 52. Cases involving covert listening devices or video recording were also resolved by case law, ECHR, *Allan v. the United Kingdom*, November 5, 2002, no. 48539/99; ECHR, *P.G. and J.H. v. the United Kingdom*, September 25, 2001, no. 44787/98; ECHR, *Vetter v. France*, May 31, 2005, no. 59842/00; bulk interception of communication, ECHR, *Liberty and others v. the United Kingdom*, July 1, 2008, no. 58243/00; ECHR, *Big Brother Watch and others v. the United Kingdom (1)*, September 13, 2018, 58170/13, 62322/14 and 24960/15; ECHR, *Centrum För Rättvisa v. Sweden (2)*, May 25, 2021, no. 35252/08; disclosure of data by online service providers, ECHR, *Benedik v. Slovenia*, April 24, 2018, no. 62357/14; ECHR, *Ringler v. Austria*, May 12, 2020, no. 2309/10. The court calls those techniques secret surveillance measures. The literature also uses the expression "clandestine" measures, see J.-C. Saint-Pau, "Les investigations numériques et le droit au respect de la vie privée," *Actualité juridique Pénal*, Dalloz, 2017, p. 321

[7] ECHR, *Amann v. Switzerland*, October 18, 2011, no. 27798/95, ¶ 65; ECHR, *Leander v. Sweden*, March 26, 1987, no. 9248/81, ¶ 48

[8] ECHR, *Benedik v. Slovenia*, *op. cit.* note 6, ¶ 100. It should be underlined that the concept of private life includes data obtained in public space, ECHR, *P.G. and J.H.*, *op. cit.* note 6, ¶ 56; ECHR, *Peck v. the United Kingdom*, January 28, 2003, no. 44647/98, ¶ 59

Accordingly, countries should heed this case law and not wait for a conviction to amend it.[9] Such convictions are particularly easy to obtain, as the court broadly interpreted the notion of "*victim*."[10] Indeed, it "*accepts that an individual may […] claim to be the victim of a violation occasioned by the mere existence of secret measures […] without having to allege that such measures were, in fact, applied to him*."[11]

205. To justify the interference,[12] states are required to prove that the technique is "*in accordance with the law*," follows a legitimate aim,[13] and is "*necessary to a democratic society*."[14] The court usually studies national frameworks from the perspective of the first criterion: The law must include specific provisions.[15] These can be divided into three categories: scope of the technique (A), procedure related to the

[9] Like France, which has been convicted many times by the ECHR: ECHR, *Kruslin v. France*, April 24, 1990, no. 11801/85; ECHR, *Huvig v. France*, April 24, 1990, no. 11105/84; ECHR, *Lambert v. France*, August 24, 1998, no. 88/1997/872/1084; ECHR, *Matheron v. France*, March 29, 2005, no. 57752/00; ECHR, *Vetter*, *op. cit.* note 6; ECHR, *Wisse v. France*, December 20, 2005, no. 71611/01; ECHR, *Ben Faiza v. France*, February 8, 2018, no. 31446/12. See also J.-P. Marguénaud, "La réécriture du droit criminel français sous la dictée de la cour européenne des droits de l'homme," *in* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 936. It must be underlined that the right to privacy is not similarly translated under the Spanish framework. The Spanish Constitución, Article 18, protects the right to personal and family intimacy. Consequently, originally, authors would distinguish between this right, "*aimed at protecting the individual against any invasion of their personal and family life*," and data protection, which "*aim[s] to guarantee the individual a power of control or disposition over their personal data, its use and destination, with the purpose of preventing its unlawful trade and detrimental to their dignity and right*," V.L. Gutiérrez Castillo, "Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa," *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, Facultad de Derecho, 2005, no. 3, p. 32. While the Tribunal Constitucional first acknowledged data protection through the right of intimacy, Tribunal Constitucional, July 20, 1993, no. 254/1993; it then disconnected it from it to assess it as an independent fundamental right, Tribunal Constitucional, November 30, 2000, no. 292/2000

[10] Article 34 of the CPHR

[11] ECHR, *Klass*, *op. cit.* note 5, ¶ 34. Precisely, the court will, to consider a person as a victim, will study "*the availability of any remedies at the national level and the risk of secret surveillance measures being applied to*" that person, ECHR, *Kennedy v. the United Kingdom*, May 18, 2010, no. 26839/05, p. 124

[12] Article 8.2 of the CPHR

[13] This criterion is not usually developed as those techniques aim at "*the prevention of disorder or crime*."

[14] In its first cases, the court relied on the criterion of "*necessary to a democratic society*," see ECHR, *Klass*, *op. cit.* note 5; ECHR, *Weber and Saravia v. Germany*, June 29, 2006, no. 54934/00. However, in the development of its case law, the requirements mentioned within the third criterion have moved to the one related to the quality of the law. For a clear merging of those two criteria, see ECHR, *Roman Zakharov v. Russia*, December 4, 2015, no. 47143/06, ¶ 236

[15] First, the court considers if there is a legal basis for the law, then its accessibility, and finally its foreseeability, which is the point that is the most developed, ECHR, *Kruslin*, *op. cit.* note 9, ¶ 27; ECHR, *Kopp v. Switzerland*, March 25, 1998, no. 13/1997/797/1000, ¶ 55. Regarding accessibility, French authors have criticized the poor redaction quality of the texts on digital investigative techniques and their instability due to a large number of amendments, E. De Marco, "La captation des données," *in* K. Blay-Grabarczyk et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection "Colloques & Essais" no. 44, 2017, pp. 99-100; C. Lazerges, "Dédoublement de la procédure pénale et garantie des droits fondamentaux," *in* B. Bouloc, F. Alt-Maes (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, p. 589

technique (B), and protection of the data obtained (C).

A. Scope of the technique

206. First, the law must regulate the scope of digital investigative techniques. It should develop the personal scope, potentially meaning affected (1); the material scope, regarding the nature of offenses (2); and the temporal scope, or duration (3).[16]

1. Personal scope

207. Defining personal scope. The personal scope of investigative techniques considers the people who may be the targets of the measures. The main category is investigated persons, which is very clear in Spanish legislation on communications interception;[17] by contrast, the categories of persons affected by a computer search in France are quite broad.[18] However, most of the national frameworks do not define the personal scope of the techniques, particularly for interception of communications,[19] geotagging,[20] the use of drones,[21] and remote access to correspondences[22] in France[23], as well as geotagging[24] in Spain and any electronic surveillance measure in

[16] ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶ 249; ECHR, *Huvig*, *op. cit.* note 9, ¶ 34; ECHR, *Valenzuela Contreras v. Spain*, July 30, 1998, no. 58/1997/842/1048, ¶ 46; ECHR, *Weber and Saravia*, *op. cit.* note 14, ¶ 95; ECHR, *Amann*, *op. cit.* note 7, ¶¶ 56-58; ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶¶ 243, 250. Such limits are consistent with the prohibition on "*general and indiscriminate retention*" of data developed by the CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen*, December 21, 2016, C-203/15 and C-698/15

[17] The intercepted devices "*must be those habitually or occasionally used by the person under investigation*," Article 588 ter b.1 of the Ley de Enjuiciamiento Criminal. For a similar provision for audio recording, see Article 588 quater a. Third parties' devices can only be intercepted if "*(1) there is evidence that the person under investigation uses it to transmit or receive information; or (2) the holder collaborates with the person under investigation*," Article 588 ter c. The law extends the measure to the victim's device in cases of "*serious risk to their life or integrity*," Article 588 ter b.2 ¶2. Similarly, in France, the provision on cyber infiltration explicitly mentions investigated persons, but the technique is not limited to them, Article 230-46.1° of the Code de procédure pénale.

[18] A search can be authorized against any "*persons who appear to have participated in the crime or to be in possession of documents, information, or objects relating to the incriminated acts*," Article 56 ¶1 of the Code de procédure pénale

[19] Article 100 of the Code de procédure pénale, as supplemented by case law, emphasizes that the persons affected by the measure do not have to be "*only those on whom there are clues of culpability*," Cour de Cassation, Chambre criminelle, July 17, 1990, no. 90-82614; Cour de Cassation, Chambre criminelle, November 26, 1990, no. 90-84590; Cour de Cassation, Chambre criminelle, December 9, 1991, no. 88-80786, 90-84994

[20] Article 230-32 of the Code de procédure pénale

[21] Article 230-47 of the Code de procédure pénale

[22] Article 706-95-1 of the Code de procédure pénale mentions only the "*targeted person*."

[23] The personal scope of computer searches is also criticized for not being limited to the suspected person or to "*data to which the suspected person has access when identified on the computer system*," B. Roussel, *Les investigations numériques en procédure pénale*, Thesis, Université de Bordeaux, July 7, 2020, p. 93

[24] Article 588 quinquies b of the Ley de Enjuiciamiento Criminal

Romania.[25] Nevertheless, in Spain,[26] extending digital investigative techniques to third parties by applying the principles of specialty and suitability requires "*a reinforced motivation*"[27] in the authorization. Still, the "dragging collection" of third-party data is accepted when it occurs in an indirect way as it relates to the investigated person[28]. The technological procedures cannot be emptied of their content without affecting the rights of third parties more than proportionally.[29]

208. Restricted personal scope. Nonetheless, the three countries prohibit the techniques from being authorized for specific groups of people.[30] Romania imposes specific restrictions on all electronic surveillance measures used to monitor lawyers,[31] while Spain considers broader restrictions for searches, including digital ones, in certain private spaces[32] and limitations regarding communications between a lawyer and persons investigated or charged.[33] France provides for an even wider range of restrictive regulations for searches[34] and interception of communications.[35]

209. However, this criterion seems inappropriate for measures that focus on an

[25] Although the person subject to the measure must be mentioned in the authorization, only if known, Article 145.5.f of the Codul de Procedură Penală

[26] Article 588 bis h of the Ley de Enjuiciamiento Criminal

[27] I. López-Barajas Perea, "Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley," *Revista de Derecho Político*, Universidad Nacional de Educacion a Distancia (UNED), 2017, no. 98, p. 112

[28] Fiscalía General del Estado, Circular 1/2019 sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, March 6, 2019, pp. 30073-30074

[29] M. Cedeño Hernán, "Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017

[30] That is also studied by the ECHR, see, for instance, ECHR, *Kopp*, *op. cit.* note 15, ¶ 73; ECHR, *Aalmoes and Others v. the Netherlands*, November 25, 2004, no. 16269/02, p. 24

[31] Article 139.4 of the Codul de Procedură Penală, see also Article 34 of the Legea nr. 51/1995 pentru organizarea și exercitarea profesiei de avocat

[32] Those restrictions of the regime of entry in private spaces regards: the Parliament, Article 548 of the Ley de Enjuiciamiento Criminal; religious places, Article 549; royal places, Articles 555 and 556; representatives of foreign nations, Articles 559 and 560; foreign warships, Article 561; foreign consuls, Article 562. However, all those places are not considered "home searches," while the article on computer search is limited to those situations, Article 588 sexies a.

[33] Articles 118.4 and 520.7 of the Ley de Enjuiciamiento Criminal. However, their location in the code is criticized since it is not connected to the investigative techniques, R. Bellido Penadés, *La captación de comunicaciones orales directas y de imágenes y su uso en el proceso penal (propuestas de reforma)*, Tirant lo Blanch, 2020, pp. 144-145

[34] Regarding lawyers, Article 56-1 of the Code de procédure pénale; media companies, Article 56-2; a doctor, a notary, a court bailiff, Article 56-3 of the Code de procédure pénale; a place with items "*protected by national defense secrecy*," Article 56-4; a "*person exercising jurisdictional functions and which tend to the seizure of documents likely covered by the secrecy of the deliberation*," Article 56-5.

[35] Regarding members of the Parliament, lawyers, and magistrates, Article 100-7 of the Code de procédure pénale. This article is extended to remote access to electronic correspondence, Article 706-95-3, voice and image recording, Article 706-96-1, and legal hacking, Article 706-102-5.

object or device.[36] An evolution of the ECHR's criterion would allow for consideration of the difficulties of the investigation when a device has not yet been linked to a physical person. Still, it is questionable that the personal scope of digital investigative techniques is so blurry, especially considering the potential close connection between traffickers and victims.

2. Material scope

210. Defining material scope. Second, the scope of the measures should define the nature of the offenses that could trigger the authorization of these techniques.[37] As mentioned, states can delimit the material scope through a list of offenses,[38] such as in the Romanian framework,[39] and can define a different threshold to establish the material scope as a level of seriousness for the offense.[40] Almost all digital investigative techniques in the three countries comply with this criterion, except for geotagging in Spain, since the law does not consider its material scope.[41]

211. Material scope and online offenses. However, more doubts arise when techniques define their material scope by using general notions. According to the

[36] For example, in France, geotagging can be used to track any object that is not associated with a person, Article 230-32 of the Code de procédure pénale. The Spanish and Romanian frameworks on computer search focus more on a device than a person, Article 588 sexies a of the Ley de Enjuiciamiento Criminal and Article 168.6.f of the Codul de Procedură Penală. On legal hacking, the French and Spanish provisions do not define the categories of persons that could face such measures, but the authorization should only specify the concerned device, Article 706-102-3 of the Code de procédure pénale and Article 588 septies a.2.a of the Ley de Enjuiciamiento Criminal. In its functioning, the IMSI catcher device does not even focus on a specific device but on a geographical space. Although, in the French regulation, if communications are intercepted, they must be limited to the person or the device specified in the authorization, Article 706-95-20.II of the Code de procédure pénale. Also, see Article 588 ter l of the Ley de Enjuiciamiento Criminal. A similar scope is considered for the recording of images and sounds in the French framework, since the authorization specifies places and not persons, Article 706-97 of the Code de procédure pénale

[37] ECHR, *Kennedy*, *op. cit.* note 11, ¶ 159

[38] It should be underlined that if the list is exhaustive, the ECHR prohibits extending the list by analogy or by case law, ECHR, *Dumitri Popescu v. Romania*, April 26, 2007, no. 71525/01, ¶ 64

[39] Article 139.2 of the Codul de Procedură Penală. See also, for cyber infiltration in Spain, Article 282 bis.4 of the Ley de Enjuiciamiento Criminal; or the lists of offenses for the special investigative techniques in France, Articles 706-73 and 706-73-1 of the Code de procédure pénale.

[40] In that regard, the court usually requires a certain level of gravity, but a very large category of offense does not imply a violation of Article 8. The court criticized the legislation of Russia, where pickpocketing was included in a broad list of offenses allowing interception of communications, ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 244. Such flexibility on the part of the court on that criterion could be highly denounced with regard to the proportionality principle derived from the criterion of "necessary to a democratic society." On the contrary, the court requires a specific level of seriousness of the prevented or prosecuted offenses for bulk investigative techniques, ECHR, *Big Brother Watch (1)*, *op. cit.* note 6, ¶ 386. Also, the case law of the CJEU is more restrictive on that topic, see CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen*, *op. cit.* note 16, ¶ 102; CJEU, *Ministerio Fiscal*, October 2, 2018, C-207/16, ¶ 54.

[41] Article 588 quinquies b of the Ley de Enjuiciamiento Criminal only considers the principles of necessity and proportionality, to be developed in the authorization, Article 588 bis b.2.1° and 2°

ECHR, general terms can be used to delimit the material scope, but only if those terms are defined.[42] The French and Spanish codes use a general concept of offenses committed online.[43] In Spain, the notion results from the jurisprudence of the *Tribunal Supremo*: Serious offenses are considered not only on the basis of their penalty but also on "*the incidence of the use of information technologies*."[44] This concept is not questioned in French literature, but it is criticized in Spanish literature.[45] This material scope, on its own, is considered insufficient to justify the implementation of a technique, but it is necessary to prove "*the greater difficulty of clarifying the offense in the absence of*" it.[46] In particular, the absence of a minimum penalty to complement such a generic term, which is included in France, is criticized.

212. Material scope and organized criminality.[47] Another general notion relates

[42] ECHR, *Big Brother Watch and others v. the United Kingdom (2)*, May 25, 2021, 58170/13, 62322/14 and 24960/15, ¶¶ 368-371. On the contrary, a failure to define the concept implies a violation of Article 8, ECHR, *Iordachi and others v. Moldova*, February 10, 2009, no. 25198/02, ¶ 46

[43] Article 588 ter a of the Ley de Enjuiciamiento Criminal for interception of communications and Article 588 septies a for remote access to correspondence and legal hacking: "*offenses committed by means of computer tools or any other information or communication technology or communication service*." Article 230-46 of the Code de procédure pénale for cyber infiltration, Article 100¶ 3 for interception of communications: offenses "*committed through electronic communications*."

[44] Tribunal Supremo. Sala Segunda, de lo Penal, February 3, 2006, no. 104/2006; C. Sanchís Crespo, "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2017, no. 125, p. 3

[45] F. Bueno de Mata, *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, Aranzadi derecho penal no. 1151, Primera edición, 2019, 2019, p. 193; E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019, p. 542

[46] L. Bachmaier Winter, "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad," *in* M. Cedeño Hernán (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017; I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 164

[47] It is possible to note that even if the Romanian legal framework does not use this notion to delimit the scope of surveillance measures, the offense of establishment of an organized criminal group defines it as: "*a structured group, consisting of three or more persons, constituted for a certain period of time and to act in a coordinated manner for the purpose of committing one or more offenses*," Article 367.6 of the Codul penal. Other offenses, such as human trafficking, do not need to be committed within an organized criminal group to be included within the DIICOT's competence, Article 11 of the Ordonanță de Urgență nr. 78/2016 pentru organizarea și funcționarea Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (DIICOT)

to the concept of "*organized crime group*."[48] In Spain, the notions are clearly defined.[49] However, in France, the notion of "organized group" is less detailed,[50] with no information regarding the number of persons involved, the temporal basis of the group, or the nature of the offenses committed. The notion is thus criticized in the literature.[51] Various criteria—such as a group of individuals related for the purpose of committing the offense, coordinated preparatory acts, or a structured organization—were used by the jurisdictions.[52] Because of the lack of well-defined criteria, the existence or absence of the circumstance is left to the prosecutor[53] and is largely uncontrolled by the *Cour*

[48] This notion is defined at the international level by the Palermo Convention, Article 2: "*a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses […] to obtain, directly or indirectly, a financial or other material benefit*." This definition was then adopted within the Council of Europe, Committee of Ministers, "Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime," Council of Europe, September 19, 2001. The EU definition is almost identical but lowers the threshold of an association of two or more persons, Article 1, Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organized crime

[49] The cyber infiltration technique relies on the notion of "organized crime," defined as: "*the association of three or more persons for the purpose of committing, on a permanent or repeated basis*," an offense, Article 282 bis.4 of the Ley de Enjuiciamiento Criminal. On this definition, see J.L. De la Cuesta, "Organised Crime Control Policies in Spain: A 'Disorganised' Criminal Policy for 'Organised' Crime," *in* C. Fijnaut, L. Paoli (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime no. 4, 1st ed., 2006, pp. 796-797. Interception of communications (Article 588 ter a of the Ley de Enjuiciamiento Criminal in relation with Article 579.1.2°) and audio and image recording (Article 588 quater b.2.a.2°) rely on the notion of "criminal group or organization," defined as: a "*group formed by more than two persons on a stable basis or for an indefinite period of time, who, in a concerted and coordinated manner, shares various tasks or functions for the purpose of committing offenses*," Article 570 bis of the Código penal, introduced by the Ley Orgánica 5/2010. On the recognition of the concept in Spain, see S. Córdoba Moreno, "¿Son las bandas latinas en España crimen organizado?," *in* L. Zúñiga Rodríguez (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, pp. 167-169. Although it can hinder a good understanding of the law to have two very similar notions, they are both well defined. This criticism could be extended to the existence of a third definition of a similar concept, the aggravating circumstance for committing human trafficking, within an organization of more than two people, Article 177 bis.6 of the Código penal. On these three definitions, see M. Cabanes Ferrando, *La trata de seres humanos: concepto desde el marco normativo: una aproximación al delito*, J.M. Bosch Editor, 2022, pp. 254-257

[50] Defined as an aggravating circumstance: "*any grouping formed or any agreement established with a view to the preparation, characterized by one or more material facts, of one or more offenses*," Article 132-71 of the Code pénal, since the Loi n°92-683 portant réforme des dispositions générales du Code pénal. A similar definition is considered for "association de malfaiteurs," Article 450-1.

[51] C. Lazerges, "La dérive de la procédure pénale," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2003, p. 644; E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004," *Actualité juridique Pénal*, Dalloz, 2004, p. 181; T. Godefroy, "The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference," *in* C. Fijnaut, L. Paoli (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime no. 4, 1st ed., 2006, p. 763; C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies," *Revue Le Lamy Droit de l'immatériel*, October 1, 2010, no. 64; C. Lazerges, "Le déclin du droit pénal : l'émergence d'une politique criminelle de l'ennemi," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 649

[52] E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004," *op. cit.* note 51, p. 181

[53] C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies," *op. cit.* note 51

of Cassation.[54] As a result, the notion does not appear to conform to the ECHR's condition of foreseeability. Additionally, the notion is not convincing for many practitioners,[55] who will rely more on the seriousness of the offense than on the complexity of the facts.[56] This is particularly underlined in the investigation of human trafficking,[57] in which this circumstance is far from present in every case, especially since new technologies facilitate the development of individual traffickers.

213. After considering both the personal and material scopes of digital investigative techniques, the ECHR contemplates their temporal scope.

3. Temporal scope

214. Maximal duration. The temporal scope is mainly left to "*the discretion*" of the state,[58] but the law must clearly consider three elements.[59] First, the law is required to define the maximal duration of the digital investigative technique. Indeed, most techniques are temporally limited,[60] but the regulation of searches, including computer

[54] E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004," *op. cit.* note 51, p. 181. However, in 2016, the court seemed to consider two criteria for the notion that "*presupposes the premeditation of the offenses and a structured organization of its members*," Cour de Cassation, Chambre criminelle, June 22, 2016, no. 16-81834

[55] Opinion underlined by prosecutors at the specialized section on organized crime in the Tribunal Judiciaire of Paris; as well as by the doctrine, T. Godefroy, "The Control of Organised Crime in France," *op. cit.* note 51, p. 763

[56] The Conseil Constitutionnel relies on the latter criterion to apply the proportionality principle, for example, when it censored the extension to any criminal offense of all the special investigative techniques within the preliminary investigation, Conseil constitutionnel, *Loi de programmation 2018-2022 et de réforme pour la justice*, March 21, 2019, 2019-778 DC, ¶¶ 161-166. However, it should be underlined that the motivation of the Conseil also relies on the lack of control by the judge of liberties and custody within the flagrancy and preliminary investigation. Therefore, those techniques could be further extended to other offenses (crimes and misdemeanors), without the circumstances of an organized crime group if they were would be controlled by a judge and not a prosecutor. A similar interrogation arises from the censure by the Conseil of the extension of interception of communications to flagrancy and preliminary investigations, which was considered for any offense punishable by a maximum of at least three years of imprisonment, *Ibid.* ¶¶ 138-147

[57] E. Vergès, "La notion de criminalité organisée après la loi du 9 mai 2004," *op. cit.* note 51, p. 181; M. Chawki, *La traite des êtres humains à l'ère numérique*, Éditions de Saint-Amans, 2010, p. 59

[58] ECHR, *Kennedy*, *op. cit.* note 11, ¶ 161, even though the court recognizes that "*The overall duration of any interception measures [should] depend on the complexity and duration of the investigation in question*."

[59] ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 250; ECHR, *Klass*, *op. cit.* note 5, ¶ 52

[60] In Romania, one article considers the same duration for every electronic surveillance technique, which is 30 days, Article 140.1 of the Codul de Procedură Penală. In Spain, in general, the implementation of the technique "*may not exceed the time necessary for the clarification of the facts*," Article 588 bis e.1 of the Ley de Enjuiciamiento Criminal, which has been criticized for being an indefined concept, E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización. Cuando la práctica forense no puede esperar," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 124. The concept is then expanded upon, as legal hacking is limited to one month, Article 588 septies c, interceptions of communication and

searches, does not establish a duration, since such searches do not last in time and intervene in a specific and limited moment. Similarly, in Spain, audio and image recordings are restricted to one particular encounter[61] and do not last in time; a new encounter will need a new authorization.[62] Furthermore, the French technique for remote access to electronic correspondence does not include a time limit. However, it differs from a search: Police officers can technically access such correspondences every day during an undefined period. Furthermore, neither France nor Spain establishes a duration for the cyber-infiltration.[63] Lastly, the ECHR evaluates whether the law mandates the authorization to be limited to a specific duration,[64] which is provided for in the Spanish[65] and Romanian[66] laws. However, in France, such specification is explicitly mentioned only for the interception of communications.[67]

215. Measure renewal. Second, the law must be precise on the temporal limit and

geotagging to three months, Articles 588 ter g and 588 quinquies c. In France, audio and image recording, the IMSI catcher, legal hacking, the use of drones, and the interception of communications are limited to one month within the flagrancy and preliminary investigation and four months within the judicial information, Articles 706-95-16, 706-95, 230-48 and 100-2 of the Code de procédure pénale. As an exception, the IMSI catcher used for interception of communications can only be authorized for 48 hours, Article 706-95-20.II. Geotagging is limited, in the first instance (authorization by the prosecutor), to eight days within the flagrancy and preliminary investigation, or fifteen days if investigating a crime or the listed offenses linked to organized crime, and in the second instance (authorization by the judge of liberties and custody) to one month; and to four months within the judicial information, Article 230-33. As most of the durations are very similar both in Spain and in France, a harmonization could be carried out.

[61] The need to bring evidence that the encounter will happen challenge the implementation of the measure, E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* note 45, pp. 443-444. The use of this concept instead of setting a duration for the technique has been highly criticized by the literature, *Ibid.* p. 442; F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 45, p. 103; R. Bellido Penadés, *La captación de comunicaciones orales directas y de imágenes*, *op. cit.* note 33, p. 109

[62] Article 588 quater e of the Ley de Enjuiciamiento Criminal. This new authorization is needed even when encounters happen in a regular basis, M. Díaz Martínez, "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos," *in* F. Bueno de la Mata, M. Díaz Martínez, I. López-Barajas Perea (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, p. 105

[63] Article 230-46 of the Code de procédure pénale and Article 282 bis.6 of the Ley de Enjuiciamiento Criminal

[64] A criterion that was especially underlined in one of the first ECHR French case law, ECHR, *Kruslin*, *op. cit.* note 9, ¶ 35

[65] Article 588 bis c.3.e of the Ley de Enjuiciamiento Criminal, and on the request form, Article 588 bis b.2.7°

[66] Article 140.5.e of the Codul de Procedură Penală

[67] Article 100-1 of the Code de procédure pénale (and Article 706-95 for the authorization by the judge of liberties and custody). There is no detail on this topic in Articles 706-95-13 and 230-33 (even the circular on geotagging does not consider it, Ministère de la Justice, Circulaire du de présentation de la loi n°2014-372 relative à la géolocalisation, April 1, 2014). One decision of the Cour de cassation considered that "*The duration for which the measure is authorized constitutes an essential guarantee against the risk of a disproportionate infringement of the right to privacy*," Cour de Cassation, Chambre criminelle, January 9, 2018, no. 17-82946. As no other decision appears on that topic, it is not possible

the reasons for the renewal(s).[68] In Romania and in Spain,[69] the renewal must be justified by both the soliciting organ and the authorizing organ,[70] and the laws establish maximal durations, including renewals.[71] Usually,[72] in France, techniques implemented during the flagrancy and preliminary investigation can be renewed once;[73] during the judicial information, the code considers a maximal total duration.[74] The maximal duration set in France and in Spain, up to 18 months or two years, has been criticized in the literature as disproportional,[75] calling into question its compliance with ECHR standards.

216. Measure cancellation. Finally, the digital investigative technique should be allowed to be canceled at any time, especially if the reasons for its authorization disappear. This is explicitly mentioned in the Spanish and Romanian codes.[76] On the contrary, the French[77] code does not consider the possibility of canceling the measure before its termination.

217. Therefore, the French criminal procedure framework appears to be particularly questionable regarding the case law of the ECHR on the temporal scope of digital

---

to consider that the case law makes this criterion foreseeable. As no other decision appears on that topic, it is not possible to consider that the case law makes this criterion foreseeable.

[68] ECHR, *Szabó and Vissy v. Hungary*, January 12, 2016, no. 37138/14, ¶ 74

[69] It should be noted that the computation of deadlines posed a problem of interpretation in Spain. It was questioned whether the time limit of the technique began on the day of its authorization or on the day of its effective start (after the implementation of the devices, for example). Both the Tribunal Constitucional and the Tribunal Supremo decided for the former option, Tribunal Constitucional, July 18, 2005, no. 205/2005; Tribunal Supremo. Sala Segunda, de lo Penal, January 22, 2014, no. 7/2014. For an opposite opinion, see F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 45, pp. 79-80

[70] Article 144.1 of the Codul de Procedură Penală; Articles 588 bis e.2 and 3 and 588 bis f of the Ley de Enjuiciamiento Criminal

[71] In Romania, the maximal duration is six months for all techniques, Article 144.3 of the Codul de Procedură Penală. In Spain, 18 months for interception of communications and geotagging, Articles 588 ter g and 588 quinquies c of the Ley de Enjuiciamiento Criminal; three months for legal hacking, Article 588 septies c

[72] Geotagging is limited to one or two years in the case of investigating organized crime, Article 230-33 of the Code de procédure pénale; and the use of the IMSI catcher for intercepting communications can only be renewed once, Article 706-95-20.II. As the code does not regulate the duration of remote access to electronic correspondence, it also does not regulate the renewal of the measure.

[73] See Articles 230-33.1°, 230-48.1°, 706-95-16.1° and 706-95 of the Code de procédure pénale

[74] Two years for audio and image recording, IMSI catcher, and legal hacking, Article 706-95-16 of the Code de procédure pénale, and for the use of drones, Article 230-48.2°; one or two years in the case of investigating organized crime for interception of communications, Article 100-2.

[75] E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización," *op. cit.* note 60, p. 134; F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 45, pp. 61, 149

[76] Articles 588 bis e.1 and 588 bis j of the Ley de Enjuiciamiento Criminal; Article 142.4 of the Codul de Procedură Penală, but the termination of the measure comes from the prosecutor and not the judge.

[77] Except for audio and image recording, IMSI catcher, and legal hacking, the authorizing organ can stop the measure at any moment, but the article does not detail why, Article 706-95-14 of the Code de procédure pénale

investigative techniques. The ECHR has developed further criteria regarding its procedure.

B. Procedure of the technique

218. Next, the law must detail the modalities of the procedure and the organs that control the digital investigative techniques.[78] Usually, the court focuses on the initial control (1), then groups the ongoing and *a posteriori* controls (2).[79]

1. A priori control

219. Reviewing organ. Although the ECHR highlighted that the organ authorizing the technique is not required to be a judge,[80] it must be independent.[81] In France and Romania, prosecutors are not judicial authorities for the ECHR's standards,[82] and today, most digital investigative techniques are authorized by a judge.[83] However, doubts remain. In cases of emergency, French and Spanish police officers can implement geotagging devices;[84] in Romania, the prosecutor can authorize any surveillance measure for 48 hours;[85] and in Spain, no authorization is required for remote access to and legal hacking of electronic devices,[86] and interception of communications can be authorized by the executive branch to investigate armed

[78] ECHR, *Roman Zakharov*, *op. cit.* note 14, p. 257
[79] ECHR, *Klass*, *op. cit.* note 5, ¶ 55
[80] Although, it is deemed very important in the literature, see P. Beauvais, "La nouvelle surveillance pénale," *in* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 273
[81] For example, for a non-judicial supervisory body see ECHR, *Weber and Saravia*, *op. cit.* note 14, ¶ 117. On the contrary, the ECHR considers that a reviewing body of a political nature violates Article 8, see ECHR, *Szabó and Vissy*, *op. cit.* note 68, ¶¶ 75-76.
[82] For France, see ECHR, *Moulin v. France*, November 23, 2010, no. 37104/06, ¶ 59; for Romania, see ECHR, *Vasilescu v. Romania*, May 22, 1998, no. 53/1997/837/1043, ¶¶ 40-41; ECHR, *Dumitri Popescu*, *op. cit.* note 38, ¶ 71. For example, in France, on geotagging, the case law of the Cour de Cassation had to evolve. First, the court agreed to the possibility for a prosecutor to authorize geotagging, Cour de Cassation, Chambre criminelle, November 22, 2011, no. 11-84308. Two years later, the court orders that the authorization be granted by an independent magistrate, rather than a prosecutor, Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81949; Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81945. No decision on this topic has been found for the Spanish prosecutor, although the literature also criticizes its lack of independence, F. Bueno de Mata, *Las diligencias de investigación penal*, *op. cit.* note 45, p. 30
[83] Judge of liberties and custody or judge of instruction in France; judge of rights and liberties in Romania; judge of instruction in Spain (even if some articles do not explicitly mention the judge, they mention a "judicial resolution," for example, Article 588 quater a of the Ley de Enjuiciamiento Criminal)
[84] Measure to be confirmed by the magistrate within 24 hours, Article 230-35 of the Code de procédure pénale. In the Spanish framework, Article 588 quinquies b.4 of the Ley de Enjuiciamiento Criminal
[85] Within 24 hours after the termination of the measure, the prosecutor must refer it to the judge of rights and liberties, who will then must confirm it within 24 hours, Article 141 of the Codul de Procedură Penală
[86] Article 588 sexies c.4 of the Ley de Enjuiciamiento Criminal

gangs or terrorist offenses.[87] These procedures could be deemed proportionate and necessary for the prosecution of offenses, but the lack of required elements to consider the situation an emergency is heavily criticized.[88] Other procedures could face the censorship of the ECHR:[89] Spain does not require any authorization to use an IMSI catcher,[90] and in France, geotagging is always authorized by the prosecutor for the first days.[91]

220. The scope of the review. This reviewing organ classically evaluates the material, personal, and temporal scopes. In France, the content of the authorizations is very broadly regulated,[92] but in Spain[93] and Romania,[94] the law details the specific content of the document. In general, the authorizations rely on several broad principles. The Spanish framework considers the principles of specialty, suitability, exceptionality and necessity, and proportionality, in an effort to consider "*all the circumstances of the case and the sacrifice of the rights and interests affected so that it does not outweigh the benefits*."[95] In Romania, the code also recognizes the principles of exceptionality

[87] Artículo 588 ter d.3 de la LECrim

[88] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática*, *op. cit.* note 45, pp. 423-427; E. Gómez Soler, "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización," *op. cit.* note 60, p. 134; I. López-Barajas Perea, "El derecho a la protección del entorno virtual y sus límites," *op. cit.* note 46, pp. 142-143; C. Sanchís Crespo, "Puesta al día de la instrucción penal," *op. cit.* note 44, p. 5. It is also criticized because the case law appears to broaden the cases of urgency to include other digital investigative techniques, Tribunal Supremo. Sala Segunda, de lo Penal, April 20, 2016, no. 329/2016

[89] However, such censorship is not flagrant, since the ECHR usually considers the legal framework as a whole, taking other safeguards into account, if one of the criteria is not fully conforming.

[90] The control is only posterior, according to Article 588 ter of the Ley de Enjuiciamiento Criminal, when the investigators request an interception of communications based on the obtained data.

[91] Eight days in general, 15 days when investigating organized crime, Article 230-33 of the Code de procédure pénale

[92] Except for the interception of communications, since Article 100-1 of the Code de procédure pénale develops some of the elements that should be included; and for legal hacking, Article 706-102-3. For a criticism on the latter, see E. De Marco, "La captation des données," *op. cit.* note 15, p. 103. Articles 230-33 and 706-95-13 of the Code de procédure pénale require that the motivation be based on legal and material facts. The code only mentions the need to motivate the authorization without reference to legal and material facts, Article 706-95-1. However, for audio recording, the Cour de Cassation already asked for more detailed authorizations, Cour de Cassation, Chambre criminelle, January 6, 2015, no. 14-85448; T. Meindl, "Fascicule 20 : Procédure applicable à la criminalité et la délinquance organisées – Poursuite. Instruction. Jugement. Assistants spécialisés – Dispositions dérogatoires de procédure – Articles 706-73 à 706-106," *JurisClasseur Procédure pénale*, LexisNexis, January 31, 2020, ¶ 59; P. Collet, "Le renforcement progressif des garanties applicables à deux mesures intrusives : la géolocalisation et la sonorisation," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2021, p. 29. On the contrary, Saint-Pau considers that the principles of necessity and proportionality are indeed required, but he defines the first one as the need that be issued within a criminal procedure, which does not conform to the other definitions of this principle, J.-C. Saint-Pau, "Les investigations numériques et le droit au respect de la vie privée," *op. cit.* note 6, p. 321

[93] Article 588 bis c of the Ley de Enjuiciamiento Criminal

[94] Article 140.5 of the Codul de Procedură Penală

[95] Article 588 bis a of the Ley de Enjuiciamiento Criminal. Regarding the principle of proportionality, the law provides guidelines, meaning that the judge must consider "*the seriousness of the act, its social*

and proportionality.[96] Thus, the Spanish and Romanian procedures are more foreseeable.

221. Entering closed spaces. Finally, the ECHR also verifies that the procedure provides for a specific authorization to enter closed spaces, especially to install technical devices.[97] In Romania, an additional authorization is needed for entering private spaces for video, audio, or photo surveillance, but no similar provision is included for other measures, such as geotagging.[98] Similarly, in Spain, the installation of audio recording devices in private spaces requires explicit authorization,[99] but no measures are needed for geotagging and for legal hacking. On the contrary, in France, specific authorizations for the installation of technical devices are provided for every technique.[100]

222. However, *a priori* control is insufficient to comprehensively supervise digital investigative techniques. As a result, the ECHR examines additional control criteria.

2. A posteriori control

223. Controlling implementation. First, the implementation of the measure must be supervised.[101] Regarding the supervising organ, in Spain, the judge of instruction establishes the form and frequency of the information by police agents, and such control takes place in any case at the end of the measure.[102] By contrast, in Romania, the supervision of the techniques is handled by the prosecutor, who informs the judge only at the termination of the measure,[103] which could be deemed not to conform to the ECHR's standards. In France,[104] for every technique, the code underlines that the authorizing judge controls the measure.[105] Regarding the tools provided for the

signification or the technological scope of commission, the intensity of the existing evidence and the relevance of the intended result."

[96] Article 139.1.b and c of the Codul de Procedură Penală

[97] ECHR, *Vetter*, *op. cit.* note 6, ¶ 27

[98] Article 140.2 of the Codul de Procedură Penală

[99] Article 588 quater a of the Ley de Enjuiciamiento Criminal

[100] Geotagging, Article 230-34 of the Code de procédure pénale; audio and image recording, Article 706-96-1; and legal hacking, Article 706-102-5.

[101] ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 238; ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶ 249

[102] Article 588 bis g of the Ley de Enjuiciamiento Criminal; the provision is detailed for the interception of communications, Article 588 ter f, and for audio and image recording, Article 588 quater d.

[103] Article 143.5 of the Codul de Procedură Penală

[104] In general, the judge of instruction must check all the obtained data, Article 81¶5 of the Code de procédure pénale, and the preliminary investigation is controlled by the prosecutor, Article 75¶2

[105] IMSI catcher, audio and image recording, legal hacking, Article 706-95-14¶1 of the Code de procédure pénale; interception of communications, Articles 100¶1 and 706-95¶1; access to stored data,

supervision of the techniques, the ECHR particularly studies the keeping of records of the operations,[106] and these recordings are highly detailed in Romanian legislation.[107] In Spain, records are only indirectly required for some techniques[108] but not for the use of the IMSI catcher or legal hacking.[109] In France, records are requested for almost every technique[110] with the exception of remote access to electronic correspondence.[111]

224. Notifying the measure. Second, the notification is a highly relevant factor for the control of the measure.[112] In Romania, the prosecutor must notify the affected person,[113] but in Spain, the secrecy of digital investigative techniques is automatic.[114] In general, secrecy is terminated at least 10 days before the end of the investigation.[115] Specifically for interception of communications,[116] the code provides for the disclosure of information to the parties, and the notification of other affected persons.[117] In France,

---

Article 706-95-3¶1; geotagging, Article 230-37. However, the latter provision does not specify who controls the measure when it is only authorized by the prosecutor, meaning there could be no judicial prior or ongoing review.

[106] ECHR, *Kennedy*, *op. cit.* note 11, ¶ 165; ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 272

[107] Article 143.1 to 4 of the Codul de Procedură Penală

[108] Interception of communications, Article 588 ter f of the Ley de Enjuiciamiento Criminal, *in fine*; audio and image recording, Article 588 quater d, *in fine*; geotagging, Article 588 quinquies c, *in fine*

[109] The legal regime of searches in private spaces also considers the need to record the operation, Article 572 of the Ley de Enjuiciamiento Criminal, but it is not explicit if it applies to computer searches.

[110] Interception of communications, Articles 100-4 and Article 100-5 of the Code de procédure pénale; geotagging, Articles 230-38 and 230-39; searches, Article 56; audio and image recording, IMSI catcher and legal hacking, Article 706-95-18.

[111] Articles 706-95-1 and 706-95-2 of the Code de procédure pénale

[112] ECHR, *Klass*, *op. cit.* note 5, ¶ 57; alternatively, for intelligence measures, the ECHR requires the possibility to file a complaint with the courts without the need of notification if a person suspects an infringement of their right to privacy (in particular the interception of their communications), ECHR, *Kennedy*, *op. cit.* note 11, ¶ 167. The court also recognized the need to postpone the notification until it does not hinder the effectivity of the measure, ECHR, *Klass*, *op. cit.* note 5, ¶ 58

[113] The notification must take place within ten days at the termination of the measure, or "*at the latest until the end of the criminal investigation or until the case is closed*" only in specific delicate cases, Article 145 of the Codul de Procedură Penală. This notification is intended for all affected parties, not just the defendant: the code was amended in this regard following the Curtea Constituţională, *Decizia referitoare la excepția de neconstituționalitate a dispozițiilor art. 145 din Codul de procedură penală*, April 6, 2017, no. 244/2017

[114] Article 588 bis d of the Ley de Enjuiciamiento Criminal

[115] Article 302 of the Ley de Enjuiciamiento Criminal

[116] Article 588 ter i of the Ley de Enjuiciamiento Criminal

[117] "*Unless it is impossible, [if it] would require a disproportionate effort or would be detrimental to future investigations*," Article 588 ter i.3 of the Ley de Enjuiciamiento Criminal. This exception has been highly criticized, A. Rodríguez Álvarez, "Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal," *in* J.M. Asencio Mellado, M. Fernández López (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1st ed., 2017, p. 175. Other techniques, on the other hand, can infringe on the right to privacy of people who are not involved in the criminal process. Thus, it is considered that, although not explicitly provided for, this concept should be applied to voice and image recording, M. Díaz Martínez, "La captación y grabación de comunicaciones orales," *op. cit.* note 62, p. 111, especially since it was required by the case law prior

in general, the investigation is secret,[118] and the files of the case will be open to consultation by the parties once the investigation is closed.[119] Therefore, there is no provision regarding the notification of third parties or a notification prior to the end of the investigation.[120,121]

225. As elements of non-conformity to the ECHR's standards arise from the study of the scope and supervision of digital investigative techniques available to prosecute cyber trafficking, the law also must consider the protection of obtained data.

C. Protection of obtained data

226. Processing data. Finally, the ECHR provides various criteria regarding the protection of the obtained personal data. First, the state should have in place a law regarding the protection of personal data in the framework of enforcement activities.[122] This topic has been harmonized in the EU by the Directive 2016/680,[123] which has

to the 2015 reform, Fiscalía General del Estado, Circular 2/2019 sobre interceptación de comunicaciones telefónicas y telemáticas, March 6, 2019, p. 30109. Bellido Penadés still advocates for the introduction of a similar concept as in for the interception of communications, R. Bellido Penadés, *La captación de comunicaciones orales directas y de imágenes*, *op. cit.* note 33, p. 143

[118] Article 11 of the Code de procédure pénale. Increased secrecy is considered for geotagging to protect the victim, with a specific regime for the suspected person to litigate, Articles 230-40 and 230-41

[119] B. Bouloc, G. Stefani, G. Levasseur, *Procédure pénale*, Dalloz, Précis, 27th ed., 2020, ¶¶ 819-820

[120] Particularly criticized for legal hacking and distance access to electronic correspondence, see O. Décima, "Terreur et métamorphose À propos de la loi n° 2016-731 du 3 juin 2016 sur la lutte contre le terrorisme," *Recueil Dalloz*, Dalloz, 2016, no. 31, p. 1826

[121] Also, the remedies offered by the law within an already ongoing criminal investigation are not usually studied by the ECHR. It is a topic closely linked to Article 13. Of the 38 cases studied, 15 were based on both Articles 8 and 13. The court sometimes relies on the study of this criterion derived from Article 8 to not check the conformity to Article 13, ECHR, *Malone*, *op. cit.* note 5, ¶ 91; ECHR, *Liberty and others*, *op. cit.* note 6, ¶ 73; ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶ 376. Although it is not included within the scope of the study, it should be underlined that all the Spanish and Romanian authorizations and most of the French authorizations regarding digital investigative techniques are not open to plea. In Spain, to be open to appeal, the law must provide it explicitly, Article 217 of the Ley de Enjuiciamiento Criminal, which the code does not do for digital investigative techniques. In Romania, see Article 140.7 of the Codul de Procedură Penală. However, the legality of the administration of such evidence as well as the legality of the authorization of those techniques may be censored in the preliminary chamber phase, Article 342. In France: interceptions of communications, Article 100¶2 of the Code de procédure pénale; geotagging, Article 230-33¶3; IMSI catcher, audio and video recording, and legal hacking, Article 706-95-13. On the contrary, decisions to grant access to stored data are not deemed non-jurisdictional, so the prosecutor could appeal them, Articles 706-95-1 to 706-95-3 in relation to Article 185. As a result, the remedies will only be available after the technique has been implemented in relation to the notification, as criticized in the literature by M. Touillier, "Les droits de la défense dans les procédures d'exception : une évolution « vent dessus, vent dedans »," *Actualité juridique Pénal*, Dalloz, 2016, p. 119. It is less problematic in the Romanian framework thanks to the comprehensive regime of notification.

[122] ECHR, *Liberty and others*, *op. cit.* note 6, ¶ 69; ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶ 312

[123] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties

been transposed by both France[124] and Romania.[125] However, Spain published its transposition[126] a few months after its conviction by the CJEU for the lack of transposition.[127] This law must specify the procedure for data processing,[128] especially that the quality of data should be checked and that the storage should be secured. The French,[129] Spanish,[130] and Romanian[131] laws consider both. Moreover, the law should regulate the use of data, especially for other purposes, and its communication to other parties;[132] this point is considered by the three national frameworks.[133] Lastly, non-relevant data should be erased, and the data should not be used in another procedure.[134] In Romania, non-relevant data are first archived and then erased one year after the settlement of the case;[135] in Spain, their erasure is not regulated, as in France,[136] although the data recorded should be "*useful for the manifestation of the truth*,"[137] so it is supposed to be a selection of relevant data. In Romania, data can be used to investigate offenses in the material scope of electronic surveillance

[124] Articles 87 to 114, of the Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, by modification of the Loi n°2018-493 relative à la protection des données personnelles

[125] Lege 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date

[126] Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

[127] CJEU, *European Commission v. Kingdom of Spain*, February 25, 2021, C-658/19

[128] The court sees those criteria closely linked to the obligation to keep records of the operations, ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶¶ 310-311

[129] Articles 4.4° and 6°, 97 and 99 or the Loi n°78-17

[130] Articles 10 and 37 of the Ley Orgánica 7/2021

[131] Articles 5.1.d and f, 7.4 and 35 of the Lege 363/2018. Moreover, the criminal procedure code includes the possibility of relying on an electronic signature to check the integrity of the data, Article 142^1 of the Codul de Procedură Penală. Specific provisions are also considered for the preservation of data depending on the result of the procedure, Article 146.

[132] ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 231 Indeed, as a principle, the "*knowledge and documents thereby obtained may not be used for other ends*," ECHR, *Klass*, *op. cit.* note 5, ¶ 52.

[133] Article 91 of the Loi n°78-17, although the article is limited to the transfer of data for other purposes, and not, for example, to other law enforcement authorities for the same general purpose of repressing offenses; Article 9 of the Lege 363/2018; Article 11 of the Ley Orgánica 15/1999 in a very broad manner. In that regard, it should be noted that the regulation of internal transfers is much simpler than the framework for international transfers. The court also considers the sharing of data with other countries, but the international cooperation framework will be studied later on, ECHR, *Centrum För Rättvisa (2)*, *op. cit.* note 6, ¶ 318; see *infra* 247 to 254.

[134] ECHR, *Liberty and others*, *op. cit.* note 6, ¶ 65

[135] Article 142.6 of the Codul de Procedură Penală

[136] Specific provisions exist when data is transmitted through the Plateforme nationale des interceptions judiciaires (PNIJ), see Articles R40-42 to R40-56 of the Code de procédure pénale

[137] Interception of communications, Article 100-5 of the Code de procédure pénale; geotagging, Article 230-39; audio and image recording, IMSI catcher, and legal hacking, Article 706-95-18, that specifies that "*No record of private life unrelated to the offenses referred to in the authorization orders may be kept in the file of the proceedings*" (this provision could have been extended to all the digital investigative techniques). No similar provision is considered for access to stored electronic correspondence.

techniques[138], and in Spain, with judicial authorization.[139] These data are not regulated in France.[140]

227. Erasing data. Finally, the most important criterion for the ECHR is "*the circumstances in which recordings may or must be erased*."[141] In general, Romanian law does not consider data erasure.[142] On the contrary, in Spain, the destruction of original data is mandatory following completion of a case, upon order of the tribunal, and, for the copies, five years "*after the sentence has been executed or when the crime or sentence is prescribed*."[143] In France, the destruction of data must be requested by the prosecutor at the end of the delay in the prescription of public action.[144] However, no provision on that topic exists for remote access to electronic correspondence.[145]

228. In light of ECHR case law on the right to privacy, the regimes of digital investigative techniques appear unstable. Each national law does not conform to all criteria for all techniques. Digital investigative techniques could be used to strengthen the prosecution of cyber trafficking, but such instability makes the law enforcement authorities unadventurous. Moreover, those techniques meet the criteria of Article 6 of the CPHR.

---

[138] Article 142.5 of the Codul de Procedură Penală

[139] Articles 588 bis i and 579 bis of the Ley de Enjuiciamiento Criminal

[140] The code only specifies, for certain techniques, that the discovery of other offenses does not nullify the technique: geotagging, Article 230-37 of the Code de procédure pénale; audio and image recording, IMSI catcher, and legal hacking, Article 706-95-14; and access to stored electronic correspondence, Article 706-95-3. On the contrary, the techniques "*may not, upon penalty of being declared null and void, have any purpose other than the investigation and establishment of the offenses referred to in the*" authorization, access to stored electronic correspondence (Article 706-95-3), audio and image recording, IMSI catcher, and legal hacking (Article 706-95-14). The lack of consistency in the code on this topic is particularly flagrant.

[141] ECHR, *Roman Zakharov*, *op. cit.* note 14, ¶ 231. Precisely, they should be erased "*as soon as they are no longer needed to achieve the required purpose*," ECHR, *Klass*, *op. cit.* note 5, ¶ 52

[142] It is only considered in the case of non-relevant data, Article 142.6 of the Codul de Procedură Penală; when it concerns the relations between the lawyer and the suspect, Article 139.4; or when the technique is declared void after a prosecutor's authorization, Article 141.6. However, the concerned person can request the destruction of data based on Article 13.e of the Lege 363/2018, although no specific article is dedicated to such action.

[143] Except if the court considers it necessary to preserve the data. In this situation, there is no time limit, see Article 588 bis k of the Ley de Enjuiciamiento Criminal

[144] Interception of communications, Article 100-6 of the Code de procédure pénale; geotagging, Article 230-43; Audio and image recording, IMSI catcher, and legal hacking, Article 706-95-19. Guerrier has criticized the fact that the destruction is not dependent on the outcome of the procedure, C. Guerrier, "« Loppsi 2 » et l'utilisation des nouvelles technologies," *op. cit.* note 51

[145] Nevertheless, in general, the person concerned can request the destruction of the data based on Article 106.I.4° of the Loi n°78-17

II. The state's digital legitimate coercion powers and the right to a fair trial

229. The requirement of effectiveness in law enforcement authorities' actions sometimes results in unlawful operations.[146] Conviction of such practices is necessary to protect the rule of law.[147] As a result, the ECHR considers whether a fair trial occurred[148] (A), and the French[149] *Cour de Cassation* examines the loyalty of proof[150] (B).

A. Entrapment in the ECHR case law

230. Notion of entrapment. According to the ECHR, the right to a fair trial is

---

[146] P. Maistre du Chambon, "La régularité des « provocations policières » : l'évolution de la jurisprudence," *La Semaine Juridique Edition Générale*, LexisNexis, December 27, 1989, no. 51, ¶ 3

[147] Indeed, "*The public interest cannot justify the use of evidence obtained as a result of police incitement, as to do so would expose the accused to the risk of being definitively deprived of a fair trial from the outset*," ECHR, *Ramanauskas v. Lithuania (1)*, February 5, 2008, no. 74420/01, ¶ 54. This limit is particularly important when the evidence is used for conviction, ECHR, *Teixeira de Castro v. Portugal*, June 9, 1998, no. 44/1997/828/1034, ¶ 35, *in fine*

[148] Article 6 of the CPHR. However, the "*rules on the admissibility of evidence [are] primarily a matter for regulation under national law*," ECHR, *Schenk v. Switzerland*, July 12, 1988, no. 10862/84, ¶ 46

[149] The problem does not appear to be discussed in Romania, because Article 101 of the Codul de Procedură Penală expressly prohibits the provocation of crime, and case law of the Înalta Curte de Casaţie şi Justiţie relies on ECHR criteria, Înalta Curte de Casaţie şi Justiţie - Secţia Penală, February 18, 2010, no. 626/2010; see B. Micu, "Reflection of the Principle of Loyalty in Matters regarding the Adduction of Evidence in the Romanian Criminal Proceedings," *Lex ET Scientia International Journal*, 2015, vol. 22, no. 1, pp. 166-174. In Spain, "*Jurisprudence already makes a clear distinction […] between provocation of a crime and police provocation*," J.L. De la Cuesta, "Organised Crime Control Policies in Spain," *op. cit.* note 49, p. 809. Regarding infiltration, the code explicitly prohibits the provocation, Article 282 bis.5 of the Ley de Enjuiciamiento Criminal. In particular, entrapment is made of three elements: "*1. A subjective element constituted by a deceitful incitement to commit a crime by the agent to those who are not determined to commit a crime. 2. An objective element, consisting of the arrest of the provoked subject who commits the induced crime. 3. A material element consisting of the non-existence of any risk to the protected legal right and, as a consequence, the atypical nature of such action*," F. Harbottle Quirós, "El agente encubierto informático: Reflexiones a partir de la experiencia española," *Revista Judicial, Poder Judicial de Costa Rica*, 2021, no. 131, pp. 126-128. For a summary of the differences between undercover agent and entrapment, see Tribunal Supremo. Sala Segunda, de lo Penal, February 7, 2019, no. 65/2019. For an example prohibiting fishing techniques to detect human trafficking, see Tribunal Supremo. Sala Segunda, de lo Penal, November 13, 2019, no. 554/2019. When sharing illicit files, entrapment is frequently mentioned, A. Valiño Ces, "El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil," *in* F. Bueno de Mata (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, p. 284. Simply explained, judicial authorization is thought to make it possible to rule out the possibility of entrapment in all cases, B. Rizo Gómez, "La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica," *in* J.M. Asencio Mellado, M. Fernández López (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1st ed., 2017, p. 118. However, some scholars are in favor of the regulation of this topic in the Ley de Enjuiciamiento Criminal, R. Bellido Penadés, *La captación de comunicaciones orales directas y de imágenes*, *op. cit.* note 33, pp. 133-140

[150] Cour de Cassation, Chambre criminelle, September 15, 1999, no. 98-87624; Cour de Cassation, Chambre criminelle, February 7, 2006, no. 05-81888; Cour de Cassation, Chambre criminelle, April 24, 2007, no. 06-87656

violated when "*the officers […] do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offense that would otherwise not have been committed*."[151] Such case law has been developed mainly for classical infiltration, but it helps provide an understanding of the limits of cyber infiltration and of state sovereign coercion. To begin, the ECHR creates a substantive test to ensure compliance. Those limits arise regarding legal safeguards and the passive behavior of the undercover agent.[152]

231. Legal safeguards. The ECHR establishes the legal framework,[153] particularly the procedural safeguards.[154] First, it requires a "*clear and foreseeable procedure for authorizing investigative measures*."[155] However, the French cyber-infiltration technique does not provide for authorization;[156] in Romania, the prosecutor authorizes the infiltration;[157] and in Spain, both the judge of instruction and the prosecutor can authorize this measure.[158] The lack of coherent authorization is questionable. Second,

---

[151] ECHR, *Ramanauskas (1)*, *op. cit.* note 147, ¶ 55. The ECHR relies on the concepts of entrapment, police incitement, and *agent provocateur*. The notion of entrapment comes from the United States, E. Burda, L. Trellova, "Admissibility of an Agent Provocateur and an Advocate Acting as an Agent Law," *Balkan Social Science Review*, 2019, vol. 14, p. 58

[152] Those criteria are part of the ECHR substantive test, if the operations can be characterized as entrapment. If the first test is not conclusive, ECHR, *Edwards and Lewis v. the United Kingdom*, July 22, 2003, 39647/98 and 40461/98, ¶ 46; ECHR, *Matanović v. Croatia*, April 4, 2017, no. 2742/12, ¶ 131, then the court relies on a procedural test, to check if the applicant had the opportunity to challenge the admissibility of the evidence, ECHR, *Bannikova v. Russia*, November 4, 2010, no. 18757/06, ¶¶ 37-65; ECHR, *Matanović v. Croatia*, ¶ 122; ECHR, *Ramanauskas v. Lithuania (2)*, February 20, 2018, no. 55146/14, ¶ 55. The procedure must be adversarial, thorough, comprehensive, and conclusive. For example, a decision dismissing an applicant's plea of entrapment should be "*sufficiently reasoned*," ECHR, *Sandu v. the Republic of Moldova*, February 11, 2014, no. 16463/08, ¶ 38; ECHR, *Tchokhonelidze v. Georgia*, June 28, 2018, 5753/09 and 11789/10, ¶ 52

[153] ECHR, *Teixeira*, *op. cit.* note 147, ¶ 38; on the contrary, for an operation outside the legal framework, see ECHR, *Ramanauskas (1)*, *op. cit.* note 147, ¶ 64

[154] ECHR, *Nosko and Nefedov v. Russia*, October 30, 2014, 5753/09 and 11789/10, ¶ 64

[155] ECHR, *Teixeira*, *op. cit.* note 147, ¶ 37; although at this time, Ormerod criticized that "*The European Court did not go so far as to prescribe that pre-operation judicial supervision/authorization was necessary*," D. Ormerod, A. Roberts, "The Trouble with Teixeira: Developing a Principled Approach to Entrapment," *International Journal of Evidence & Proof*, 2002, vol. 6, no. 1, p. 43. Given the extensive ECHR case law on other digital investigative techniques, such criticism is harsh. The court highlights that a "*simple administrative decision by the body which later carried out the operation*" is not enough; and that the authorizing decision must be properly motivated, ECHR, *Vanyan v. Russia*, December 15, 2005, no. 53203/99, ¶¶ 46-47; ECHR, *Khudobin v. Russia*, October 26, 2006, no. 59696/00, ¶ 135

[156] Article 230-46 of the Code de procédure pénale. An authorization is needed for the acquisition of "*any content, product, substance, sample, or service, including illicit content, or transmit[ing] in response to an express request for illicit content*." It should be underlined that the latter concept is not defined. On the contrary, the physical infiltration requires one, Article 706-81, specially motivated, Article 706-83.

[157] Article 148.1 of the Codul de Procedură Penală. The prosecutor may also authorize participation in specific activities, Article 150. The authorizations should be motivated.

[158] Specific authorization is required for cyber infiltration, as well as exchanging, sending, and analyzing "*illegal files by reason of their content*," Article 282 bis.6 of the Ley de Enjuiciamiento Criminal. The latter

the ECHR regulates the supervision of the measure.[159] In France and Romania, the prosecutor is in charge of overseeing cyber-infiltration,[160] while the operations in Spain are under the supervision of the magistrate who authorized the measure.[161] These procedures are especially relevant since "*it falls to the prosecution to prove that there was no incitement*."[162] However, cyber infiltration frameworks do not conform to the other criteria regarding general legal safeguards. The criterion of personal scope is difficult to apply to a specific and known offender, particularly due to the use of pseudonyms. The French framework allows the undercover agent to participate in conversations with potential offenders or other persons.[163] The main point of interest is the temporal scope, which is not considered in the French[164] and Spanish[165] frameworks.[166] Additionally, no specific provisions are detailed concerning data protection.[167]

232. Passive behavior. The ECHR also regulates the reality of the operations. In particular, agents should "*not incite*."[168] First, regarding the potential criminal behavior,

concept is not defined, like in France. For cyber infiltration, the law does not provide detail on the motivation.

[159] It considers the best supervision to be judicial, ECHR, *Vanyan*, *op. cit.* note 155, ¶¶ 46-47; ECHR, *Khudobin*, *op. cit.* note 155, ¶ 135; however, it accepts the supervision by a prosecutor, *Ibid.* ¶ 135; ECHR, *Milinienė v. Lithuania*, June 24, 2008, no. 74355/01, ¶ 39; ECHR, *Tchokhonelidze*, *op. cit.* note 152, ¶ 51

[160] Article 230-46 of the Code de procédure pénale and Article 148.5 of the Codul de Procedură Penală. Voices raised to ask in support for a control by the judge of liberties and custody, J.-M. Brigant, "Mesures d'investigation face au défi numérique en droit français," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 234; A. Reverdy, H. Matsopoulou, C. Mascala, *Le Lamy, droit pénal des affaires*, Wolters Kluwer France, 2020, ¶ 6155

[161] Article 282 bis.1 of the Ley de Enjuiciamiento Criminal

[162] ECHR, *Ramanauskas (1)*, *op. cit.* note 147, ¶ 70. The "*authorities may be prevented from discharging this burden by the absence of formal authorization and supervision of the undercover operation*," ECHR, *Teixeira*, *op. cit.* note 147, ¶ 38; ECHR, *Lüdi v. Switzerland*, June 15, 1992, no. 12433/86

[163] Article 230-46.1° and 2° of the Code de procédure pénale

[164] On the contrary, the "physical" infiltration is limited to four months, but the code does not provide limits for renewals, Articles 706-83 and 706-85 of the Code de procédure pénale

[165] Although the false identity is attributed for a period of six months, renewable, with no limit to those renewals, Article 282 bis.1 of the Ley de Enjuiciamiento Criminal

[166] In Romania, infiltration, including cyber infiltration, is limited to 60 days, renewable for a total of one year. However, this limit is suppressed for a list of offenses, including human trafficking, with no global temporal limit provided, Article 148.10 of the Codul de Procedură Penală. However, the temporal limit should be included in the authorizing document, Article 148.2.b. On the contrary, authorized participation in certain activities is limited to one year in total, with no exception, Article 150.8.

[167] Except for the report on the operations that need to be realized within the Romania framework, Articles 148.5 and 150.5 of the Codul de Procedură Penală. On this topic, since the ECHR case law focuses on "physical" infiltration and not cyber infiltration, further criteria could be hoped for in the future.

[168] ECHR, *Khudobin*, *op. cit.* note 155, ¶ 128. It takes into account "*the reasons underlying the covert operation and the conduct of the authorities carrying it out [and if] there were objective suspicions*" against the applicant, ECHR, *Bannikova*, *op. cit.* note 152, ¶ 38. In general, the ECHR wants proof of "*good reasons for mounting the covert operation*," ECHR, *Ramanauskas (1)*, *op. cit.* note 147, ¶¶ 63-64; ECHR, *Malininas v. Lithuania*, July 1, 2008, no. 10071/04, ¶ 36. This distinction is similar to the American case law, see J. Pradel, *Droit pénal comparé*, Dalloz, 2016, p. 352

the court will consider various criteria. The person could have been "*predisposed to commit the offense*"[169] or was suspected of "*prior involvement*."[170] This "*pre-existing criminal intent must be verifiable*."[171] Regarding cyber infiltration to investigate human trafficking, these criteria appear to limit operations to those meant to contact already known traffickers or victims. Second, an agent's attitude should be passive, limited to joining criminal acts and not instigating them. In particular, the court considers the first contact.[172] Therefore, if the agent contacts someone in response to an online advertisement of a job, or of a sexual service,[173] their behavior is passive. However, doubts arise if the agent shares a message indicating that they are looking for a job or a way to earn money.

233. Even if the undercover agent would like to speed up the process of trafficking to obtain evidence, the notion of entrapment makes it risky to be more active in the implementation of cyber infiltration. Such risk also derives from the apparent inconsistencies in the solutions the French *Cour de Cassation* provides.

B. Loyalty of proof in the French case law

234. Concept. To regulate the principle of proof freedom, the loyalty (fairness) of proof was developed in France.[174] According to the case law of the *Cour de Cassation*, the operations to obtain evidence should rely on certain standards,[175] and unfair proof

[169] ECHR, *Teixeira*, *op. cit.* note 147, ¶ 38, for example, by demonstrating "*familiarity with the crime*," ECHR, *Shannon v. the United Kingdom*, October 4, 2005, no. 6563/03, or because the person earns a pecuniary benefit, ECHR, *Khudobin*, *op. cit.* note 155, ¶ 134

[170] ECHR, *Teixeira*, *op. cit.* note 147, ¶¶ 37-38; ECHR, *Eurofinacom v. France*, September 7, 2004, no. 58753/00. However, the criminal record is not "*by itself indicative of any ongoing criminal activity*," ECHR, *Constantin and Stoian v. Romania*, September 29, 2009, 23782/06 and 46629/06, ¶ 55

[171] ECHR, *Vanyan*, *op. cit.* note 155, ¶ 49; ECHR, *Khudobin*, *op. cit.* note 155, ¶ 134

[172] ECHR, *Sequeira v. Portugal*, May 6, 2003, no. 73557/01; ECHR, *Eurofinacom*, *op. cit.* note 170; ECHR, *Milinienė*, *op. cit.* note 159, ¶¶ 37-38; ECHR, *Burak Hun v. Turkey*, December 15, 2009, no. 17570/04, ¶ 44; ECHR, *Sepil v. Turkey*, November 12, 2013, no. 17711/07, ¶ 34. The court also considers whether the applicant was pressured to commit the offense, ECHR, *Ramanauskas (1)*, *op. cit.* note 147, ¶ 67; in particular, if the agent took the initiative in contacting the applicant, renewing the offer despite his initial refusal, ECHR, *Malininas*, *op. cit.* note 168, ¶ 37; or by appealing to the compassion of the suspected person, ECHR, *Vanyan*, *op. cit.* note 155, ¶ 49

[173] It should be noted that in France, clients of prostitution are now criminalized in certain circumstances, Articles 225-12-1 and followings of the Code pénal. For "physical" infiltration, the code protects the undercover agents for the commission of specific offenses, which do not seem to include the use of prostitution, Article 706-82 of the Code de procédure pénale, but no similar provision is provided for cyber infiltration.

[174] Article 427 of the Code de procédure pénale

[175] The 1888 decision was only applicable to magistrates, H. Vlamynck, "La loyauté de la preuve au stade de l'enquête policière," *Actualité juridique Pénal*, Dalloz, 2014, p. 325; the principle was extended to investigators in 1952, E. Vergès, "Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale," *Recueil Dalloz*, 2014, p. 407. However, the first explicit mention of the principle arose in Cour

is not admissible. The French case law distinguishes between the provocation for the commission of an offense and the production of evidence[176] to determine whether the undercover agent made the affected person lose their free will to commit the offense.[177] However, this case law is criticized as being unstable.[178]

235. Cases. First, the *Cour de Cassation* ruled on the creation of websites to identify potential offenders, a technique similar to cyber infiltration. The first case involved the creation of a child pornography website by an American police authority;[179] one offender was located in France. An investigation was opened, and illicit materials were found during a digital search. In its first ruling, the court decided, without providing any explanation, that such a technique was unfair and that all subsequent evidence was inadmissible.[180] As a result, in the same case, a second ruling determined that there was no prior element to suspect the offense as the sole criterion.[181] Therefore, the court seems to rely on the restrictive criterion of the passive agent, requiring prior clues of the commission or preparation of an offense.[182] In the second case, the US police

---

de Cassation, Chambre criminelle, February 27, 1996, no. 95-81366. The principle is applicable to any proof, meaning that it is not limited to the framework of the cyber infiltration, see, for example, Cour de Cassation, Chambre criminelle, December 16, 1997, no. 96-85589; Cour de Cassation, Chambre criminelle, January 19, 1999, no. 98-83787

[176] A. Bensoussan, A. Lepage, M. Quéméner, "Loyauté de la preuve et nouvelles technologies : entre exigences processuelles et efficacité répressive," *in* S. Guinchard et al. (eds.), *Les transformations de la justice pénale: cycle de conférences 2013 à la Cour de cassation*, 2014, p. 236; M. Quéméner, "Fascicule 1110 : Infiltrations numériques," *JurisClasseur Communication*, LexisNexis, July 3, 2019, ¶ 39. In the regime of cyber infiltration, such a criterion has been explicitly introduced. However, this provision is limited to the acts considered at Article 230-46.3° of the Code de procédure pénale, which is inconsistent with practice since any act could in theory provoke the offense.

[177] The literature mentions various criteria, such as previous criminal activity, the social aim of the measure, the seriousness of the offense, the characteristics of the offender, etc., P. Maistre du Chambon, "La régularité des « provocations policières »," *op. cit.* note 146, ¶¶ 8, 10, 15. Perrier also distinguishes between internal unfairness, which derives meaning from the operations (the modalities of the measure), and external unfairness, which is related to the rules or rights that the agents wished to avoid (the goal of the measure), J.-B. Perrier, "Le fair-play de la preuve pénale," *Actualité juridique Pénal*, Dalloz, 2017, p. 436. However, in the modalities, he only considers the legal safeguards, which is just one of the criteria of the ECHR.

[178] M. Quéméner, "Les spécificités juridiques de la preuve numérique," *Actualité juridique Pénal*, Dalloz, 2014, p. 63; J.-B. Perrier, "Le fair-play de la preuve pénale," *op. cit.* note 177, p. 436; A. Lepage, "Provocation sur Internet - La distinction entre provocation à la preuve et provocation à la commission d'une infraction à l'épreuve d'Internet," *Communication Commerce électronique*, September 2014, no. 9. For a list of case law admitting or excluding fair or unfair proofs, see H. Vlamynck, "La loyauté de la preuve au stade de l'enquête policière," *op. cit.* note 175, p. 325. For an example of theorization of the elements (material and formal) of loyalty of proof, see O. Décima, "De la loyauté de la preuve pénale et de ses composantes," *Recueil Dalloz*, Dalloz, 2018, no. 02, p. 103

[179] It should then be underlined that the loyalty of proof applies to all the evidence brought to the court, independently of whether it was obtained by French law enforcement authorities or abroad.

[180] Cour de Cassation, Chambre criminelle, February 7, 2007, no. 06-87753

[181] Cour de Cassation, Chambre criminelle, June 4, 2008, no. 08-81045

[182] The inadmissibility of evidence relies on the chronology of the procedural act, refusing to consider all the evidence obtained after the unfair operation. The court does not consider the chronology of the commission of the offenses, J. Francillon, "Provocation à la commission d'actes de pédophilie organisée

created a forum to share information about bank card frauds, and one user was located in France. Evidence was found during a search to confirm the prior commission of the offense.[183] While no prior clues existed, the court admitted the evidence as fair.[184] Therefore, the main criterion does not appear to rely on prior clues but rather on the behavior of the suspected person. The mere connection to a child pornography website does not create suspicion that the person is a criminal.[185] Thanks to the presumption of innocence, it can always be considered that clicking on a link could have been a mistake.[186] In contrast, if the suspected person writes messages after accepting an invitation to join a forum, the process would not be considered unfair. A last case involved blackmail based on the distribution of a sex tape,[187] and a police officer acted as a friend of the victim to obtain evidence. The officer used a pseudonym, and some of the conversations took place at their initiative.[188] Thus, the court considered the process to be unfair.[189] Two years later, the case was resolved by the plenary assembly of the court, which determined that the process was fair since the commission of the offense did not depend on the action of the agent.[190]

236. Summary. Consequently, it is clear that the *Cour de Cassation* struggles to establish criteria to provide for a coherent regime on the loyalty of proof, which creates legal instability on the use of state coercion through cyber infiltration,[191] particularly to investigate cyber human trafficking. The threshold between the provocation necessary to commit an offense and the production of evidence is not well defined. Could an undercover agent directly contact a suspected trafficker if the main criterion is the

---

par un service de police étranger utilisant le réseau internet (suite)," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 621

[183] The decision does not specify if such offense was committed before or after the exchange of messages on the forum.

[184] Cour de Cassation, Chambre criminelle, April 30, 2014, no. 13-88162

[185] Especially since the offense would not have been committed without the fake website, J. Francillon, "Cyberdélinquance et provocations policières," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2014, p. 577

[186] J. Buisson, "Contrôle de l'éventuelle provocation policière : création d'un site pédo-pornographique un policier, même étranger," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 663. However, if the identification of the offender was followed by the surveillance of their Internet flows and it is proven that the person consulted various similar websites, the doubt could have been erased. Such case law then encourages law enforcement authorities to gather more evidence.

[187] Usually, a video of sexual activities.

[188] G. Pitti, "L'affaire de la sextape : on ne dribble pas le principe de loyauté des preuves !," *Gazette du Palais*, September 19, 2017, no. 31, p. 18

[189] Cour de Cassation, Chambre criminelle, July 11, 2017, no. 17-80313

[190] Cour de Cassation, Assemblée plénière, December 9, 2019, no. 18-86767, ¶¶ 27-31

[191] A. Lepage, "Enquête sous pseudonyme sur les réseaux numériques," *Communication Commerce électronique*, April 2018, no. 4, p. comm. 29

suspected person's active behavior? Or should the agent reply only to online messages? Could the agent impersonate someone selling sexual services to attract clients and traffickers who are already recruiting persons for this activity? Consequently, considering the instability of the case law, law enforcement authorities seem reluctant to use cyber infiltration, especially to investigate trafficking.[192] French case law could introduce the criteria of the ECHR to systematize its decisions and create a more stable regime.

237. New digital coercion tools were designed to strengthen states' sovereignty. However, the regulators seem to disregard full consideration of the case law of the ECHR, resulting in the legal instability of digital investigative techniques. Additionally, practical obstacles challenge states to exercise the full range of their digital coercion to combat cyber trafficking.

§2. The practical instability of the state's digital legitimate coercion powers

238. States are developing digital investigative techniques, extending them to new offenses. The criminal procedure offers many opportunities to combat cyber human trafficking, but when considering the implementation of these techniques is considered, the reality challenges the theory. To study the validity of law, Delmas-Marty considers its empirical validity, or effectiveness, including on the basis of pragmatic elements such as material resources.[193] These techniques are not a magic wand to obtain evidence against traffickers. On the contrary, various challenges are posed during the collection of information (I), while the techniques are limited by both human and technical implementation (II).

I. Collecting data: extraterritoriality and quantity

239. Limits of territoriality. To collect and analyze data, investigators face a number of obstacles. First, questions arise from the extraterritoriality of national

[192] That was especially mentioned during the meeting of the French working group on the prostitution of minors, which focuses on the impact of Internet and social networks, that took place on April 14, 2021. French and Romanian prosecutors underlined the same problem.

[193] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit no. 1, 2004, pp. 194-223. Nonetheless, she criticized the fact that effectiveness has become the sole criterion for determining the legality of a law, M. Delmas-Marty, *Une boussole des possibles: Gouvernance mondiale et humanismes juridiques - Leçon de clôture prononcée le 11 mai 2011*, Collège de France, 2020, ¶ 4. Similarly, Thibierge considers the effectiveness of norms to study their "*normative reach*" and, in general, their "*normative strenght*," C. Thibierge, "Le concept de 'force normative,'" *in* C. Thibierge (ed.), *La force normative : naissance d'un concept*, LGDJ-Lextenso éd. Bruylant, 2009, p. 813

investigative techniques**.** According to criminal sovereignty, the principle of territoriality defines not only jurisdiction but also the geographical limit of the investigation.[194] However, data can easily cross borders through cyberspace. Outside of cyberspace, territoriality is materialized by the location of devices. Regarding interception, the French *Cour de Cassation* is clear:[195] The communication must involve a French telephone operator.[196] Therefore, investigators can intercept communications through a foreign phone since the foreign operator will need to use the French network. This is particularly relevant for transnational trafficking, as the traffickers and victims might use a foreign operator. On the contrary, in cyberspace, the location of data is uncertain.[197] In France, mutual assistance is necessary for searches[198] if it is "*established that these data […] are stored in another computer system located outside the national territory*."[199] In the absence of proof, the investigators will continue as long as the data are available on French territory.[200] Consequently, there is uncertainty about the

[194] Although this principle has been adapted and has exceptions to better fit with the evolution of crimes, including for non-digital investigative techniques, see T. Herran, *Essai d'une théorie générale de l'entraide policière internationale*, Thesis, Université de Pau et des Pays de l'Adour, 2012, p. 377

[195] Neither Spain nor Romania have such a provision. For example, in Spain, interception of communications abroad must rely on a European investigation order within the EU, A. Melón Muñoz (ed.), *Procesal penal 2021*, Francis Lefebvre, Memento práctico, 2020, ¶¶ 5090-5091

[196] Cour de Cassation, Chambre criminelle, June 20, 2018, no. 17-86651; Cour de Cassation, Chambre criminelle, June 20, 2018, no. 17-86657. Also, if an interception of communications started in one state of the EU and continued in another, the French framework facilitates the continuation of the measure, Article 100-8 of the Code de procédure pénale, which does not require a European investigation order as soon as the country is notified. Such provisions will smooth the use of such techniques, especially considering transnational transportation during trafficking, in particular with neighboring countries except the United Kingdom due to Brexit and Switzerland. On the contrary, for geotagging, a mutual assistance request is necessary, M. Quéméner, "Fascicule 982 : Géolocalisation dans le cadre pénal - Articles 689 à 693," *JurisClasseur Communication*, LexisNexis, July 3, 2019, ¶¶ 55-60; Cour de Cassation, Chambre criminelle, February 9, 2016, no. 15-85070; Cour de Cassation, Chambre criminelle, April 10, 2018, no. 17-85607

[197] But the question is not considered by the Spanish and Romanian frameworks. The criterion of localization of servors is even more fragile since, for the biggest online service providers, data can be stored in various servors at the same time and can be moved from one to another frequently. For more information, see *infra* 282. Such a boundary is especially important when conducting searches and accessing stored electronic correspondence. Legal hacking will not be included here since the objective of the measure is to monitor what someone is doing on a device and not to enter a place in cyberspace (although it can be an indirect consequence).

[198] No similar provision is considered for access to stored electronic correspondence, even if the result is very similar to a search, O. Violeau, "Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques," *Actualité juridique Pénal*, Dalloz, 2017, p. 324

[199] Article 57-1 of the Code de procédure pénale. In the absence of an international request, the operations and the resulting data would be null and void, B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 23, p. 99. However, the case law of the Cour de Cassation does not detail how the data can be established as being located outside the territory.

[200] *Ibid.* p. 98; Cour de Cassation, Chambre criminelle, November 6, 2013, no. 12-87130. Therefore, the criterion is very permissive. In practice, in cases of doubt, they apply the French procedure without relying on an international procedure, which has been confirmed by investigators from the French Sous-Direction de la Lutte contre la Cybercriminalité. On the contrary, for instance, in Belgium, the investigators are required to select the flight mode of the seized devices, to only access what is stored

validity of the evidence due to the ubiquitous nature of cyber offenses and their potential extraterritorial localization.

240. When there is no or too much data. Despite their broadness, the results of digital investigative techniques are not always effective, especially with regard to the interception of communications, the "golden" technique that frequently is used to investigate trafficking. However, this technique faces an important obstacle: encryption.[201] While Internet flows can be intercepted, they do not include an understandable version of data from encrypted websites, because traffickers mostly use common applications, such as WhatsApp, and Instagram, which are encrypted.[202] On the contrary, digital investigative techniques can result in obtaining a significant amount of data,[203] even too much to be analyzed by humans.[204] Investigators monitor the Internet and extract large amounts of data from websites, particularly to fight cyber human trafficking.[205] Research can be conducted via through digital tools—keywords,

in them, V. Franssen, O. Leroux, "Recherche policière et judiciaire sur Internet : analyse critique du nouveau cadre législatif belge," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 142; C. Forget, "Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict ?," *Revue du droit des technologies de l'information*, 2017, no. 66/67, p. 25

[201] See *infra* 335 to 339 on encryption.

[202] Although the content of the data communications is not accessible, the proportion of the phone's use for data can be one of the clues to consider that the device was used to commit the trafficking offense. This limit has been particularly underlined by all the legal practitioners and in the following report, Groupe de travail sur la prostitution des mineurs, *Rapport sur la prostitution des mineurs*, France, June 28, 2021, p. 165. On the contrary, an investigation was developed quickly in southern France, since the traffickers only used regular phone calls, Le Figaro, AFP, "Un réseau international de traite des êtres humains démantelé dans le sud de l'Europe," *Le Figaro.fr*, March 5, 2021, online https://www.lefigaro.fr/faits-divers/un-reseau-international-de-traite-des-etres-humains-demantele-dans-le-sud-de-l-europe-20210305 (retrieved on April 19, 2021). Remote access as a solution is limited as traffickers might use message self-destruction options, For example, Wickr, see J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1694. Signal and Snapchat were mentioned during discussions with law enforcement authorities. For the latter, see also J. Stearns, "Street Gangs and Human Trafficking," *in* M. Palmiotto (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 153

[203] d. boyd et al., *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the US*, Microsoft Research Connections, December 2011, p. 8; GRETA, "Online and technology-facilitated trafficking in human beings. Full report," Council of Europe, March 2022, pp. 46-47

[204] From tracing "*working hours, working conditions, threats and logistics of transport, as well as the daily income and the constant control and abuse of the women*," I. Chen, C. Tortosa, "The Use of Digital Evidence in Human Trafficking Investigations," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 123; to more abstract data: information, dates, connection times, etc.

[205] Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, "Final Report," Committee for Equality between Women and Men, Council of Europe, September 16, 2003, pp. 70, 75, 76, EG-S-NT (2002) 9 rev.

for example[206]—but anti-trafficking law enforcement authorities appear to still rely mostly on manual tools.

241. Aside from limitations due to the localization and quantity of data, law enforcement authorities face challenges posed by human and material resources.

II. Implementing digital investigative techniques: resources

242. Human resources. The realm of law is not abstract, and its implementation strongly depends on technical and human resources.[207] First, law enforcement authorities need enough personnel to investigate trafficking cases,[208] and those involved should be highly specialized.[209] In the context of cyber trafficking, their training should include not only the phenomenon but also the digital context and available tools.[210] The implementation of digital investigative techniques also requires time and

[206] S. Raets, J. Janssens, "Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business," *European Journal on Criminal Policy and Research*, October 26, 2019, p. 13; Inter-agency coordination group against trafficking in persons, *Human trafficking and technology: trends, challenges and opportunities*, Issue Brief, no. 7, UN, 2019, p. 3; UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, UN, May 2015, p. 47; M. Quéméner, "Fascicule 20 : La preuve numérique dans un cadre pénal - Articles 427 à 457," *JurisClasseur Procédure pénale*, LexisNexis, April 18, 2019, ¶¶ 84-85. See *infra* Part 2. Title 1. Chapter 2. Section 2. on algorithms to process data within investigations on human trafficking.

[207] GRETA, *Online and technology-facilitated trafficking in human beings. Full report*, *op. cit.* note 203, pp. 47-49

[208] This problem has been highlighted by all law enforcement authorities interviewed. Interestingly, in France, the focus seemed to be on the need to hire magistrates, in particular prosecutors, while in Romania, the need for more police officers was underlined to be able to focus on proactive investigations.

[209] Usually, the particularities of human trafficking are not part of the general curriculum of magistrates, and further trainings are not mandatory. On the digital component of human trafficking, legal practitioners specializing in the latter are, in general, not specializing in the former, and *vice versa*. The GRETA underlines a lack of formation, in particular in Romania, GRETA, "Evaluation Report - Romania - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, June 3, 2021, ¶¶ 136-138, and in France, GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by France - Second evaluation round," Council of Europe, 2017, ¶ 266. Although trainings are available in France, there is no inventory and they are poorly advertised, making them less accessible, Groupe de travail sur la prostitution des mineurs, *Rapport sur la prostitution des mineurs*, *op. cit.* note 202, pp. 144-154. The last GRETA report noted improvements but still underlined the need to strengthen training, GRETA, "Evaluation Report - France - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, February 18, 2022, ¶¶ 151, 205. While trainings are widely available to police officers in Spain, GRETA, "Evaluation Report - Spain - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, June 12, 2023, ¶ 144, anti-trafficking units lack specialization on digital elements of the investigation. Thus, the Madrid unit on cyber trafficking of the Unidad Central de Redes de Inmigración Ilegal y Falsedades Documentales (UCRIF) tends to collaborate with the Unidad Central de Ciberdelincuencia (conversation with the central unit of the UCRIF).

[210] M.C. Rayón Ballesteros, J.A. Hernández, "Cibercrimen: particularidades en su investigación y enjuiciamiento/Cybercrime: particularities in investigation and prosecution," *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario "Escorial-María Cristina," 2014, no. 47, p. 230. In

timing. Installing a device enables access to the trafficker's or victim's device without them noticing,[211] but time is at the core of this cyber infiltration: Exchanges will likely happen outside office hours, while agents still need to conform to labor laws.[212] Therefore, this technique requires extreme availability.[213] Specialization and timing are highly important regarding the entity authorizing the measure.[214] While prosecutors and instruction judges can be specialized, French judges of liberties and custody and Romanian judges of rights and liberties are not,[215] and as a result of this lack of training, these judges are less willing to use new investigative techniques.[216] Moreover, when the request for authorization is urgent, it lessens its *a priori* control.[217] However, if the authorization process takes too long, it can limit the opportunities to gather evidence and protect victims.[218]

243. Technical resources. Second, law enforcement authorities need appropriate

France, while the Office central pour la répression de la traite des êtres humains (OCRTEH) can rely on the expertise of one cyber-specialized officer, the Office central de lutte contre le travail illégal (OCLTI) has none. On the contrary, the OCRTEH does not have a financial-specialized officer, while a lot of the personnel of the OCLTI have undergone such training (data from conversations in 2021). Furthermore, in France, only specific police officers can be authorized to use cyberinfiltration, Article 2 of the Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme. In 2016, the lack of certified officers was stressed, Inspection générale des affaires sociales, Inspection générale de l'administration, Inspection générale de la justice, "Evaluation de la loi du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées," France, December 2019, p. 9. However, in 2021, the OCRTEH mentioned three certified police officers and underlined that cyber infiltration is not usually used in their cases, in particular due to its legal instability.

[211] Also, if the request for authorization is made too early, the authorizing body may rule that there are not enough clues or evidence; on the contrary, waiting for strong evidence might generate more violations of the victims' rights. This point has been particularly noted by Romanian practitioners. In France, this distinction would be less problematic for techniques allowed by the prosecutor during the preliminary investigation, and by the judge of instruction during the judicial information.

[212] For example, it questions the continuation of the operations if the police officer takes a leave.

[213] Groupe de travail sur la prostitution des mineurs, *Rapport sur la prostitution des mineurs*, *op. cit.* note 202, p. 166. Also, the procedure's final result is usually far from the one expected and in accordance with the means implemented by the police. One case was mentioned during an exchange with an investigator, regarding an operation of cyber infiltration and an exchange of more than 100 emails; but the offender was only convicted to a suspended sentence of three months of imprisonment.

[214] C. Lazerges, "Dédoublement de la procédure pénale et garantie des droits fondamentaux," *op. cit.* note 15, pp. 587-588

[215] O. Cahn, "Réflexions désabusées sur le chapitre I du titre I de la loi n° 2016-731 du 3 juin 2016," *Actualité juridique Pénal*, Dalloz, 2016, p. 408

[216] J. Pronier, "La clarification des règles encadrant le recours à un dispositif de captation des images et des paroles," *Actualité juridique Pénal*, Dalloz, 2013, p. 227

[217] It is particularly notable in Romania, where the judge of rights and liberties must answer the same day the request was formulated, Article 140.3 of the Codul de Procedură Penală. In Spain, the judge must solve the request in 24 hours, Article 588 bis c.1 of the Ley de Enjuiciamiento Criminal.

[218] The latter was highlighted in France for cyber infiltration and the authorization to buy or transmit illegal content, weakening the spontaneity of communications and the trust of the suspected person. It is even more problematic considering that exchanges can take place outside of normal working hours.

technical tools.[219] The tool must exist, the state must have access to it,[220] and trained personnel must use it.[221] When traffickers use all available technologies, states need to create their own tools or open a public market to buy private ones.[222] Consequently, the costs of legal procedures are constantly on the rise,[223] even as states usually emphasize the need to control those these expenses.[224] As a cost-cutting measure, central entities have been created, particularly to intercept communications.[225] Therefore, through a pragmatic economic analysis of criminal procedures, not all investigative techniques will be implemented in every case that could use them. This These decisions must be made not only within the context of trafficking—for example, employing more resources in organized crime settings or when multiple victims are involved— but also with regard to criminal policy priorities. For example, terrorism and

[219] In general, more tools are needed for the surveillance of cyberspace, independently from the implementation of digital investigative techniques, in particular for the analysis of social networks, Groupe de diagnostic stratégique, *Vers une police 3.0 : enjeux et perspectives à l'horizon 2025*, no. 3, INHESJ, France, 27e Session nationale « Sécurité et Justice » - 2015/2016, June 2016, p. 48

[220] Even when the state has the device, it must have enough of it. A similar problem has arisen for electronic bracelets (tagging devices for the control of suspected or convicted persons), P. Gonzalès, "Un risque de pénurie pèse sur les bracelets électroniques," *Le Figaro*, March 10, 2021, online https://www.lefigaro.fr/actualite-france/un-risque-de-penurie-pese-sur-les-bracelets-electroniques-20210310 (retrieved on October 28, 2021). Similarly, the number of IMSI catchers is limited.

[221] B. Roussel, *Les investigations numériques en procédure pénale*, *op. cit.* note 23, pp. 196-198 ; M.C. Rayón Ballesteros, J.A. Hernández, "Cibercrimen," *op. cit.* note 210, p. 231

[222] Regarding legal hacking, in France, the possible implementation of such technique has been delayed due to "*complex technical issues*," even though the law already regulates the technique, M. Quéméner, "Les techniques spéciales d'enquête en matière de lutte contre la cybercriminalité," *Actualité juridique Pénal*, Dalloz, 2015, p. 403

[223] For instance, in France, it reached 648.4 million euros in 2022. Particularly, it has increased for criminal cases since the beginning of the pandemic. In 2004, the implementation of digital investigative techniques represented 27% of the total of costs of legal procedures, J.-L. Warsmann, *Rapport d'information sur la mise en application de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*, no. 2378, Assemblée nationale, France, June 15, 2005, pp. 27-30. The cost of using legal hacking is also deemed prohibitively high, M. Untersinger, "Justice : les enquêteurs pourront bientôt utiliser des logiciels espions," *Le Monde.fr*, November 14, 2017, online https://www.lemonde.fr/pixels/article/2017/11/14/justice-les-enqueteurs-pourront-bientot-utiliser-des-logiciels-espions_5214397_4408996.html (retrieved on April 29, 2021)

[224] In France, see, for instance, L. Saint-Martin, P. Hetzel, *Rapport général au nom de la commission des finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2022 (n° 4482) - Annexe n° 18 Justice*, no. 4482, Assemblée Nationale, France, October 7, 2021, pp. 27-28. However, the more increasing expenses do not seem to be linked to digital investigative techniques, but rather "*genetic and toxicological analyses, psychological and psychiatric expertise, interpreting, and translation costs*," Mission ministérielle Projets annuels de performance, *Budget général - Annexe au projet de loi de finances pour 2021 - Justice*, République française, 2020, p. 49

[225] In Spain, the Sistema Integrado de Interceptación Telefónica. In France, the Plateforme nationale des interceptions judiciaires, Article 230-45 of the Code de procédure pénale. However, the project, which is still not fully implemented, cost a total of 385 million euros, C. Serre, C. Evrard, "Du rififi chez les grandes oreilles," *Dalloz Actualité*, Dalloz, February 4, 2020. It has already been decided that the service will be reformed in 2024, to become the Système d'Information des Techniques d'Enquêtes Numériques Judiciaires.

drug trafficking cases typically take precedence over human trafficking cases.

244. Conclusion of the section. States have strengthened their digital coercion powers to extend their sovereignty in cyberspace, including to investigate human trafficking. However, these powers face numerous limitations. The legal frameworks for digital investigative techniques are unstable when facing human rights standards,[226] which are vital to democracy and the rule of law. These techniques offer new opportunities to gather evidence on cyber trafficking but their admissibility is not secured. When reforming criminal procedure codes, national legislators should consider ECHR case law. Additionally, human and material resources are still limited to fully implement these data-gathering approaches. These practical limitations are increased in the context of human trafficking, as a result of the absence of specialization in cyber investigations. Then, states must rely on a pragmatic perspective and agree to supplement their powers with those of other entities. Consequently, the anti-trafficking framework supports cooperation.

Section 2. Complementing states' powers of coercion: from cooperation to partnerships

245. The global 3P strategy to repress human trafficking was traditionally divided into three components: prevention, protection, and prosecution.[227] A fourth transversal component, partnership, has been manifested[228] in recent years, calling for a comprehensive strategy among various entities that already were involved in the repression of trafficking.[229] Although it is "*widely agreed that collaboration is necessary between organizations in the public, private, and civil society sectors*,"[230] the use of partnerships to combat trafficking is discussed. It is the ugly duckling of the global

[226] P. Maistre du Chambon, "La régularité des « provocations policières »," *op. cit.* note 146, ¶ 19

[227] General Assembly, "Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons," UN, July 30, 2010, A/RES/64/293; reaffirmed by General Assembly, "Resolution 72/1. Political declaration on the implementation of the United Nations Global Plan of Action to Combat Trafficking in Persons," UN, September 27, 2017, p. 1, A/RES/72/1. Partnerships have been at the core of the Department of State, "Trafficking in persons report," US, June 2023, pp. 8-36

[228] It is very well underlined in the global strategy, as references to cooperation can be found in each of the 3P components, in addition to the Partnership autonomous component, General Assembly, *Resolution 64/293*, *op. cit.* note 227

[229] Deputy secretary-general, "Add 'partnership' to 'three P' agenda of United Nations anti-trafficking protocol, deputy secretary-general urges General Assembly thematic debate," UN Press Release, June 3, 2008, DSG/SM/397-GA/10713-HR/4956

[230] K. Foot, "Multisector Collaboration Against Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 660

strategy, the "*forgotten fourth P*."[231] After one recognizes the limits of the states' powers to fight cyber trafficking, it is clear that the sovereign state must enhance its partnerships. The evolution of its meaning in the anti-trafficking framework exemplifies the need to consider a pragmatic sovereignty, to "*engag[e] governments* (§1)*, the private sector* (§3)*, and civil society* (§2) *as a coalition for good*."[232]

§1. First layer of partnerships: states' classical cooperation

246. The classical first layer of partnership involves sovereign states, as they have the positive obligations to combat human trafficking; this responsibility has been explicitly underlined since the 1990s by both the EU[233] and the Council of Europe,[234] and the United Nations has followed this trend.[235] In particular, the UN's 2010 global strategy mentioned the need for "*effective cooperation […] among countries of origin,*

[231] M. McSween, "Investing in the Business against Human Trafficking: Embracing the Fourth P - Partnerships," *Intercultural Human Rights Law Review*, 2011, vol. 6, p. 286. To some authors, this addition was not necessary, N. Jägers, C. Rijken, "Prevention of Human Trafficking for Labor Exploitation: The Role of Corporations," *Northwestern Journal of International Human Rights*, 2014, vol. 12, no. 1, p. 51. It is not included as an autonomous element in many international evaluations. For example, the Anti-Trafficking Policy Index builds indicators to evaluate national policies on human trafficking. It includes cooperation only within the prevention component, reducing it to a very limited number of actions, S.-Y. Cho, "Evaluating Policies Against Human Trafficking Worldwide: An Overview and Review of the 3P Index," *Journal of Human Trafficking*, January 2, 2015, vol. 1, no. 1, p. 89. Similarly, the Trafficking in Persons Report published by the United States only explicitly considers the 3P strategy in its country narratives, see, for example, Department of State, "Trafficking in persons report," US, June 2021. Nor is it in many international resolutions. For example, the OSCE Plan of Action against Human Trafficking mentioned the need for cooperation since 2003 but considered partnerships as an autonomous component only in 2013, OSCE, "Decision No. 557: OSCE Action Plan to Combat Trafficking in Human Beings," July 24, 2003, PC.DEC/557; OSCE, "Decision nº 1107 Addendum to the OSCE Action plan to combat trafficking in human beings: one decade later," December 6, 2013, PC.DEC/1107/Corr.1

[232] C. Bain, "Entrepreneurship and Innovation in the Fight Against Human Trafficking," *Social Inclusion*, June 23, 2017, vol. 5, no. 2, p. 82. On this evolution, see C. Bauloz, M. McAdam, J. Teye, "Human trafficking in migration pathways: Trends, challenges and new forms of cooperation," *in* International Organization for Migration (ed.), *World Migration Report 2022*, May 21, 2020, pp. 269-277. Cooperation with international intergovernmental organizations will not be studied due to length and relevance to the topic of this thesis.

[233] Advocates for international cooperation to repress the "*trade of women*," European Parliament, "Resolution on trade in women," EU, September 16, 1993, ¶ 1, OJ No C 268, p.141; and human trafficking, European Parliament, "Resolution on trafficking in human beings," EU, February 5, 1996, ¶ 3, OJ No C 120/2, p.352; European Commission, "Communication to the Council and the European Parliament on trafficking in women for the purpose of sexual exploitation," EU, November 20, 1996, pp. 15-17

[234] Parliamentary Assembly, "Recommendation 1325 (1997) Traffic in women and forced prostitution in Council of Europe member states," Council of Europe, April 23, 1997, ¶ 4. See also Parliamentary Assembly, "Recommendation 1545 (2002) Campaign against trafficking in women," Council of Europe, January 21, 2002, ¶ 10.a; and Committee of Ministers, "Recommendation No. R (2000) 11 to member states on action against trafficking in human beings for the purpose of sexual exploitation," Council of Europe, May 19, 2000, ¶ 7

[235] General Assembly, "Resolution 58/137. Strengthening international cooperation in preventing and combating trafficking in persons and protecting victims of such trafficking," UN, February 4, 2004, ¶ 3

transit and destination."[236] Such collaboration entails strengthening mutual assistance among states to fight a transnational crime such as trafficking (I). At the regional level, this focus decreases as the offense is considered both national and transnational and since the trafficking framework can rely on general cooperation frameworks (II).

I. States' international cooperation against trafficking and sovereignty

247. Cooperation in historical treaties. The first treaties on "white slavery" highlighted the need for state cooperation because the offense was transnational.[237] The four existing conventions on trafficking were substituted by the 1950 Convention for the Suppression of the Traffic in Persons and of the Exploitation of the Prostitution of Others.[238] The condition of transnationality of the offense disappeared,[239] yet the convention continued to focus on state cooperation and was meant to facilitate extradition[240] and repatriation.[241] Additionally, states were "*bound to execute letters of request*," with the possibility of being transmitted directly through judicial authorities or a competent authority.[242] Moreover, the states were required to share information,

[236] General Assembly, *Resolution 64/293*, *op. cit.* note 227, ¶¶ 51-52 (annex)
[237] The International Agreement for the Suppression of the White Slave Traffic of 1904 created a framework to regulate the repatriation of "*women or girls [trafficked] for immoral purposes abroad*," through the nomination of an authority to offer direct communication on this topic, Articles 1, 3 and 4. Articles 1 and 2 of the 1910 International Convention for the Suppression of the White Slave Trade considered the fact that one could hire, abduct, or entice "*a woman or a girl […] for immoral purposes, even when the various acts which together constitute the offense were committed in different countries*." The 1921 International Convention for the Suppression of the Traffic in Women and Children broadens the scope of the definition to include children of both sexes, Article 2. The convention contemplated three tools for international cooperation. To begin, while the convention did not establish a legal framework for extradition, it stated that this offense will be "*deemed* ipso facto *to be included among the offenses giving cause for extradition according to already existing Conventions*," Article 5. The 1921 International Convention for the Suppression of the Traffic in Women and Children that supplemented the 1910 convention broadened the regulation of extradition, introducing the possibility to extradite even in the absence of an extradition convention, Article 4. Second, the 1910 convention considers the transmission of rogatory commissions through possible direct communication between judicial authorities, which was quite pioneering at this time, Article 6. Third, the convention provided for the communication of the sentences related to those offenses, Article 7. Later, the 1933 International Convention for the Suppression of the Traffic in Women of Full Age, relying on the authorities created by the 1904 agreement, considered the transfer of information, in particular records of convictions, and measures of refusal of admission or expulsion on the territory, directly and without delay, Article 3. The scope of the 1933 convention was similar to the previous ones, defining the traffic as "*whoever in order to gratify the passions of another person, has procured, enticed or led away even with her consent a woman or girl in full age for immoral purposes to be carried out in another country*," Article 1.
[238] Article 28 of the 1950 convention
[239] Articles 1 and 2 of the 1950 convention
[240] It includes the offense in any extradition treaty, Article 8 of the 1950 convention, and the principle of *aut dedere aut judicare*, Article 9, by which a state is mandated to prosecute a suspected offender when refusing the extradition.
[241] Through the exchange of information, Articles 18 and 19 of the 1950 convention
[242] Article 13 of the 1950 convention

such as police and conviction records.[243] Finally, the states were asked to nominate a service "*in charge of coordination and centralization*" of the investigation of the offense.[244]

248. Cooperation in the Palermo treaties. Fifty years later, the Palermo Convention and protocol offered a more effective tool due to their global level of ratification.[245]. First, by defining human trafficking at the international level, the protocol facilitates mutual assistance by verifying the condition of dual criminality.[246] Second, the protocol[247] is supplemented by the general provisions of the Palermo Convention, which provides for a detailed framework[248] on international cooperation, including mutual assistance,[249] which is particularly relevant to obtain evidence against cyber human trafficking.

249. Mutual assistance in the Palermo Convention. The Palermo Convention facilitates mutual assistance, and the possible acts are listed in a general way.[250] Consequently, the door is open to the evolution of cooperation to request digital evidence. The accepted languages for requests are disclosed by the parties,[251] and the reasons for refusal of cooperation are exhaustively listed.[252] However, mutual

[243] Including fingerprints and photographs, Article 15 of the 1950 convention
[244] Article 14 of the 1950 convention
[245] The 1904 agreement, updated by the protocol of Lake Success of 1949 counts around 60 participants; the 1910 convention, updated by the protocol of Lake Success of 1949 counts around 50 participants; the 1921 convention, updated by the protocol of Lake Success of 1947 counts around 65 participants; and the 1933 convention, updated by the protocol of Lake Success of 1947 counts around 30 participants. The 1950 convention had more success, with 95 participants (but only 13 of them signed the treaty). By contrast, the Palermo Convention has 191 parties, and the Palermo Protocol, 181.
[246] A. Fournier, "Aperçu critique du principe de double incrimination en droit pénal international," *in* B. Bouloc, F. Alt-Maes (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, pp. 339-341; B. Lavaud-Legendre, "La coopération répressive en matière de traite des êtres humains - Du droit à sa mise en oeuvre," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 7. However, it should be underlined that those transpositions can still differ and the principle of dual criminality is still considered by the Palermo Convention, Article 18.9. Moreover, exploitative offenses are often used to qualify trafficking, while they are not harmonized. Such practice will then hinder the possibilities of mutual assistance, M. Poelemans, I. Orbegozo Oronoz, "Forces et limites de la coopération franco-espagnole," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 67
[247] Article 10 of the protocol also considers information exchange, in particular regarding travel documents.
[248] B. Lavaud-Legendre, "La coopération répressive en matière de traite des êtres humains," *op. cit.* note 246, p. 8
[249] Article 18 of the Palermo Convention. Also: confiscation, Articles 13 and 14, extradition, Article 16, transfer of sentenced persons, Article 17, transfer of criminal proceedings, Article 21, and informal cooperation, Article 27.
[250] Article 18.3 of the Palermo Convention
[251] In case of emergency, oral requests can be made, Article 18.14 of the Palermo Convention
[252] The non-conformity to the detailed framework of the convention, the exception of public order, the application of the *non bis in idem* principle, and the impossibility to execute the request if it would be contrary to the legal order of the requested state, Article 18.21 of the Palermo Convention. It is possible

assistance is limited to human trafficking offenses that are "*transnational [and involve] an organized criminal group*."[253] The condition of transnationality is broadly understood in this article, "*including [when] evidence [is] located in the requested State Party*."[254] This definition is inconsistent with the notion of transnationality in Article 3.2 of the convention's scope, which broadens the possibilities for requesting mutual assistance. The requirement to prove the involvement of an organized criminal group is still a significant shortcoming, especially in light of cyber trafficking, which benefits sole traffickers. Another shortcoming is the lack of direct request communication, as in previous conventions.[255] A final problem is the absence of time limit for execution, mentioning only that the parties must execute the request, "*as soon as possible*."[256]

250. Sovereignty *versus* treaties. When sovereignty was theorized by Bodin, it was inalienable, prohibiting its transfer.[257] Therefore, the sovereign state could not oblige itself to reduce its powers.[258] For this reason, authors questioned the reduction of sovereignty due to the extension of international law,[259] and this question became particularly acute when studying criminal law, the acme of states' sovereignty.[260] Consequently, anti-trafficking treaties that create a framework for international cooperation could hinder states' sovereignty and autonomy. However, territorial classical sovereignty is facing transnational, globalized crime, including human trafficking. As this crime defies territorial limits, states must go beyond their borders and cooperate with their peers.[261] For this reason, treaties on criminal matters are a

to add that bank secrecy and fiscal matters cannot be invoked to refuse assistance, Article 18.8 and 22; and that the communication of government public records is mandatory, Article 18.29.a.

[253] Article 18.1 of the Palermo Convention

[254] Article 18.1 of the Palermo Convention

[255] Article 18.13 of the Palermo Convention

[256] Article 18.24 of the Palermo Convention

[257] O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, p. 190

[258] *Ibid.* p. 102. Similarly, Hobbes considers that the sovereign does not have to comply with the law, as it can always produce a new law to challenge the first one; and that any "*attempt by the sovereign to give away one of [the] rights [of sovereignty] should be regarded as void*," D. Dyzenhaus, "Kelsen, Heller and Schmitt: Paradigms of Sovereignty Thought," *Theoretical Inquiries in Law*, 2015, vol. 16, no. 2, p. 346

[259] N.-S. Politis, "Le problème des limitations de la souveraineté et la théorie de l'abus des droits dans les rapports internationaux (Volume 6)," *Collected Courses of the Hague Academy of International Law*, Brill, January 1, 1925, p. 61

[260] M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020, p. 44

[261] M. Poelemans, I. Orbegozo Oronoz, "Forces et limites de la coopération franco-espagnole," *op. cit.* note 246, p. 62; M. Massé, "Des figures asymétriques de l'internationalisation du droit pénal," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006, p. 755; J. Daskal, "Borders and Bits," *Vanderbilt Law Review*, 2018, no. 71, p. 226

defensive reaction to the evolution of crime, meant to effectively protect sovereignty.[262] In that sense, treaties are the "*state of law of globalization*."[263] Additionally, from a legal perspective, states play a role in the negotiation of and participation in these treaties. The decision to interact with the international community is a legal freedom[264] that could be distinguished from the natural and absolute freedom of states to order their internal affairs. In international law, all states are equal and are free to access international instruments; by conforming to treaties, the state obeys only itself.[265]

251. As the various shortcomings of the Palermo Protocol and Convention limit the effective protection of states' sovereignty, further frameworks for cooperation have been developed in Europe.

II. States' regional cooperation against trafficking and sovereignty

252. Cooperation in Europe. As with the Palermo Protocol, the Warsaw Convention promotes international cooperation,[266] but its scope is broader and is not limited to transnational and organized trafficking.[267] Nonetheless, partnerships can be seen as included in all parts, not as an autonomous one, of the global strategy.[268] Furthermore, no complete framework has been developed regarding extradition[269] or mutual assistance. On the contrary, the preamble of the convention refers to "*other*

[262] M. Massé, "Des figures asymétriques de l'internationalisation du droit pénal," *op. cit.* note 261, p. 758. Indeed, it is the origin of the concept of "transnational law" theorized by Philip Jessup, meaning applicable rules to a vertical legal situation that exceed the power of just one state on its own territory, G. Lhuilier, *Le droit transnational*, Dalloz, Méthodes du droit, 2016, pp. 6-7

[263] G. Lhuilier, *Le droit transnational*, *op. cit.* note 262, p. 18. René David emphasized in 1968 the need to understand how the "*international unification of law*" would occur, M. Delmas-Marty, "Le phénomène de l'harmonisation : L'expérience contemporaine," *in* B. Fauvarque-Cosson, D. Mazeaud (eds.), *Pensée juridique française et harmonisation européenne du droit*, Société de législation comparée, Droit privé comparé et européen no. 1, 2003, p. 39

[264] J. Combacau, "Pas une puissance, une liberté : la souveraineté internationale de l'Etat," *Pouvoirs*, 1993, no. 67, pp. 51-52. In that sense, exercising sovereignty to participate in international instruments reduces freedom but not the state's inherent power, J. Combacau, S. Sur, *Droit international public*, LGDJ, 2014, p. 261

[265] From this idea results the principle of *pacta sunt servanda*. Moreover, it should be noted that most of the treaties provide a way to denounce a treaty and therefore not be compelled to apply it anymore, Article 19 of the Palermo Protocol and Article 40 of the Palermo Convention.

[266] Article 1.1.c of the Warsaw Convention. Its sixth chapter is dedicated to the topic. However, this chapter only considers cooperation regarding endangered or missing persons, Article 33 of the Warsaw Convention; and feedback to requests and voluntary disclosure of information, Article 34. Elements of cooperation can also be found outside of this chapter: enticing direct communication between border authorities, Article 7.6; requests for verification of travel and identity documents, Article 9; collaboration for the identification of victims and their repatriation, Articles 10.2 and 16

[267] Article 2 of the Warsaw Convention

[268] Article 32 of the Warsaw Convention

[269] Although Article 31.3 of the Warsaw Convention provides for the principle *aut dedere aut judicare*, and Article 23.1 underlines that the level of sanction should give rise to extradition.

international legal instruments."[270] Similarly, the first anti-trafficking instruments of the European Community were focused mainly on cooperation,[271] but later texts, including the 2002 Framework decision[272] and the Directive 2011/36/EU, refer to general instruments on cooperation.[273]

253. EU criminal law *versus* sovereignty. Criminal texts adopted by the EU, including those to fight trafficking or foster cooperation,[274], have long questioned the sovereignty of member states.[275] From the first generation of ineffective texts after the 1992 Maastricht Treaty to the third generation of criminal norms since the 2007 Lisbon Treaty,[276] EU criminal law exists and is empirical. Thus, states are no longer in total control of their criminal legislation, and authors argue that the EU hinders states' criminal sovereignty.[277] In particular, Article 83.1 of the Treaty on the Functioning of

[270] M. Chawki, *La traite des êtres humains à l'ère numérique*, *op. cit.* note 57, p. 204. For the development of these norms, see *infra* 292 and 296 to 298.

[271] The first 1996 joint action was meant to "*develop coordinated initiatives*," Article 1.1 of the joint action 96/700/JHA, in particular for "*training, exchange programs and training courses, organization of multidisciplinary meetings and seminars, studies and research, dissemination of information*," Article 1.3. Article 7 provides for the creation of documentation networks. The second 1997 joint action considers the facilitation of extradition and mutual assistance, for example, underlining that the requests should be dealt with quickly, offering the possibility of "*direct transmission*," and requiring the appointment of a contact authority, Titles II.D, III.C to E of the joint action 97/154/JHA

[272] Except for the mention of the principle *aut dedere aut judicare*, Article 6.3 of the Council framework decision 2002/629/JHA. This text substitutes the 1997 joint action, Article 9.

[273] Paragraphs 8 and 9 of the preamble of the Council framework decision 2002/629/JHA and Paragraphs 12 and 13 of the preamble of the Directive 2011/36/EU. However, the latter does not mention tools for mutual legal assistance, which can be seen as an oversight (it only briefly mentions the European Arrest Warrant and the legal framework on cooperation for confiscation and seizure within a financial investigation).

[274] For a study of general texts on state cooperation, see *infra* 286 and followings.

[275] In addition to the general issue of whether or not the EU has sovereignty. It should be underlined that the question is not, however, the main subject of the thesis. As a result, it considers the existence of the EU legal framework in a pragmatic manner to deal primarily with the powers of the private sector, particularly digital actors, when confronted with the limits of the exercise of state sovereignty.

[276] M.-E. Morin, *Le système pénal de l'Union européenne*, Thesis, Université d'Aix-Marseille, November 28, 2017, ¶¶ 4-10; E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, Fondation Varenne, LGDJ, Collection des thèses no. 31, 2009, p. 441. The second generation corresponds to the adoption of framework decisions after the 1997 Amsterdam Treaty and to the explicit inclusion of criminal matters in the policies of the Community at the 1999 Tampere Program.

[277] E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 299. In particular, they invoke the absence of unanimity rules to adopt the EU texts, Articles 82 (procedural criminal matters), 83 (substantive criminal matters), and 294 (ordinary legislative procedure) of the Treaty on the Functioning of the EU; P. Mortier, *Les métamorphoses de la souveraineté*, Thesis, Université d'Angers, January 1, 2011, ¶ 726; E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 350. They criticize EU principles such as primacy, direct effect, and conform interpretation to EU law, G. Giudicelli-Delage, "Introduction générale," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 17. They question the legitimacy of the European Parliament regarding criminal matters, H. Satzger, "Le principe de légalité," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au*

the EU, the legal basis for adapting anti-trafficking texts, does not consider the principle of subsidiarity, implicitly considering EU-level norms to be indispensable without justification.[278] However, the EU is seen as the only solution to face globalization.[279] Gindre advocates for a "*divided*"[280] EU criminal sovereignty,[281], "*defined as a negative of state criminal sovereignty*."[282] As a result, it can be viewed as sharing criminal competencies rather than transferring state sovereignty.

254. Limited EU criminal sovereignty. Furthermore, the EU criminal sovereignty is limited by the subsidiarity and proportionality principles.[283] The former, known as a "*back-up law*,"[284] limits EU action to restrictive and attributed competencies when it is more effective.[285] The latter requires, from a substantive perspective, the necessity of the means adopted regarding the intended goals, and, from a formal perspective, the coherence of the entire system.[286] Moreover, harmonization is not unification, and

---

lendemain du Traité de Lisbonne, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, pp. 90-93

[278] Without setting any criteria, E. Gindre, "Discussion L'harmonisation pénale accessoire. Éléments de réflexion sur la place du droit pénal au sein de l'Union européenne," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 199

[279] R. Badinter, "Conclusion," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 331. In particular, by creating collective standards in the primary treaties, to avoid blockage during the adoption of norms, L. Bal, *Le mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Thesis, Université de Strasbourg, February 3, 2012, p. 246

[280] S. Braum, "'Rechtsstaat' and European criminal law – From the end of sovereignty," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 1, 2021, vol. 12, no. 1, p. 16. See also the notion of "*disaggregated sovereignty*" in A.-M. Slaughter, *A new world order*, Princeton University Press, 2004, pp. 19, 34

[281] E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 345

[282] E. Gindre, "Discussion," *op. cit.* note 278, pp. 202-203. Ginder emphasizes that states only lose the right not to punish when they are forced to create and sanction specific behaviors.

[283] Simon considers that the principle of proportionality is the main limit, P. Simon, *La compétence d'incrimination de l'Union européenne*, Thesis, Université Paris Est, Université du Luxembourg, Droit de l'Union européenne Thèses, 2019, ¶ 226

[284] X. Pin, "Discussion Subsidiarité versus efficacité," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, pp. 49-51

[285] E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 465; M. Van de Kerchove, "Le principe de subsidiarité," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 34; M.-E. Morin, *Le système pénal de l'Union européenne*, *op. cit.* note 276, ¶ 833

[286] C. Sotis, "Les principes de nécessité et de proportionnalité," *in* G. Giudicelli-Delage, C. Lazerges, Association de Recherches Pénales Européennes (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, pp. 59-65. It should be noted that the literature is not unified when

states still have a margin of appreciation,[287] particularly regarding directives.[288] Finally, the legislative power on criminal matters is not the only component of criminal sovereignty; it also includes the power to exercise jurisdiction, which the EU does not have.[289] Thus, the power of the EU could thus rely on the notion of "subreignty," in which "*States govern the Union, which in turn affects states […,] reflect[ing] a power over sovereign states that they voluntarily accept, but only in certain matters and under certain circumstances*."[290]

255. This definition of partnership is limited to sovereign states, but national laws that are designed to repress cyber trafficking face limitations in cyberspace.[291] Consequently, the global strategy against trafficking must include non-state actors.

§2. Second layer of partnerships: civil society

256. The second layer of the concept of partnership includes civil society, particularly NGOs.[292] Their role was already underlined in 1989 by the EU[293] and in

explaining the principle of proportionality, offering various interpretations, K. Nuotio, "A legitimacy-based approach to EU criminal law: Maybe we are getting there, after all," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 1, 2020, vol. 11, no. 1, p. 23; M.-E. Morin, *Le système pénal de l'Union européenne*, *op. cit.* note 276, ¶ 800

[287] E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 359

[288] The Directive 2011/36/EU definition of human trafficking did not preclude differences in national transpositions, S. Lannier, *Le blanchiment d'argent dans le cadre de la traite d'êtres humains en sa forme d'exploitation sexuelle : une approche comparative*, Master Dissertation, Université de Bordeaux and Vietnam National University, 2019, pp. 32-34 and see *supra* 19 and 20.

[289] E. Gindre, *L'émergence d'un droit pénal de l'Union européenne*, *op. cit.* note 276, p. 381. Nevertheless, the creation of the European Public Prosecutor's Office is questioning this last argument.

[290] P. Mortier, *Les métamorphoses de la souveraineté*, *op. cit.* note 277, ¶ 1011

[291] To which it is possible to add "*individual, material, and political oppositions*" to the implementation of cooperation, as well as corruption, B. Lavaud-Legendre, "La coopération répressive en matière de traite des êtres humains," *op. cit.* note 246, pp. 11-12

[292] Through this expression, it is possible to include associations specialized in the protection of victims. Cooperation with trade unions is at the core of the repression of trafficking for forced labor, GRETA, "Human trafficking for the purpose of labour explotation - Thematic Chapter of the 7th General Report on GRETA's Activities (covering the period from 1 January to 31 December 2017)," Council of Europe, October 2019, p. 29. It should be underlined that internal cooperation can be understood in a broader way. Indeed, various entities, even inside the structure of the state, will be necessary to repress human trafficking. For example, the financial approach to the offense will imply cooperation between law enforcement authorities specializing in trafficking and those focused on money laundering. When considering cybertrafficking, the former will also have to collaborate with authorities dedicated to cybercrime. Also, other institutions of the state have a role in this framework, such as labor inspectorates, border police, administrations managing reparations to victims, granting residence and work permits… Thus, the Palermo Protocol (Article 10) and the Warsaw Convention (Article 29.2) consider the necessary collaboration between state entities. Surprisingly, although the EU joint action 97/154/JHA provided for national coordination (Title II.H), the Directive 2011/36/EU does not mention this topic.

[293] European Parliament, "Resolution on the exploitation of prostitution and the traffic in human beings," EU, April 14, 1989, p. 352, OJ No C 120/2, p.352; European Parliament, *Resolution on trade in women*, *op. cit.* note 233, ¶ 2; European Parliament, *Resolution on trafficking in human beings*, *op. cit.* note 233,

1991 by the Council of Europe.[294] The 2003 Organization for Security and Co-operation in Europe (OSCE) plan of action[295] and UN resolutions[296] also highlighted the need for such cooperation. As the role of civil society is recognized in the literature and by the legal instruments (I), it questions state sovereignty (II).

I. The role of civil society

257. Civil society: role. Due to a criticized lack of state response,[297] NGOs are at the forefront of protecting and assisting trafficked victims, as well as raising awareness of human trafficking.[298] Consequently, the institutions in direct contact with victims are usually NGOs. These organizations are "*far more flexible than governmental structures*" and can "*harness voluntary initiative, transcend borders and societies, and wield moral authority*."[299] Since victims of trafficking might fear law enforcement

¶ 30; European Commission, *Trafficking in women for the purpose of sexual exploitation*, *op. cit.* note 233, p. 6; European Commission, "Communication to the Council and the European Parliament - For further actions in the fight against trafficking in women," EU, December 9, 1998, p. 1; Parliamentary Assembly, *Recommendation 1545 (2002)*, *op. cit.* note 234; European Commission, "Communication to the European Parliament and the Council - Fighting trafficking in human beings : an integrated approach and proposals for an action plan," EU, October 18, 2005, p. 10

[294] Committee of ministers, "Recommendation no. R (91)11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults," Council of Europe, September 9, 1991, ¶ A.b.11; Committee of Ministers, *Recommendation No. R (2000) 11*, *op. cit.* note 234, ¶¶ 6-7

[295] OSCE, *Decision No. 557*, *op. cit.* note 231, p. 2

[296] General Assembly, *Resolution 58/137*, *op. cit.* note 235, ¶¶ 3, 9; General Assembly, "Resolution 61/180. Improving the coordination of efforts against trafficking in persons," UN, December 20, 2006, ¶ 1; General Assembly, "Resolution 67/190. Improving the coordination of efforts against trafficking in persons," UN, December 20, 2012, p. 4

[297] To justify this situation, the authors mention "*significant budget constraints*," J. Todres, "The Private Sector's Pivotal Role in Combating Human Trafficking," *California Law Review Circuit*, 2012, vol. 3, p. 88; M. McSween, "Investing in the Business against Human Trafficking," *op. cit.* note 231, p. 292; European Commission, "Report on the progress made in the fight against trafficking in human beings as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims," EU, May 19, 2016, p. 15, COM(2016) 267 final; a lack of interest of the states, S.A. Limoncelli, "The global development of contemporary anti-human trafficking advocacy," *International Sociology*, SAGE Publications Ltd, November 1, 2017, vol. 32, no. 6, p. 822; the lack of compelling provisions on victims' assistance in the Palermo Protocol, A. Schloenhardt, R. Hunt-Walshe, "The Role of Non-Governmental Organisations in Australia's Anti-Trafficking in Persons Framework," *University of Western Australia Law Review*, 2013 2012, vol. 36, no. 1, p. 64; and the non application of existing frameworks, B. Lavaud-Legendre, "La traite des êtres humains comme objet de politique publique," May 2014, p. 9, online https://hal.archives-ouvertes.fr/hal-01188870 (retrieved on October 29, 2021)

[298] M. Tzvetkova, "NGO responses to trafficking in women," *Gender & Development*, Routledge, March 1, 2002, vol. 10, no. 1, p. 60. In France, see A. Dölemeyer, J. Leser, "Entre coopération et conflit," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, p. 48

[299] N. Godsey, "The Next Step: Why Non-Governmental Organizations Must Take a Growing Role in the New Global Anti-Trafficking Framework," *Regent Journal of International Law*, 2012 2011, vol. 8, no. 1, p. 43. Godsey also mentions that "*NGOs have the unique ability to address issues in a non-political and thereby potentially non-polarizing-manner*." However, most of the organizations advocating for victims and some of the organizations assisting victims have political goals or at least have a predetermined position on specific topics, such as the decriminalization or criminalization of sex work/prostitution.

authorities due to their administrative situation or a general lack of trust, NGOs are seen as a useful alternative to identify and help these victims.[300] Finally, NGOs can occupy a suitable place "*in executing anti-trafficking strategies*" due to their actions at the local level.[301] Consequently, one challenge is "*the quality of interactions between [civil society and] state actors*."[302] This division of competencies broadens the gap between institutions with a prosecution approach, such as(state justice entities, and those with a protection approach, such as civil society.[303] However, both need to cooperate to develop a comprehensive approach to repressing trafficking.[304]

258. Cooperation with civil society in legal texts. The three anti-trafficking supranational frameworks consider cooperation with civil society. The Palermo Protocol[305] recognizes the role of civil society in the assistance to victims,[306] in the adoption of prevention programs,[307] and in the training of law enforcement authorities.[308] The Warsaw Convention includes one article dedicated to the topic,[309] and the text is punctuated "*with references advocating for other private-public partnership efforts*."[310] Through its monitoring mechanism,[311] the Council of Europe

[300] M. Tzvetkova, "NGO responses to trafficking in women," *op. cit.* note 298, p. 61
[301] N. Godsey, "The Next Step," *op. cit.* note 299, p. 44; M. Darley, "Le statut de la victime dans la lutte contre la traite des femmes," *Critique internationale*, 2006, vol. 30, no. 1, p. 105
[302] B. Lavaud-Legendre, *Approche globale et traite des êtres humains - De l'« injonction à la coopération » au travail ensemble*, CNRS, July 1, 2018, p. 54, online https://halshs.archives-ouvertes.fr/halshs-02177213 (retrieved on October 29, 2021)
[303] A. Schloenhardt, R. Hunt-Walshe, "The Role of Non-Governmental Organisations in Australia," *op. cit.* note 297, p. 71
[304] The assistance of NGOs to victims is essential to build trust and place them in a safe environment in which they can accept giving testimony. The role of law enforcement authorities is essential to conducting the investigation for the criminal process to ensure the conviction of traffickers and reparations to the victims.
[305] It should be highlighted that many NGOs had a very important input in the negotiation of the protocol, A.T. Gallagher, "Trafficking in transnational criminal law," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 25
[306] Article 6.3 of the Palermo Protocol
[307] Article 9.3 of the Palermo Protocol
[308] Article 10.2 of the Palermo Protocol
[309] Article 35 of the Warsaw Convention
[310] M. McSween, "Investing in the Business against Human Trafficking," *op. cit.* note 231, p. 301. Cooperation with civil society should be developed for prevention measures, Article 5.6 of the Warsaw Convention; for measures to discourage the demand, Article 6.b; and to assist victims, Article 12.5. Going further, the convention highlights the opportunity to cooperate with civil society for identification procedures, Article 10.1; repatriation programs, Article 16.5; and to support the victims during the criminal process, Article 27.3.
[311] When evaluating countries, the GRETA takes into consideration the voices of local NGOs, M. van Doorninck, "Changing the system from within The role of NGOs in the flawed antitrafficking framework," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 428

recognized the lack of states' action on victims' protection[312] and the active role of NGOs.[313] Consequently, the GRETA requires the states to financially support NGOs[314] and to include them in the elaboration of national policies and training.[315] References to cooperation with civil society are more laconic in the EU framework. Although NGOs are mentioned in the Directive 2011/36/EU preamble,[316] specific provisions are very limited.[317]

259. National cooperation. At the national level, the formalization of this cooperation is variable. The 2003 OSCE Plan mentions the necessity of creating a national referral mechanism[318] "*through which state actors fulfill their obligations to protect and promote the human rights of trafficked persons, coordinating their efforts in a strategic partnership with civil society*."[319] In France, no similar mechanism or

[312] N. Le Coz, "Tu coopéreras sans retard et dans la plénitude de tes obligations Bilan sur les principales difficultés rencontrées dans la coopération internationale contre la traite des êtres humains," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 19

[313] Reports make it abundantly clear that civil society, particularly in France, does the majority of the work of assisting victims, GRETA, *France - Second evaluation round*, *op. cit.* note 209, ¶ 147; GRETA, *France - Third evaluation round*, *op. cit.* note 209, ¶ 225; a similar situation is to be found in Romania, GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, p. 5; in Spain, the measures of assistance seem to be distributed in a more balanced way between civil society and the state, GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Spain - Second evaluation round," Council of Europe, 2018, ¶ 153; GRETA, *Spain - Third evaluation round*, *op. cit.* note 209, ¶¶ 242-243

[314] GRETA, *France - Second evaluation round*, *op. cit.* note 209, ¶ 161; GRETA, *France - Third evaluation round*, *op. cit.* note 209, ¶ 226; GRETA, *Spain - Second evaluation round*, *op. cit.* note 313, ¶ 157; GRETA, *Spain - Third evaluation round*, *op. cit.* note 209, ¶¶ 248-255; GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, ¶¶ 207, 213. It has particularly been criticized the lack of measures on NGO funding in the Ministerio de Justicia et al., Anteproyecto de Ley Orgánica integral contra la trata y la explotación de seres humanos, 2022; I. Diez Velasco, "La protección de personas víctimas de trata en el anteproyecto de Ley Orgánica Integral contra la Trata y la Explotación de Seres Humanos: el caso de la infancia y las personas solicitantes de asilo," *IgualdadES*, June 20, 2023, vol. 8, p. 161

[315] GRETA, *France - Second evaluation round*, *op. cit.* note 209, ¶¶ 296-304; GRETA, *France - Third evaluation round*, *op. cit.* note 209, ¶¶ 181, 210; GRETA, *Spain - Second evaluation round*, *op. cit.* note 313, ¶¶ 277-280; GRETA, *Spain - Third evaluation round*, *op. cit.* note 209, ¶ 142; GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, ¶ 213

[316] Paragraph 6 of the preamble of Directive 2011/36/EU

[317] The directive only provides for "*cooperation with relevant support organizations*" for identification, assistance, and support of victims, Article 11.4 of the directive 2011/36/EU; for prevention (in particular information an awareness) measures, Article 18.2; and for "*gathering of statistics*," Article 19.

[318] OSCE, *Decision No. 557*, *op. cit.* note 231, ¶ V.3

[319] Office for Democratic Institutions and Human Rights, *National referral mechanisms - Joining efforts to protect the rights of trafficked persons - A practical handbook*, OSCE, 2nd ed., 2022, p. 14. Even though the framing body is usually not operational, it publishes and formalizes guidance for cooperation between state entities and civil society. It is possible to suppose that formalized cooperation would result in improved collaboration among all stakeholders; in that sense, national referral mechanisms are advocated for. But it should be underlined that the existence of written documents does not always mean a sudden and perfect collaboration, which also depends on other factors such as financial and human resources, interpersonal relationships, training, etc. Thus, the monitoring of those mechanisms is very important.

framework document exists,[320] resulting in fluctuating cooperation.[321] In Romania, a general framework is provided, in which NGOs are the main actors in the mechanism for victim identification.[322] In Spain, the 2011 framework protocol exists for the identification and protection of trafficked victims, establishing a division of competencies among all stakeholders.[323] The protocol has been updated and adapted to the local necessities;[324] nevertheless, some of these protocols remain dedicated to trafficked victims for sexual exploitation, limiting a comprehensive approach.[325]

260. Cooperation with civil society is necessary to improve the protection of victims and, thus, the fight against trafficking. Nevertheless, such cooperation questions the impact of the distribution of competencies on sovereignty.

II. Civil society cooperation and sovereignty

261. The role of civil society in the identification of victims. Sovereignty

[320] There are some guides available to share good practices on identification and assistance, such as those from an association, Association ALC, "Identifier, accueillir et accompagner les victimes de la traite des êtres humains - Guide pratique," Dispositif National Ac.Sé, République française, February 2014; or from a researcher and expert on the field, B. Lavaud-Legendre, *Guide d'identification et d'orientation des victimes de traite des êtres humains*, COMPTRASEC, June 2016

[321] B. Lavaud-Legendre, *Approche globale et traite des êtres humains*, *op. cit.* note 302, p. 125. With the exception of initiatives developed to solve a specific problem, such as at the local level or with the Ac.sé initiative, to accommodate victims in danger through a geographical displacement, managed by an association but legally recognized through a convention with the ministry of social action, Article R425-8¶2 of the Code de l'entrée et du séjour des étrangers et du droit d'asile

[322] The framework includes a task and role distribution as well as the sharing of common indicators and models of document, Agenţia Naţională Împotriva Traficului de Persoane, "National Identification and Referral Mechanism of Victims of Trafficking in Persons," Romania, 2019. Its implementation, on the other hand, has been criticized due to a lack of financial and human resources within the Agenţia Naţională Împotriva Traficului de Persoane, GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, ¶ 193

[323] Ministerio de Justicia et al., "Framework protocol for protection of victims of human trafficking," Spain, October 28, 2011, ¶ XV. See also, on the identification process, C. Azcárraga Monzonís, "La mujer inmigrante en la extranjería y el asilo," *El principio de igualdad ante el derecho privado: una visión multidisciplinar*, Dykinson, 2013, pp. 254-256

[324] For instance, the protocol of Valencia City is to be highlighted as one of the most recent (2017), with a detailed diagram of the steps of identification and assistance and a list of all relevant actors, Regidoria d'igualtat i polítiques inclusives, "Protocolo de intervención con víctimas de trata para la explotación sexual en la ciudad de València," Ajuntament de València, Spain, April 2017, p. 18. Similarly, the Community of Madrid offers a detailed protocol, with a list of the competences of numerous associations, Dirección General de la Mujer, "Protocolo para la protección de las víctimas de trata de seres humanos en la comunidad de Madrid," Comunidad de Madrid, Spain, November 2017, pp. 48-49

[325] See, for example, the protocols of Galacia, Extremadura and Navarra, Delegación del Gobierno contra la Violencia de Género, "Protocolos de Coordinación Interinstitucional," *Ministerio de Igualdad*, no date, online https://violenciagenero.igualdad.gob.es/otrasFormas/trata/normativaProtocolo/marco/home.htm (retrieved on December 2, 2021)

highlights the primary role of states to protect their population.[326] As the assistance of trafficked victims is heavily reliant on the work of NGOs, the state's sovereignty is argued to be eroding.[327] However, NGOs still depend on national frameworks;[328] in particular, only the state can officially identify trafficked victims. In Spain, the framework protocol stipulates that formal identification is made only by police units,[329] although other actors, including NGOs, can refer victims to the police.[330] Similarly, the French law permits the identification of foreign victims only by police or *gendarmerie* services.[331] On the contrary, in the new Romanian National Identification and Referral Mechanism, all relevant actors, including NGOs, are able to identify victims,[332] which

[326] It should be underlined that protection of witnesses is still a prerogative of the state, M. Tzvetkova, "NGO responses to trafficking in women," *op. cit.* note 298, p. 62

[327] One author also mentions a "*danger to democracy because they wield governmental influence that is not counterbalanced by democratic mechanisms of accountability*," N. Godsey, "The Next Step," *op. cit.* note 299, p. 53

[328] M. Tzvetkova, "NGO responses to trafficking in women," *op. cit.* note 298, p. 64. In particular, few options exist to protect those with an undocumented or temporary administrative status, P. de Montvalon, "« Venir ici n'est pas gratuit ! » Négocier un passage aux frontières extérieures et intérieures de la France pour des prostituées nigérianes," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, p. 37

[329] Ministerio de Justicia et al., *Framework protocol for protection of victims of human trafficking*, *op. cit.* note 323, ¶ VI.A.1, despite the fact that Article 59 bis.1 of the Ley Orgánica 4/2000 sobre derechos y libertades de los extranjeros en España y su integración social provides for the identification of victims by any "*competent authorities*." On the contrary, regarding non-EU victims, it is explicitly stated that the identification can only be done by law enforcement authorities, Article 141.2 of the Reglamento de la Ley Orgánica 4/2000.

[330] *Ibid.* ¶ V.D.1. Despite the broadening of actors that can identify trafficked, the referral mechanims in the project of comprehensive law against human trafficking still gives a prevalent role to law enforcement authorities, C. Villacampa Estiarte, "Acerca del Anteproyecto de Ley Orgánica Integral contra la Trata y la Explotación de Seres Humanos," *Diario La Ley*, Wolters Kluwer, 2023, no. 10267, p. 1

[331] Article R425-1 of the Code de l'entrée et du séjour des étrangers et du droit d'asile. That results in huge differences between the data from the state regarding the number of victims, and the data from associations, A. Sourd, L. Benaddou, L. Vignolles, *La traite des êtres humains en France Le profil des victimes suivies par les associations en 2021*, Service statistique ministériel de la sécurité intérieure, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, 2022; Service statistique ministériel de la sécurité intérieure, "La traite et l'exploitation des êtres humains depuis 2016 : une approche par les données administratives," *Interstats*, October 2022, no. 49, p. 1. A similar gap is criticized in Spain, C. Villacampa Estiarte et al., "Dimensión de la trata de seres humanos en España," *in* C.V. Estiarte, A.P. Gargallo (eds.), *La trata de seres humanos tras un decenio de su incriminación: ¿es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, 2022, pp. 181-216

[332] Such identification is direct for law enforcement authorities, who must only notify the National Agency against Human Trafficking, Agenţia Naţională Împotriva Traficului de Persoane, *National Identification and Referral Mechanism of Victims of Trafficking in Persons*, *op. cit.* note 322, p. 36. It is indirect when the victim is detected by other actors: the detection is notified to the agency, and a posterior interview is run to officially identify the person as a victim, either by the Regional Centers of the National Agency or by a NGO. Those interviews can also be done by the General Directorate for Social Assistance and Child Protection and the International Organization for Migration, *Ibid.* pp. 41-43. Once identified, those institutions will refer the victims to the protection and assistance program, *Ibid.* pp. 75 and following. This mechanism no longer relies on informal and formal identification, the latter of which is restricted to law enforcement authorities, GRETA, "Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Romania - Second evaluation round," Council of Europe, 2016, ¶¶ 96-97

provides civil society with additional power to ensure the rights of trafficking victim. At the same time, this process seems better integrated in the national framework, thus protecting states' sovereignty by maintaining control over the entire process through a national agency.[333]

262. Limited role of civil society. Moreover, civil society is still confined to the prevention of the crime, particularly through lobbying, and assistance of victims. NGOs have little do not have much power to influence the prosecution, the acme of states' sovereignty, which is underlined in supranational and national texts.[334] Additionally, various studies highlight that most NGOs are engaged only in public education and

[333] It is very explicit at Article 27^2 of the Lege privind prevenirea și combaterea traficului de persoane: "*1. To improve the access of victims of trafficking in human beings to assistance and protection services, non-governmental institutions and organizations with responsibilities in this field shall cooperate with a view to implementing the National Mechanism for the Identification and Referral of Victims of Trafficking in Persons. […] 3. The monitoring of the functioning of the National Mechanism for the identification and referral of victims of trafficking in human beings is ensured by the National Agency against Trafficking in Persons*"

[334] It is very clear in the 2003 OSCE Action Plan that NGOs are primarily mentioned in the prevention and protection fields, OSCE, *Decision No. 557*, *op. cit.* note 231, pp. 10-14. However, they are briefly mentioned in the prosecution part as being able to "*support victims in court hearings*," *Ibid.* p. 5. In the 2013 updated plan, they are mainly limited to the protection part of the strategy and very briefly mentioned in the partnership section without development, OSCE, *Decision n° 1107*, *op. cit.* note 231, pp. 6-7. It is even clearer in the 2010 UN global strategy, in which they are not even mentioned in the partnership section but only broadly mentioned for prevention, General Assembly, *Resolution 64/293*, *op. cit.* note 227, ¶¶ 18, 23 (annex); and protection, *Ibid.* ¶¶ 29, 32, 40 (annex), see also in the updated plan, General Assembly, *Resolution 72/1*, *op. cit.* note 227, ¶ 8. The same assessment is made in the 2021 UN report, which emphasizes cooperation with civil society mostly for detection and assistance to victims, Secretary-General, "Report. Improving the coordination of efforts against trafficking in persons," Crime prevention and criminal justice, UN, June 28, 2021, ¶ 31, A/76/120; and in the 2021 EU strategy, principally mentioning civil society for awareness campaigns and protection of victims, European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," EU, April 14, 2021, pp. 5, 6, 10, 13, 14, COM(2021) 171 final. Also, if efforts have been made to improve investigation at the supranational level, no similar institution exists, in particular at the European level, regarding victim protection, M. Malloch, P. Rigby, "Contexts and Complexities," *in* M. Malloch, P. Rigby (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, p. 6. This trend is also to be found in national action plans. The French action plan recognizes the role of associations for prevention (Measure 3), identification (Measure 16), and protection (Measures 22, 29, and 30), but also their expertise for gathering data (Measure 8) and for training (Measures 13, 14, and 19), Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, "2nd plan d'action national contre la traite des êtres humains 2019-2021," France, 2019. The limited action of NGOs is also very clear in the Romanian action plan, although its adds "*involvement of civil society members in the decision-making process*," Guvernul, "Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022," Romania, October 31, 2018, p. 19. In Spain, civil society's role is limited to detection and assistance (Measures 2.2.B regarding identification, 2.3.C, E and F and 4.1.A regarding referral after identification for assistance, 4.2.A regarding international cooperation, 4.3.A to E in particular), Centro de inteligencia contra el terrorismo y el crimen organizado, "Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023," Secretaría de Estado de seguridad, Ministerio del Interior, Spain, January 2022

awareness, while, for example, only 27–29% of NGOs are providing shelter.[335] Finally, civil society faces practical obstacles such as budget constraints[336] and the focus on social and administrative assistance.[337] NGOs mostly remain under the control of the state through a dependence on its funding[338] as well as a reliance on "*private sector funding*."[339] They also have limited technical resources to fight against cyber trafficking. One association in France mentioned realizing cyber roaming, with few results.[340]

263. Consequently, due to the expertise and data needed, the policy and legal framework to repress cyber human trafficking turned to the business sector.

§3. Third layer of partnerships: business sector

264. The necessary cooperation with the business sector[341] was the last step in the

[335] S.A. Limoncelli, "What in the World Are Anti-Trafficking NGOs Doing? Findings from a Global Study," *Journal of Human Trafficking*, Routledge, October 1, 2016, vol. 2, no. 4, p. 323; K. Foot, "Actors and activities in the anti–human trafficking movement," *in* J. Heine, R.C. Thakur (eds.), *The dark side of globalization*, UN University Press, 2011, p. 260; M. Tzvetkova, "NGO responses to trafficking in women," *op. cit.* note 298, p. 62

[336] J. Todres, "The Private Sector's Pivotal Role," *op. cit.* note 297, p. 88. In particular in Spain, see N. Torres Rosell, C. Villacampa Estiarte, "Protección jurídica y asistencia para víctimas de trata de seres humanos," *Revista General de Derecho Penal*, Iustel, 2017, no. 27, pp. 32-34

[337] M. Jakšić, N. Ragaru, "Réparer l'exploitation sexuelle. Le dispositif d'indemnisation des victimes de traite en France," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, p. 128

[338] S. Birkenthal, "Human Trafficking: A Human Rights Abuse with Global Dimensions," *Interdisciplinary Journal of Human Rights Law*, 2012 2011, vol. 6, no. 1, p. 36; M. Darley, "Le statut de la victime dans la lutte contre la traite des femmes," *op. cit.* note 301, p. 108. It should also be noted that there is a North/South divide because "*Funding is often coming from countries in the Global North and anti-trafficking INGOs based in the north are often working in countries of the Global South*," S.A. Limoncelli, "What in the World Are Anti-Trafficking NGOs Doing?," *op. cit.* note 335, pp. 324-325; S.A. Limoncelli, "The global development of contemporary anti-human trafficking advocacy," *op. cit.* note 297, p. 817. Consequently, to continue their work, they must overcome obstacles such as their independence from state policies on human trafficking, M. van Doorninck, "Changing the system from within," *op. cit.* note 311, pp. 422-425, 455. And an NGO's "success" is determined by its ability to provide effective assistance, P. de Montvalon, "« Venir ici n'est pas gratuit ! »," *op. cit.* note 328, pp. 42-43

[339] M. McSween, "Investing in the Business against Human Trafficking," *op. cit.* note 231, p. 292

[340] The association received only 143 answers for the 1,642 SMS and emails sent, Amicale du Nid, *Rapport d'activité 2018*, June 2019, p. 10. Such technique does not seem to have been developed even during the lockdown due to the pandemic; the 2020 report only mentions the contact with sex workers through the Internet by the regional association in Bretagne (2,436 persons contacted with no information on the results), Amicale du Nid, *Rapport d'activité 2020*, June 2021, pp. 42, 76. Those techniques are to be developed according to the French plan of action against minor prostitution, Gouvernement, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, France, November 15, 2021, p. 6

[341] It can be hard to distinguish between all the notions used to talk about non state actors involved in the repression of trafficking. Literature mentions civil society, the private sector, the business sector, corporations, NGOs, associations, etc. In the preceding paragraph, civil society, specifically NGOs, was defined as entities whose primary goal was victim protection or prevention. On the contrary, the private sector seems to represent a different category, including corporations and profit-seeking entities. However, the private sector can also be understood legally as any entities that are not part of the state, the opposite of the public sector. To not rely on that blurry distinction, for example, considering corporations owned partly by the state, the paragraph will rely on the notion of the business sector,

extension of the partnership framework in the anti-trafficking global strategy.[342] The business sector is known to have a "*crucial role*"[343] in developing innovative ideas and solutions. Indeed, the sector, particularly transnational corporations, has access to resources that states and civil society lack,[344] and, like civil society, private actors might be more flexible than the state.[345] From the business sector perspective, being involved with trafficking processes can create "*reputational and financial risks to their operations*."[346] As a result, the texts introduced this sector as one of the actors in the partnerships to fight human trafficking (I), including the digital sector specifically against cyber trafficking (II).

I. Introducing the business sector to the repression of human trafficking

265. Recognition of the business sector's role. Early in the 20th century, the 1921 convention underlined the need for states to consider, "*licensing and supervision of employment agencies*."[347] Nevertheless, the first mentions related to supervision by

underlying that their primary objective is not the repression of human trafficking but developing profit. See, for example, General Assembly, *Resolution 72/1*, *op. cit.* note 227, ¶ 25.

[342] M.P. Lagon, "The Global Abolition of Human Trafficking: The Indispensible Role of the United States," *Georgetown Journal of International Affairs*, 2011, vol. 12, no. 1, p. 96. "*Just as in the nineteenth-century businesses played a crucial role in the antislavery agenda*," K. Bales, A. Gardner, "Free Soil, Free Produce, Free Communities," *in* D.W. Blight, G. LeBaron, J.R. Pliley (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, p. 88

[343] C. Bain, "Entrepreneurship and Innovation," *op. cit.* note 232, p. 81; J. Todres, "The Private Sector's Pivotal Role," *op. cit.* note 297, pp. 86-88

[344] M. McSween, "Investing in the Business against Human Trafficking," *op. cit.* note 231, p. 288; Special Rapporteur on trafficking in persons, especially women and children, "Report," General Assembly, UN, August 7, 2012, ¶ 31, A/67/261

[345] The state can be limited by "*mandatory bureaucratic policies*," M. McSween, "Investing in the Business against Human Trafficking," *op. cit.* note 231, p. 293

[346] Special Rapporteur on trafficking in persons, especially women and children, *Report*, *op. cit.* note 344, ¶ 29; Q. Lake et al., *Corporate leadership on modern slavery: How have companies responded to the Modern Slavery Act one year on?*, Hult International Business School & Ethical Trading Initiative, 2016, p. 21. However, such reputational risk can be limited, considering that the role of corporations is sometimes limited to their use by traffickers or money launderers in the framework of an organized criminal group, I. de Vries, M.A. Jose, A. Farrell, "It's Your Business: The Role of the Private Sector in Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 750. See, for example, in OSCE, *Decision No. 557*, *op. cit.* note 231, p. 2. In that sense, the objective of the business is to make sure that it is not used by those kinds of groups, while partnerships with the business sector should be broader.

[347] Article 6 of the 1921 convention. This idea remained in the 1950 convention, Article 20. Such ideas of regulating specific sectors persisted in the gray literature and highlighted the need to supervise new sectors such as "*marriage and adoption agencies*," Committee of ministers, *Recommendation no. R (91)11*, *op. cit.* note 294, ¶ D.1; "*'folk artists', dancers, au-pairs[, …] chambermaids [and] show-business agencies*," European Parliament, *Resolution on trafficking in human beings*, *op. cit.* note 233, ¶ 17; or "*domestic workers*," Parliamentary Assembly, "Recommendation 1663 (2004) Domestic slavery: servitude, au pairs and mail-order brides," Council of Europe, June 22, 2004, ¶ 6.2.b. An interesting point is that "*Persons responsible for an Internet agency site [should be] clearly identifiable and that*

the state and did not support real partnerships. Afterward, there were few mentions of the role of businesses in repressing trafficking[348] until finally, in 2008, a United Nations resolution generally included the private sector in its scope of cooperation.[349] This idea was then introduced in the UN's 2010 global strategy.[350]

266. The business sector in international frameworks. The Palermo Protocol provides only for the possibility of cooperating with commercial carriers;[351] the Warsaw Convention includes a similar measure[352] and further mentions the role of the media.[353] The third round of GRETA evaluation considers a cross-cutting issue on collaboration with the business sector.[354] For example, Romania mentioned a partnership with the Romanian Federation of the Hotel Industry to raise awareness in this sector.[355] Although the Directive 2011/36/EU does not mention cooperation with the business

users of the site [should be] obliged to identify themselves, following up marriages and providing an emergency contact number," *Ibid.* ¶ 6.4.b.

[348] They were limited to the prevention framework. It is very clear from the Secretary-General, *Report. Improving the coordination of efforts against trafficking in persons*, *op. cit.* note 334, ¶ 13. Prevention could be understood as measures to prevent human trafficking by the business sector, see, for example, OSCE, *Decision nº 1107*, *op. cit.* note 231, p. 3 (Point 1.7); but also measures to raise awareness among at risk sectors implemented by the state, *Ibid.* p. 4 (Points 1.12 and 2). Those mentions particularly focused on the role of the media, European Parliament, *Resolution on the exploitation of prostitution and the traffic in human beings*, *op. cit.* note 293, ¶ 4; Committee of ministers, *Recommendation no. R (91)11*, *op. cit.* note 294, ¶ A.a.5; Committee of Ministers, *Recommendation No. R (2000) 11*, *op. cit.* note 234, ¶ 8; Parliamentary Assembly, *Recommendation 1545 (2002)*, *op. cit.* note 234, ¶ 10.g; OSCE, "Decision No. 557/Rev.1: OSCE Action Plan to Combat Trafficking in Human Beings," July 7, 2005, p. 2, PC.DEC/1107/Corr.1. Other authors only consider broad sentences with no detail on the targeted actors. For example, the 1991 Resolution of the Council of Europe "*encourage[s] cooperation between the police and all public and private organizations*," Committee of ministers, *Recommendation no. R (91)11*, *op. cit.* note 294, ¶ A.b.8

[349] General Assembly, "Resolution 63/194. Improving the coordination of efforts against trafficking in persons," UN, December 18, 2008, ¶ 6

[350] General Assembly, *Resolution 64/293*, *op. cit.* note 227, pp. 3, 4. See also the 2013 updated OSCE plan, OSCE, *Decision nº 1107*, *op. cit.* note 231, p. 7. However, the paragraph only broadly mentions cooperation for "*prevention and protection policies and programs*," General Assembly, *Resolution 64/293*, *op. cit.* note 227, ¶ 53 (annex). Similarly, see General Assembly, *Resolution 67/190*, *op. cit.* note 296, ¶ 6.

[351] To prevent the use of their means of transport by traffickers and victims, in particular by "*ascertain[ing] that all passengers are in possession of the travel documents required for entry*," Article 11 of the Palermo Protocol

[352] However, this role is limited "*to protect the private life and identity of victims*," Article 7.3 of the Warsaw convention

[353] Article 11.3 of the Warsaw Convention

[354] "*What steps are taken to ensure that private entities take steps to prevent and eradicate trafficking from their business or supply chains and to support the rehabilitation and recovery of victims? What options exist for victims of trafficking to access effective remedies from businesses implicated in human trafficking?*," GRETA, "Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties Third evaluation round Thematic focus: Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, 2018, p. 7

[355] GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, ¶ 161

sector,[356] its latest strategy underlines the need to foster, "*the development of public-private initiatives with businesses in high-risk sectors*."[357]

267. The cooperation framework between states and the business sector remains limited, but strong partnerships will be needed with digital actors to improve the fight again cyber human trafficking.

II. Introducing the role of digital actors to repress human trafficking

268. Digital actors and trafficking: international considerations. While the literature acknowledges the importance of new technologies in creating additional forms of trafficking, the call for international cooperation remains limited. The attention is drawn to means rather than actors. The EU 1996 Joint Action asked for a study on how "*to prevent the use of telecommunications facilities, including the Internet system, for the purposes of trade in human beings*."[358] In 2005, the OSCE underlined that Interpol should address "*the use of the Internet in facilitating the trafficking of children for sexual exploitation*."[359] Since 2013, the focus has been broadened to include the "*use of the Internet and other information and communication technologies (ICTs) for committing*"[360] all forms of human trafficking; partnerships are explicitly encouraged with "*ICT companies and Internet service providers*."[361] Finally, the United Nations considered "*the importance for Member States to develop effective cooperation [with] Internet service providers*"[362] in 2018. Only in 2021 did the EU explicitly mention

[356] It should be noted that Article 18.2 of Directive 2011/36/EU considers collaboration with any type of stakeholder on the topic of prevention.
[357] The text mentions in particular the "*hospitality, garment, fishing, agriculture and construction*" sectors, as well as "*global supply chains*," European Commission, *EU Strategy on Combatting Trafficking in Human Beings 2021-2025*, *op. cit.* note 334, p. 7
[358] Article 6 of the Joint Action 96/700/JHA. Already in 1989, the European Parliament mentioned the role of pornographic video films and telephone messages in picturing women, European Parliament, *Resolution on the exploitation of prostitution and the traffic in human beings*, *op. cit.* note 293, ¶ M
[359] OSCE, *Decision No. 557/Rev.1*, *op. cit.* note 348, p. 2 Addendum
[360] OSCE, *Decision nº 1107*, *op. cit.* note 231, pp. 2, 3 (Points 1.4 and 4)
[361] *Ibid.* p. 8 (Point 6). On the contrary, the United Nations' repeated calls to understand the role of new technologies in trafficking do not mention partnerships with digital actors, General Assembly, *Resolution 72/1*, *op. cit.* note 227, ¶ 22; see also UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, *op. cit.* note 206. It only mentions the opportunity to "*develop targeted awareness raising campaigns, including for […] front line service providers and at risk industries*," General Assembly, "Resolution 72/195. Improving the coordination of efforts against trafficking in persons," UN, December 19, 2017, ¶ 14
[362] Commission on Crime Prevention and Criminal Justice, "Resolution 27/2 Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies," Economic and Social Council, UN, 2018, ¶ 4

collaboration with digital actors.[363] However, these mentions are still scarce and are limited to a broad call for cooperation with the business sector.

269. Digital actors and trafficking: national considerations. At the national level, cooperation with digital actors is on the rise but remains limited. One French action plan focuses on the cooperation with accommodation websites,[364] particularly in notifying suspect behaviors[365] (cooperation originated by digital actors) and responding to law enforcement authorities' requests (cooperation originated by law enforcement authorities).[366] However, the plan is limited to specific actors and to a specific offense: trafficking for sexual exploitation of minors. In Romania, the role of the Internet in human trafficking is recognized in the country's action plan,[367] but it does not mention the need to cooperate with digital actors. Nevertheless, the National Agency against Trafficking in Persons concluded two collaboration protocols with digital actors in 2020.[368] The second Spanish action plan generally considers the need to better detect cyber trafficking without mentioning the role of digital actors.[369]

270. Current role of digital actors. Partnerships with digital actors remain at the margins of the anti-trafficking framework, thereby preventing proper consideration of

---

[363] Despite the role of cyberspace already mentioned in the prior strategy, European Commission, "Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016," EU, June 19, 2012, p. 16, COM/2012/0286 final. The new strategy recognizes that "*Internet service providers and related companies are part of the solution*," European Commission, *EU Strategy on Combatting Trafficking in Human Beings 2021-2025*, *op. cit.* note 334, p. 11. Nevertheless, their role is very specific, limited to the "*identification and removal of online material associated with exploitation and abuse of trafficked victims*," while the business sector is broadly called for "*the development of technology-based solutions to support prevention and combatting of trafficking in human beings*."

[364] See, for example, Airbnb, "Airbnb soutient le travail du Gouvernement contre la prostitution," *Airbnb Newsroom*, November 15, 2021, online https://news.airbnb.com/fr/airbnb-soutient-le-travail-du-gouvernement-contre-la-prostitution/ (retrieved on November 20, 2021); GRETA, *France - Third evaluation round*, *op. cit.* note 209, ¶ 208

[365] Gouvernement, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, *op. cit.* note 340, p. 6

[366] *Ibid.* p. 9

[367] Guvernul, *Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022*, *op. cit.* note 334, pp. 4-5, 8. The strategy highlights recruitment through the Internet and exploitation in the pornography sector.

[368] "*OLX Romania (the largest advertising platform in Romania) [and] the dating platform Sentimente.ro*," GRETA, *Romania - Third evaluation round*, *op. cit.* note 209, ¶ 162

[369] Mere mention of the private sector, Measures 1.2.D and E, Centro de inteligencia contra el terrorismo y el crimen organizado, *Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023*, *op. cit.* note 334. The first action plan only mentioned cooperation with communication media, Ministerio de Sanidad, Servicios Sociales e Igualdad, "Plan integral de lucha contra la trata de mujeres y niñas con fines de explotación sexual 2015-2018," Spain, 2014, p. 58, Measures 9 and 12. Spain highlighted its relationships with private actors through corporate social responsability in its last report by the GRETA, GRETA, *Spain - Third evaluation round*, *op. cit.* note 209, ¶ 165. On this topic, see *infra* Part 2. Title 2. Chapter 1.

their actual opportunities to help investigate cyber human trafficking. Given digital sovereignty[370] and the evolution of traffickers' methods of operation, digital actors can gain access to the data required to prove cyber trafficking offenses. The same data that law enforcement agencies struggle to obtain is part of the services and source of profits for digital actors. Improved collaboration with these entities could save time and resources, improve evidence quality, and allow for earlier identification and protection of victims. However, digital actors, such as the business sector in general and civil society, remain limited to a primary role of prevention.

271. Conclusion of the section. Facing the limits of sovereignty in the repression of human trafficking, states have recognized the need to cooperate at the supranational level. Original and current texts highlight mutual assistance while leaving state sovereignty untouched. Applying a pragmatic approach, states acknowledge their limits within their own borders by enhancing cooperation with civil society, particularly for the protection of victims. However, states and civil society does not appear to be the appropriate partners to repress cyber trafficking. Consequently, although in a limited manner, the business sector—especially the digital sector—was included in the partnerships to repress human trafficking. To better prosecute this phenomenon, other legal investigative frameworks can be used, questioning the respective powers of states and digital actors.

272. Conclusion of the chapter. Despite criminal law being the pinnacle of states' sovereignty, the regulation and implementation of states' digital investigative techniques seem unstable. As the state attempts to adapt its legal framework to investigate potential crimes in cyberspace, it becomes more and more fragile. This appears to be the balance that must be struck with respect to fundamental rights. These techniques have a significant impact on the right to privacy. The legal standards of the ECHR that allow the use of these techniques to be necessary in a democratic society are generally met, but when detailing the frameworks, numerous elements of nonconformity with the ECHR case law continue to arise. Similarly, evidence must conform to the requirements of the court for a fair trial, underscoring the thin line between cyber-infiltration and entrapment. This instability is increased due to the frequent evolution of both national legislation and case law. However, the legal

[370] See *infra* 50.

framework on this topic cannot be studied in the abstract. The implementation of the techniques requires certain human and material resources that states might lack or might be unwilling to gather to investigate human trafficking. To summarize, the state's framework to prosecute cyber trafficking seems highly unstable and is limited in its implementation. For this reason, the legal possibilities offered by the state can be complemented by other powers to improve the repression of trafficking. From the outset, the anti-trafficking strategies recognized the necessity of state cooperation, and the importance of civil society in the protection of victims is also salient. Recently, the role of the business sector in fighting cyber trafficking has been increasingly mentioned. As the sovereignty of the state does not appear to be sufficient to comprehensively repress cyber trafficking, digital actors are stepping up as needed partners. Thus, other frameworks will support cooperation between states and digital actors, which is useful to investigate trafficking.

Chapter 2. The extension of sovereignty to face cyber human trafficking

273. Sovereignty was theorized to characterize the modern state as "*dispossessing the autonomous, 'private' agents of […] power who exist in parallel to him*."[1] However, the limitations of the state's legitimate coercion question its role as the primary actor in the fight against cyber human trafficking. To ensure an efficient fight against this phenomenon, the state cannot be seen as an independent actor any longer; it must cooperate with other states and non-state actors. However, in conducting its investigation, the state appears to have lost its powers due to the need for data as evidence, which is owned by digital actors. Consequently, states can rely on national and international frameworks, both old and new, for collaboration to improve the repression of trafficking (Section 1). However, all of these frameworks face limitations in efficiently securing data for trafficking investigation. They are still framed by the application of classical mutual legal assistance in the relationships among a state, a territorial link, and a digital actor, or between a state and a digital actor via another state. For this reason, the challenges around data requests to digital actors seem to recognize the birth of another type of sovereignty, highlighted by forms of autonomous cooperation and co-regulation. This autonomy supports not only a lack of interference from other sovereigns but also the exercise of their own external and internal powers, underscoring the fragmentation of coercion[2] and the necessity for new forms of cooperation (Section 2).

Section 1. State cooperation with digital actors to repress cyber trafficking

274. To strengthen cooperation with digital actors to obtain data as evidence to repress cyber trafficking, most of the existing frameworks, both national and supranational, have been deemed ineffective (§1). As a result, innovative solutions have been developed, although they still seem ill-fitted to the purpose of securing

[1] M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, tran. R. Livingstone, p. 37

[2] J. Black, "Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world," *Current Legal Problems*, Oxford University Press, February 21, 2001, vol. 54, no. 1, pp. 106-110

digital evidence, especially in the context of the prosecution of trafficking processes (§2).

§1. Ineffective classical tools to cooperate with digital actors

275. Cooperation with the business sector is not a recent challenge for law enforcement authorities. General frameworks already exist to require their collaboration, including through national regulations (I) and procedures of mutual assistance (II). Nonetheless, these frameworks seem unsuitable for efficiently cooperating with digital actors, particularly to obtain data to better prosecute cyber trafficking.

I. Weak national frameworks to cooperate with digital actors

276. To request the assistance of the business sector, especially digital actors, states can rely on their own national frameworks (A). Indeed, authors highlight a "*trend towards more unilateral action and the preference of many states for direct cooperation with private actors*."[3] However, this trend is challenged by the acquisition of data from multinational digital actors (B).

A. National classical obligations of cooperation

277. Cooperation to implement digital investigative techniques. Two types of cooperation with digital actors can be highlighted in the national frameworks studied to better repress cyber trafficking.[4] First, states rely on digital actors to implement digital investigative techniques. In France, no general regime of cooperation exists, but all techniques include provisions for digital actors to implement them when they are in charge of the infrastructure or the data.[5] It should be noted that the French code does

[3] V. Franssen, D. Flore, "Introduction : le droit pénal à l'ère numérique," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 14

[4] As in the prior chapter, the legislations of France, Spain and Romania will be studied.

[5] On interception of communications, Articles 100-3 and 706-95 of the Code de procédure pénale: the measure will not only be implemented by state agents but will also rely on private entities. Similar text is included for the access to stored data, Article 706-95-3¶2, relying on the knowledge of a digital actor that can access the data. On the contrary, do not rely on cooperation with non-state actors: geotagging, Article 230-36, the IMSI-catcher, sound and image recording and legal hacking, Article 706-95-17, or the use of drones, Article 230-51. It is not very clear for hacking, since Article 706-102-1 provides for the possibility to rely on experts (Article 157), which could be private entities.

not mention sanctions for a lack of cooperation.[6] On the contrary, the frameworks in both Spain and Romania include a general provision on cooperation with the business sector to implement digital investigative techniques.[7] The Spanish framework includes a general cooperation obligation article[8] and specific mentions of certain techniques,[9] and refusal to cooperate constitutes disobedience.[10] Similarly, in Romania, all "*providers of public electronic communications networks or providers of electronic communications services […] shall be obliged to cooperate*."[11] Therefore, digital actors are obliged to cooperate in the implementation of digital investigative techniques, even though, these techniques remain unstable and are not always effective in combatting cyber trafficking.[12] The states will then develop direct data requests to digital actors.

278. Request for data: France. Second, states provide for norms to request data from non-state entities, which can apply to digital actors. In France, requests for data can be made at any stage of the investigation. The prosecutor, the judge of instruction, and police officers can require any entity that is "*likely to hold information relevant to the investigation, including […] information from a computer system or processing of nominative data*."[13] First, the *Cour de Cassation* considered that these requests do not hinder the right to privacy, so they can be produced by non-judicial authorities.[14]

---

[6] Nor does the Décret n°93-119 relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646. Article R642-1 of the Code pénal provides a fine of up to 150 euros for failure to comply with a request order (Article 131-13.2°).

[7] Including regarding the confidentiality of such cooperation, Article 588 ter e.2 of the Ley de Enjuiciamiento Criminal and Article 142.3 of the Codul de Procedură Penală

[8] Directed to any "*providers of telecommunications services, of access to a telecommunications network, or of information society services, as well as any person who in any way contributes to facilitating communications by telephone or any other means or system of telematic, logical, or virtual communication*," Article 588 ter e.1 of the Ley de Enjuiciamiento Criminal

[9] In particular, for the identification of an IP address, Article 588 ter k of the Ley de Enjuiciamiento Criminal. Even if not explicitly mentioned, Spanish law enforcement authorities can also rely on "*providers of telecommunications services, access to a telecommunications network, or information society services*" to obtain data regarding "*the ownership of a telephone number or any other means of communication, or […] the telephone number or identification data of any means of communication*," Article 588 ter m. Similarly, for remote access to stored data, Article 588 septies b.1.

[10] Article 588 ter e.3 of the Ley de Enjuiciamiento Criminal, punishable by imprisonment for up to one year and a fine of up to 18 months, for a daily amount ranging from 30 to 5 000 euros for legal persons, in relation to Article 50.4.

[11] However, the law provides an interesting detail, underlining that they only must cooperate "*within the limits of their competences*," Article 142.2 of the Codul de Procedură Penală. No sanction for refusal to cooperate is mentioned, but Article 271 of the Codul Penal provides for one for those that prevent law enforcement authorities from carrying out procedural acts or that refuse to transmit information (up to one year of imprisonment and a fine).

[12] See *supra* Part 1. Title 2. Chapter 1. Section 1.

[13] Articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3 and 99-4 of the Code de Procédure Pénale

[14] Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81949. However, it questioned the kind of data that could be requested. The court upheld the request due to the lack of content data

Recently, this regime was deemed unconstitutional by the *Conseil Constitutionnel*[15] due to the broadness of data included and the lack of material and temporal scope. As a result, a specific article was created to request access to traffic or location data for specific offenses, (including trafficking.)[16]. A few months later, the integration of the CJEU case law[17] led the *Cour de Cassation* to declare that these articles on requests produced by the prosecutor were not invalid due to the absence of independent review.[18] Nonetheless, the last reform did not modify this element.[19]

279. Request for data: Spain. In Spain, the framework for requests for data is divided among three legal texts, challenging their readability. From the criminal procedure code, specific traffic data[20] can be requested to investigate serious offenses, including human trafficking,[21] upon authorization of the judge of instruction.[22] In addition, requests for any traffic data or location data are considered under the data

provided to law enforcement authorities, Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81945. See also Cour de Cassation, Chambre criminelle, November 6, 2013, no. 12-87130, in which request the content of emails has not been asked for. Maybe, content data could not be requested through that measure, being much less interesting for law enforcement authorities. Indeed, the very broad regulation of this measure has been criticized when not exercised by a judicial authority, considering the absence of limitations on the kind of data that can be asked for, B. Roussel, *Les investigations numériques en procédure pénale*, Thesis, Université de Bordeaux, July 7, 2020, pp. 131-132

[15] Conseil constitutionnel, *M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]*, December 3, 2021, 2021-952 QPC

[16] Article 60-1-2 of the Code de Procédure Pénale, as amended by the Loi n° 2022-299 visant à combattre le harcèlement scolaire

[17] CJEU, *G.D. v. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, April 5, 2022, C-140/20; B. Nicaud, "Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE," *Dalloz actualité*, Dalloz, September 5, 2022. Again, this reform emphasizes a quick reaction to European and national case law without a comprehensive examination of the request regime, J. Bossan, "Les réquisitions judiciaires relatives aux données de connexion : suite... et fin ? Commentaire des dispositions issues de la loi du 2 mars 2022 visant à combattre le harcèlement scolaire," *Droit pénal*, LexisNexis, August 2022, no. 7-8, pp. 9-14; A. Gogorza, "L'accès aux données de connexion : les affres du pluralisme normatif," *Droit pénal*, LexisNexis, October 2022, no. 10, p. 20

[18] Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-83820; Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-84096; Cour de Cassation, Chambre criminelle, July 12, 2022, no. 20-86652; Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-83710. The topic was already criticized in the literature after the decision of the Conseil Constitutionnel, A. Botton, "Droit au respect de la vie privée dans un cadre d'enquête : la stratégie d'évitement du Conseil constitutionnel," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 415

[19] Version of the articles after the Loi n° 2023-22 d'orientation et de programmation du ministère de l'intérieur

[20] Those are "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*," Article 2.b of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. That corresponds mostly to the mandatory conservation data listed in Article 3.1 of the Ley 25/2007 de conservación de datos.

[21] Article 588 ter a of the Ley de Enjuiciamiento Criminal in relation to Article 579.1

[22] Article 588 ter j of the Ley de Enjuiciamiento Criminal. There is no specific sanction for refusing to comply with the request, but a reference to the disobedience offense.

retention law; [23] this also requires a judicial authorization.[24] The material scope is slightly different: Those requests are limited to the investigation of "*delitos graves*,"[25] meaning offenses punishable by more than five years of imprisonment,[26] which includes human trafficking. The requested entity must reply within seven days.[27] Finally, the request for subscriber data[28] is deemed not to infringe on the right to privacy,[29] and, thus, does not require a judicial authorization. These requests rest on the general cooperation obligation of the personal data protection framework in the criminal sector.[30]

280. Request for data: Romania. In Romania, cooperation with the business sector also depends on the type of data.[31] Traffic and localization data can be requested upon authorization by the judge of rights and freedoms,[32] for a limited list of offenses, which includes human trafficking.[33] Furthermore, the police can order any person "*on the territory of Romania to communicate certain computer data in its possession or under its control and that is stored in a computer system or on a*

[23] Article 3.1.f of the Ley 25/2007 de conservación de datos. On the contrary, it is made explicit that content data should not be conserved and therefore cannot be requested, Article 3.2. M

[24] Article 6.1 of the Ley 25/2007 de conservación de datos

[25] Article 1.1 of the Ley 25/2007 de conservación de datos

[26] Articles 13.1 and 33.2 of the Código penal. However, the case law hesitated between interpreting Article 1.1 of the Ley 25/2007 de conservación de datos on the basis of the criteria of the Código penal, or on a case-by-case basis depending on the circumstances, finally choosing the former solution, A. Álvarez Tejero, "La solicitud de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación en el marco de la instrucción: reflexión sobre la Ley 25/2007," *Revista de Jurisprudencia El Derecho*, May 1, 2014, no. 2

[27] Article 7.3 of the Ley 25/2007 de conservación de datos. No provisions are included for late responses or refusing to comply, see Article 10 of the Ley 25/2007 de conservación de datos.

[28] Meaning "*any data […] pertaining to: the identity of a subscriber or customer, such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or email address*," Article 3.9.a of the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

[29] SIRIUS, "EU Digital Evidence Situation 2nd Annual Report," EU, 2020, p. 17

[30] Article 7 of the Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Refusal to comply is a very serious offense, Article 58.j, punished by a fine of 360.001 to 1.000.000 euros, Article 62.2.a; and failure to cooperate diligently to is a serious offense, Article 59.j, punished by a fine of 60.001 to 360.000 euros, Article 62.2.b.

[31] Article 146^1 of the Codul de Procedură Penală requires the authorization of a judge of rights and freedoms to request to a credit institution or other financial institution the monitoring of a person's financial transactions for a certain period of time; for the mere financial situation of a person, meaning the transmission of pre-existing data, the request for a prosecutor is sufficient, Article 153.

[32] Article 152.1 of the Codul de Procedură Penală. Moreover, the code underlines that this measure should be proportionate, in particular considering "*the importance of the information or evidence to be obtained or the gravity of the crime*," Article 152.1.d; and that is subsidiary, being implemented only when "*evidence could not be obtained in any other way*," Article 152.1.c. Therefore, the level of motivation is quite high. Article 138.1.j expressly prohibits requesting content data.

[33] Article 152.1.a of the Codul de Procedură Penală

computer data storage medium."[34] Since computer data is broadly defined,[35] it could include content data, although no judicial authorization is needed. However, a restrictive interpretation is preferred, since the same article provides that only subscriber data can be requested without judicial authorization.[36,37]

281. The implementation of the state's digital investigative measures to gather evidence against cyber trafficking already needs cooperation with private entities. This collaboration is enhanced by allowing requests for data to digital actors. In that sense, these requests can be seen as "*tools of the criminal police*,"[38] or the "*long arm of the law enforcement community*."[39] However, the frameworks for requests are still legally limited and unstable, and other limitations should be considered.

B. Limitations to national classical frameworks

282. Territoriality. Major digital actors[40] are based in multiple countries, and national actors can move their servers abroad, particularly through a subsidiary company. National frameworks do not mention the location or nationality of digital actors to delimit the personal scope of data requests. However, the principle of territoriality still delimits the investigation. The French *Cour de Cassation* made this clear in 2013 regarding a data request to Google: In general, law enforcement authorities do not have jurisdiction to request data outside French borders. However, when asking for data without coercive means, the answer for digital actors is voluntary; thus, the request is valid. Therefore, cooperation relies on voluntary data disclosure,[41]

---

[34] Article 170.2.a of the Codul de Procedură Penală
[35] Defined as "*any representation of facts, information or concepts in a form appropriated for processing in a computer system*," Article 138.5 of the Codul de Procedură Penală
[36] Article 170.2.b of the Codul de Procedură Penală
[37] No sanction for refusal to comply is provided in both cases, but the offense of obstruction of justice could sanction those that prevent law enforcement authorities from carrying out procedural acts or that refuse to transmit information (up to one year of imprisonment and a fine), Article 271 of the Codul Penal
[38] F.-J. Pansier, "Présentation de la loi : de la LSQ à la LSI," *Gazette du Palais*, Lextenso, March 27, 2003, no. 86, p. 2
[39] J. Vervaele, "Mesures de procédure spéciales et respect des droits de l'homme Rapport général," *Utrecht Law Review*, October 2009, vol. 5, no. 2, p. 120
[40] In particular, the GAMMA (Google, Amazon, Microsoft, Meta, and Apple). Most of the requests for data are sent to Google, Facebook and Microsoft, SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 14
[41] Cour de Cassation, Chambre criminelle, November 6, 2013, *op. cit.* note 14. However, if the data obtained should have been authorized by a judicial authority, it may not be admissible in court, since the Spanish and Romanian legislations are more detailed. See also O. Violeau, "Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques," *Actualité juridique Pénal*, Dalloz, 2017, p. 324

mostly limited to non-content data.[42]

283. A cooperation defined by digital actors. Obtaining data depends on the will of digital actors.[43] Law enforcement authorities criticize the lack of transparency in the conditions to obtain a response,[44] the level of priority given to each request,[45] and the delay in obtaining an answer[46]. Additionally, it has not been proved that digital actors check basic information, such as the competence of the sending authority, the validity of the measure, or the investigation or consider the confidentiality of the measure.[47] Thus, it is difficult to monitor the voluntary cooperation between states and digital actors.[48] Moreover, in the absence of formal partnerships, the process for the

[42] S. Tosza, "Cross-border gathering of electronic evidence: mutual legal assistance, its shortcomings and remedies," *in* V. Franssen, D. Flore, F. Stasiak (eds.), ***Société numérique et droit pénal : Belgique, France, Europe***, Bruylant, 2019, p. 274, see 18 US Code (USC) § 2702 - Voluntary disclosure of customer communications or records. Furthermore, most digital actors rely on the right to privacy to limit their cooperation, which is ironic given that the United States lacks any regulations to protect personal data. It is nowadays a "*marketing argument*," J. Charpenet, "Plateformes digitales et Etats : la corégulation par les données. Le cas des requêtes gouvernementales," *Revue internationale de droit économique*, 2019, vol. 2019/2, no. XXXIII, p. 375. This limit does not seem relevant, since "*90% of all the requests […] refer to subscriber information*," SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 13. However, it may be because law enforcement authorities do not request content data because they know they will not have an answer. Indeed, in 2017, the Council of Europe found that Facebook was only transmitting subscriber data and some traffic data; Google only user data; Microsoft only basic subscriber data and transactional data, Cybercrime Programme Office of the Council of Europe, Cybercrime@EAP III Project, "Study on Strategy of Cooperation with Multinational Service Providers," Council of Europe, August 30, 2017, pp. 22-25, 2016/DGI/JP/3608. Moreover, when asking legal practitioners, in particular prosecutors working against human trafficking, most of them abandoned the possibility of sending a request to digital actors, predicting that they would not receive an answer.

[43] European Commission, "Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters," EU, February 5, 2019, p. 2, COM(2019) 70 final

[44] Council of the EU, "Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace," EU, December 2, 2016, p. 7

[45] Cybercrime Programme Office of the Council of Europe, "Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines Revised study and guidelines," Council of Europe, 2020, p. 23

[46] Cybercrime Convention Committee, "Transborder access to data and jurisdiction: Options for further action by the T-CY," Conseil de l'Europe, December 3, 2014, p. 12, T-CY (2014)16; Europol, Eurojust, "Common challenges in combating cybercrime," EU, June 2019, p. 15

[47] R. Gauvain et al., ***Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale***, Rapport au Premier Ministre, France, June 26, 2019, p. 33. However, the digital actors process those demands through their legal departments, but a lack of transparency prevents states from monitoring how they assess them, Cybercrime Programme Office of the Council of Europe, Cybercrime@EAP III Project, *Study on Strategy of Cooperation with Multinational Service Providers*, *op. cit.* note 42, pp. 11-12. The last topic on confidentiality has been highlighted since some actors "*notif[ied] accountholders of government inquiries*," Cybercrime Convention Committee, *Transborder access to data and jurisdiction*, *op. cit.* note 46, p. 12

[48] European Commission, "Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the

cooperation is regulated by digital actors,[49] some of whom offer a global standardized form or a platform to transmit requests.[50] Nevertheless, standardized procedures are limited due to the multiplicity of digital actors. Thus, law enforcement authorities still highlight the "*difficulty in identifying how and where to send requests to companies*."[51] However, the regulation of cooperation by digital actors does not solve all challenges: They underline that they frequently receive requests sent to the wrong entity, as well as appeals for non-existent data, or a wrong account identifier. If law enforcement authorities lack knowledge regarding the functioning of digital actors, the opposite is also true, since digital actors continue to struggle to authenticate the sending authority or the legal basis of the request.[52] Due to the absence of a common legal framework, digital actors must adapt to all sovereign national norms, resulting in higher costs[53] and possible contradictory obligations.[54]

284. Even if the volume of requests is increasing[55] and the quality of cooperation seems to be improving,[56] cooperation still depends on the offense investigated[57] and on the relationships built during the process of trying to obtaining data.[58] This leads to significant differences in the responses obtained by states based on digital actors. It is also problematic, since the response depends on "*their view of a country rather than a*

---

appointment of legal representatives for the purpose of gathering evidence in criminal proceedings," EU, April 17, 2018, p. 9, SWD(2018) 118 final

[49] Economic Crime Division, Directorate General of Human Rights and Legal Affairs, "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime," Council of Europe, April 2, 2008, ¶¶ 13-14

[50] J. Charpenet, "Plateformes digitales et Etats," *op. cit.* note 42, p. 368. However, it could be underlined that such initiative from digital actors is positive, since prior requests did not have any common form, resulting in further delays, or the use of "*no secure channel of communication*," Council of the EU, *Progress Report on Improving Criminal Justice in Cyberspace*, *op. cit.* note 44, p. 7

[51] SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 21

[52] *Ibid.* pp. 49-50

[53] European Commission, *Working document impact assessment accompanying the e-evidence proposals*, *op. cit.* note 48, p. 122. Those costs may be prohibitive for smaller digital actors, which may result in the absence of cooperation, European Commission, Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, April 17, 2018, p. 2, COM(2018) 226 final

[54] S. Tosza, "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, June 1, 2020, vol. 11, no. 2, p. 169

[55] SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 6

[56] Cybercrime Convention Committee, "The Budapest Convention on Cybercrime: benefits and impact in practice," Council of Europe, July 13, 2020, pp. 23-24, T-CY (2020)16

[57] Cooperation for crimes such as terrorism and child online sexual exploitation is now quite easy.

[58] Expert Group to Conduct a Comprehensive Study on Cybercrime, "Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector Executive summary," UNODC, UN, January 23, 2013, ¶ 21, UNODC/CCPCJ/EG.4/2013/2

legal basis."[59] To summarize, this cooperation process, "*lacks reliability, transparency, accountability, and legal certainty*."[60] The problem has been highlighted particularly for investigations of human trafficking;[61] as a result, to cooperate with foreign digital actors, the most reliable tool is mutual international assistance.[62]

II. Ineffective international cooperation to obtain data from digital actors

285. Various frameworks support cooperation with digital actors through the assistance of other states. Due to the limits of diplomatic cooperation,[63] various multilateral agreements have been developed and could be used to request evidence to investigate trafficking, as they are applicable to criminal matters in general.[64] The 1959 Convention of the Council of Europe on Mutual Assistance in Criminal Matters[65] is an international reference on mutual legal assistance. This text has been

[59] Cybercrime Programme Office of the Council of Europe, *Cooperation between law enforcement and Internet service providers against cybercrime*, *op. cit.* note 45, p. 23. Google, for example, never responded to any Hungarian requests while responding to Finland for 83% of requests. Similarly, Apple discloses data to France in only 29% of requests, compared to 90% of Austrian requests, Council of the EU, *Progress Report on Improving Criminal Justice in Cyberspace*, *op. cit.* note 44, p. 10

[60] European Commission, "Security Union facilitating Access to Electronic Evidence," EU, April 2018, p. 1. Mariez argues that the absence of legal certainty is the main obstacle, J.-S. Mariez, "Une nouvelle étape vers un accès transfrontalier aux preuves numériques : l'initiative européenne « e-evidence » ou la recherche d'un équilibre entre efficacité des enquêtes pénales, droit des personnes concernées et sécurité juridique pour les fournisseurs de services internet," *Revue Lamy Droit de l'immatériel*, March 1, 2018, no. 146, p. 2. The need for legal certainty is highlighted by both law enforcement authorities and digital actors, L. Siry, "Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, September 1, 2019, vol. 10, no. 3, p. 247

[61] GRETA, "Online and technology-facilitated trafficking in human beings. Full report," Council of Europe, March 2022, p. 57; Groupe de travail sur la prostitution des mineurs, *Rapport sur la prostitution des mineurs*, France, June 28, 2021, p. 165. This topic was included in the action plan against minor prostitution in France. Indeed, Action 13 calls for administrative sanctions to be imposed on European accommodation websites such as Airbnb for failing to respond to requisitions. The plan is not ambitious, since it is limited to such kinds of digital actors, but it may be a first step towards better national cooperation to repress cyber trafficking, Gouvernement, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, France, November 15, 2021, p. 9

[62] Economic Crime Division, Directorate General of Human Rights and Legal Affairs, *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*, *op. cit.* note 49, ¶ 36

[63] R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, Thesis, Université de Lorraine, 2016, pp. 358-360

[64] For the global framework of mutual legal assistance for organized crime, see *supra* 248 and 249. However, as mentioned in this part, the Palermo Convention is limited to international cooperation when human trafficking is transnational and committed within an organized criminal group, which does not permit extending the framework to all kinds of trafficking.

[65] As complemented by the 1978 Additional Protocol and the 2001 Second Additional Protocol. For a consolidated version, see M. Kubíček, Committee of experts on the operation of European conventions on co-operation in criminal matters, European committee on crime problems, "Consolidated document reflecting the applicable provisions of the European Convention on Mutual Assistance in Criminal Matters and its two Additional Protocols," Council of Europe, November 4, 2011, PC-OC (2011) 15 Rev. The 1959 Convention cited is the consolidated version including both protocols.

supplemented by the 2000 EU Convention on Mutual Assistance in Criminal Matters.[66] Additionally, the EU provides for the specific European Investigation Order. Lastly, the EU can rely on the 2003 agreement on mutual legal assistance between the EU and the United States.[67] However, all of these agreements face multiple limitations, regarding their geographical scope (A), material scope (B), and procedural provisions (C).

A. A mostly European mutual legal assistance framework

286. European cooperation. Cooperation with digital actors through another EU member state differs from cooperation through a third-party state. The former is more developed, but the latter is particularly relevant since many digital actors, whose data are useful to obtain evidence against trafficking, are headquartered in the United States. Nonetheless, the majority of them have a European headquarters, subsidiaries, or representations.[68] In the EU, various frameworks exist due to the historical step-by-step integration and the current opt-in systems for several countries.[69]. Its last framework, the European Investigation Order, is based on the principle of mutual recognition:[70] "*Decisions of criminal courts and other competent authorities of one Member State are to be accepted by the courts and competent authorities of the other Member States and enforced on the same terms as their own*."[71] For some, this "*reflects shared sovereignty*."[72] This principle supports the application of national procedures beyond their borders,[73] thanks to a certain level of harmonization[74] and

[66] Article 1.1.a and b of the 2000 Convention established by the Council in accordance with Article 34 of the Treaty on EU, on Mutual Assistance in Criminal Matters between the Member States of the EU. It is a good example of the complementarity between the Council of Europe and the EU.
[67] Agreement on mutual legal assistance between the EU and the United States of America, July 19, 2003
[68] In particular, in Ireland. For example, Facebook, Microsoft, Google, Airbnb, etc.
[69] A. Weyembergh, "Enhanced cooperation in criminal matters: past, present and future," *in* R. Kert, A. Lehner (eds.), *Vielfalt des Strafrechts im internationalen Kontext. Festschrift für Frank Höpfel zum 65. Geburtstag*, NWV Verlag, 1st ed., January 19, 2018, pp. 605-624
[70] See Article 82.1 of the Treaty on the Functioning of the EU and Article 1.2 of the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters
[71] J.R. Spencer, "The Principle of Mutual Recognition," *in* R.E. Kostoris (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, p. 281
[72] S. Braum, "'Rechtsstaat' and European criminal law – From the end of sovereignty," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 1, 2021, vol. 12, no. 1, p. 16. Or, at least, an "*improved government-to-government cooperation*," J. Daskal, "Borders and Bits," *Vanderbilt Law Review*, 2018, no. 71, p. 202
[73] M.-E. Morin, *Le système pénal de l'Union européenne*, Thesis, Université d'Aix-Marseille, November 28, 2017, ¶ 454
[74] J.R. Spencer, "The Principle of Mutual Recognition," *op. cit.* note 71, p. 290

mutual trust.[75] As the Tampere European Council conclusions underlined, mutual recognition is the "*cornerstone of [EU] judicial cooperation*."[76] In particular, it "*offers the advantage of favoring fast evidence gathering*."[77] However, the efficiency of the European Investigation Order can be criticized,[78] especially as a result of the system of opt-in. Indeed, the directive is not applicable to Denmark and Ireland.[79] To enhance cooperation with the latter, law enforcement authorities rely on the 2000 EU convention,[80] but it has been ratified by only half of the member states.[81] Fortunately, the 1959 Council of Europe Convention has been ratified by all EU member states, including Ireland. As a result, the Council of Europe framework appears to be the best tool for securing transnational data requests regarding the repression of human trafficking.[82] Additionally, it is open to ratification by non-European countries; indeed, the convention has been ratified by a few of them, but not by the United States.

287. US–EU cooperation. The 2003 EU–US Agreement on mutual legal assistance might be seen as the solution to developing cooperation between the United States and Europe. It is a new type of bilateral treaty, negotiated by the EU and mandatory for ratification by all member states, but still relying on a bilateral decision between

[75] Such trust results in the four freedoms nowadays recognized by the treaties (namely, the freedom of circulation of capital, Article 63 of the Treaty on the Functioning of the EU, of goods, Article 28, of services, Article 56, and of people, Article 20), initially promoted by the ECJ, *Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein*, February 20, 1979, C-120/78. Additionally, a fifth freedom could be named after the principle of "*free movement of judgments*," J.R. Spencer, "The Principle of Mutual Recognition," *op. cit.* note 71, p. 286, today extends to various kinds of justice decisions.

[76] Tampere European Council, "Tampere European Council of 15 and 16.10.1999 - Conclusions of the Presidency," EU, October 1999. See also B. Lavaud-Legendre, "La coopération répressive en matière de traite des êtres humains - Du droit à sa mise en oeuvre," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 7. For a full history of European cooperation, see A. Weyembergh, "History of the Cooperation," *in* R.E. Kostoris (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, pp. 173-199

[77] M. Daniele, E. Calvanese, "Evidence Gathering," *in* R.E. Kostoris (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, p. 358

[78] S. Carrera, M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, CEPS Paper in Liberty and Security in Europe, no. 2020-01, Centre for European Policy Studies, February 2020, p. 7. On the limits of mutual recognition in general, see A. Weyembergh, "Two crucial challenges in cross-border criminal investigations," *in* S. Carrera, V. Mitsilegas, J. King (eds.), *Constitutionalising the Security Union: effectiveness, rule of law and rights in countering terrorism and crime*, Centre for European Policy Studies (CEPS), 2017, p. 21

[79] Paragraphs 44 and 45 of the preamble of the Directive 2014/41/EU

[80] Sixteen states are parties to the 1978 Additional Protocol, while the 2001 Second Additional Protocol has been widely ratified by all the EU member states except Greece. Ireland ratified both.

[81] While the 2001 Second Additional Protocol of the 1959 Council of Europe Convention comprises all the EU member states except Greece. As a result, those who did not ratify the 2000 Convention but want to work with Ireland will have to rely on the updated 1959 Council of Europe Convention.

[82] P. Bellet, "La coopération judiciaire en matière de traite des êtres humains," *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 45

each member state and the United States.[83] However, it is still a subsidiary text, applicable in the absence of or to complement a main bilateral treaty between a member state and the United States.[84] Moreover, the instrument does not preclude the conclusion of later bilateral treaties on the same topic as long as they are not in contradiction.[85] Therefore, it does not create a harmonized framework for mutual legal assistance with the United States and its digital actors.

288. Due to variable geographical scopes, no unified framework exists to secure digital evidence through cooperation with Ireland or the United States. Additionally, the material provisions of the texts further limit their applicability.

B. Material scope, human trafficking, and digital evidence

289. Inappropriate scope of the EU–US agreement. Although the 2003 EU–US agreement appears to apply to any offense and to any type of request, its content is quite limited. Indeed, it "*does not contain a legal basis for requesting digital evidence*."[86] In general, the provisions of the 2003 agreement are scarce:[87] Bilateral agreements might be more interesting and developed. However, these agreements are typically old[88] and unsuitable for the current needs to collaborate with digital actors to fight human trafficking. Therefore, the European Commission called for a new agreement dedicated to cross-border access to electronic evidence for judicial

[83] Article 3.2 of the 2003 agreement
[84] Article 3.1 and 3 of the 2003 agreement
[85] Article 14 of the 2003 agreement
[86] S. Tosza, "Cross-border gathering of electronic evidence," *op. cit.* note 42, p. 271. It only provides for the obtaining of bank information and testimony by videoconferencing, Articles 4 and 6 of the 2003 agreement. For bank information, which can be digital data in a broad sense, the application of the provision can be limited to specific offenses, Article 4.4. The example of the agreement with France shows that human trafficking is not included, Article I.B.3.a: the United States limits their assistance to money laundering, and terrorism, and certain notified criminal offenses, Instrument relatif à l'application du traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les États-Unis d'Amérique, Décret n° 2010-489 du 12 mai 2010 portant publication de l'instrument relatif à l'application du traité d'entraide judiciaire en matière pénale signé le 10 décembre 1998 entre la France et les Etats-Unis d'Amérique, signé à La Haye le 30 septembre 2004. Similarly, with Romania, see the 2007 Protocol to the 1999 Treaty Between the United States and Romania, Article 6.4; with Spain, see the 2004 Instrumento contemplado por el art 3(2) del Acuerdo de asistencia judicial entre los Estados Unidos de América y la Unión Europea, sobre la aplicación del Tratado de asistencia jurídica mutua en materia penal entre USA y el Reino de España, Article 16 bis.4
[87] The grounds of refusal mainly refer to bilateral treaties between member states and the United States, Article 13 of the 2003 agreement; and the procedure is not detailed. The latter could still be complemented by the 2016 EU-US Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses, but it is still limited to data protection, and does not mention the possibility of requiring data to digital actors.
[88] The bilateral treaty on mutual legal assistance between Romania and the United States was signed in 1999; the one with France, in 1998; and the one with Spain, in 1990.

cooperation in criminal matters,[89] and negotiations started in 2019.[90]

290. European mutual assistance. The 1959 and 2000 conventions[91] and the European Investigation Order directive[92] are comprehensive texts applicable to any offense, including human trafficking. Additionally, the forms of assistance are broader. The 1959 convention calls for "*the widest measure of mutual assistance*" [93] and includes specific provisions for handing over any property, records, or documents[94] that could be used to request data from digital actors.[95] The European Investigation Order covers "*any investigative measure*,"[96] thereby including requests for data from digital actors, although this provision is not explicit.[97] Nonetheless, the texts are still based on the principle of territoriality and require that a request be sent to the state in which the evidence is located, which can be difficult to determine for digital evidence.[98] Furthermore, the European texts consider grounds for refusal. In the 1959 convention, they include, for instance, the refusal due to a "*prejudice [to] the sovereignty, security, public order, or other essential interests of its country*,"[99] but the principle of dual criminality is not included.[100] Additionally, for the European Investigation Order, mutual

[89] European Commission, *Recommendation for a Council Decision authorising the opening of negotiations*, *op. cit.* note 43

[90] T. Christakis, F. Terpan, "EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options," *International Data Privacy Law*, 2021, p. 1

[91] Article 1.1 of the 1959 Convention

[92] Article 4.a of the Directive 2014/41/EU, including when prosecuting a legal person, Article 4.d; as well as other kinds of proceedings, Article 4.b and c

[93] Article 1.1 of the 1959 Convention

[94] Article 5 of the 1959 Convention. The main input of the 2000 Convention is to create a legal framework for certain forms of mutual assistance, in particular regarding interceptions of communications, Articles 17 to 22, R. Boos, *La lutte contre la cybercriminalité*, *op. cit.* note 63, p. 234. But the convention does not take into account the current limitations of this technic.

[95] O. Fuentes Soriano, "Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes. Las órdenes europeas de entrega y conservación de pruebas electrónicas," *in* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, p. 286. The convention also provides specificities for search and seizure of property but does not extend them to records and documents, Article 6 of the 1959 Convention

[96] Article 3 of the directive 2014/41/EU. The directive explicitly mentions the obligation for states to provide "*the identification of persons holding a subscription of a specified phone number or IP address*," Article 10.

[97] The directive "*was not designed with gathering of digital evidence in mind*." The author considers then that this tool is not adapted to obtain data from digital actors, in particular due to the absence of consideration of the volatility of data, S. Tosza, "Cross-border gathering of electronic evidence," *op. cit.* note 42, p. 277

[98] M. Giacometti, "Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ?," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 316. See also, S. Tosza, "All evidence is equal," *op. cit.* note 54, p. 169

[99] Article 2.b of the 1959 Convention; the assistance is also excluded regarding a political offense, Article 2.a, or a tax offense, unless the states are parties to the 1978 Additional Protocol, see Article 1

[100] Article 3.1 of the 1959 Convention, see Council of Europe, "Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters," Council of Europe, April 20, 1959, p. 6

recognition is mitigated "*with a series of limitations aimed at preserving the most relevant evidentiary rules of the State*."[101] The order should not violate fundamental rights,[102] and other grounds for refusal are the existence of an immunity or privilege regarding criminal liability,[103] harm to essential national security interests,[104] or the principle of *ne bis in idem.*[105] Some of the refusal grounds will not be applicable to the prosecution of human trafficking. Indeed, the absence of dual criminality cannot be argued against.[106]

291. Even when a text has appropriate geographical and wide enough material scopes, the provisions regarding the procedure are not suitable for requesting digital evidence.

C. Lengthy procedures

292. The 1959 and 2000 procedures. The 1959 convention provides that, in principle, the letters of request are to be addressed through the central authorities of the ministries of justice of the states, which lengthens the procedure. Direct communication between judicial authorities is only optional.[107] On the contrary, the 2000 convention provides for the general principle of direct communication between judicial authorities[108] to quicken the transmission of letters rogatory to request data

[101] M. Daniele, E. Calvanese, "Evidence Gathering," *op. cit.* note 77, p. 358
[102] Article 11.1 in relation with Article 1.4, and Article 11.1.f of the Directive 2014/41/EU
[103] Article 11.1.a of the Directive 2014/41/EU
[104] Article 11.1.b of the Directive 2014/41/EU
[105] Article 11.1.d of the Directive 2014/41/EU
[106] Article 11.1.g and Annex D of the Directive 2014/41/EU, when the offense is punishable by maximum imprisonment of at least three years, as is the case in France, Spain, and Romania. Due to the prior harmonization of the criminal law regarding the listed offenses, Morin considers that such exceptions to dual criminality are not major improvements, M.-E. Morin, *Le système pénal de l'Union européenne*, *op. cit.* note 73, ¶ 472. However, the harmonization also permits avoiding the ground of refusal due to extraterritorial prosecution and the absence of dual criminality in Article 11.1.e of the Directive 2014/41/EU, even if Annex D is not mentioned.
[107] Article 15.1 of the 1959 Convention. For example, Spain only accepts direct transmission in cases of emergency (declaration of March 26 2018 to the 2001 Second Additional Protocol), and Romania similarly (declaration of March 17 1999 to the 1959 Convention). There is an additional possibility for the states to request the sending of a copy to the central authority, Article 15.8. For example, even in cases of emergency, Spain requires a copy to be sent to the central authority (declaration of March 26 2018 to the 2001 Second Additional Protocol). Similarly, see France (declaration of May 23 1967 to the 1959 Convention) and Romania (declaration of March 17 1999 to the 1959 Convention)
[108] Article 6.1 of the 2000 Convention. Ireland has the possibility of requiring the procedure to go through its central authority, Article 6.3, but no declaration seems to have been made. Regarding the 2003 EU-US agreement, it only provides for communication of requests through central authorities, which is particularly problematic considering the volume of requests for data to American digital actors, Cybercrime Programme Office of the Council of Europe, Cybercrime@EAP III Project, *Study on Strategy of Cooperation with Multinational Service Providers*, *op. cit.* note 42, p. 6

from digital actors. The 1959 convention considers the possibility of transmitting the data "*through any electronic or other means of telecommunication*,"[109] to quicken the procedure.[110] Finally, the texts do not establish delays, although they are needed to ensure that the execution and transmission of data are efficient.[111]

293. The European Investigation Order procedure. The Directive 2014/41 is particularly innovative in terms of the European Investigation Order procedure. It does not rely on a certification procedure to be executed by the receiving state, nor does it require the evidence to be admissible in the issuing state.[112] The procedure uses common forms[113] that are transmitted directly to the executing authority.[114] In practice, a French prosecutor could directly send a request to a Spain prosecutor or judge to request data from a Spanish digital actor. However, the Directive "*gave up a full realization of the principle of mutual recognition [by introducing] the possibility to provide governmental controls [since] each State can designate a central authority to assist the competent judicial authority*."[115] Although this possibility is not introduced in each state,[116] the central authority still has an important role due to the lack of

[109] Article 15.9 of the 1959 Convention. The opportunity to use those new technologies for transmitting requests and answers for mutual legal assistance has been underlined by UNODC, *Report Informal Expert Working Group on Mutual Legal Assistance Casework Best Practice*, UN, 2001, p. 13. For example, France agrees to receive requests in any form as long as it is possible to check their authenticity (declaration of February 06 2012 to the 2001 Second Additional Protocol). Similarly, in the 2003 EU-US agreement, see Article 7.

[110] Moreover, the procedure can be accelerated by the general principle of absence of needed translation, Article 16.1 of the 1959 Convention; and authentication of transmitted data, Article 17. However, according to Article 16.2 of the 1959 Convention, states may reserve otherwise for the former. See Spain, reserving the right to require a Spanish translation and authentication (declaration of August 18 1982 to the 1959 Convention); and Romania, requiring a translation in one of the languages of the Council of Europe, which is still easier to comply with than just one language (declaration of March 17 1999 to the 1959 Convention)

[111] At least, the 2000 Convention develops a framework to inform and communicate on deadline matters, Article 4. Delays are not considered in the 2003 EU-US agreement, S. Tosza, "Cross-border gathering of electronic evidence," *op. cit.* note 42, p. 272. The actual framework of mutual legal assistance with the United States takes, on average, ten months to reply to the requests, European Commission, "Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence," EU, February 5, 2019, p. 2

[112] M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US*, CEPS Paper in Liberty and Security in Europe, no. 2018-07, Centre for European Policy Studies, November 30, 2018, p. 26

[113] In particular, for the order itself, Article 5 of the Directive 2014/41/EU and annex A

[114] Article 2.d of the Directive 2014/41/EU. Any further communication is also direct, Article 7

[115] M. Daniele, E. Calvanese, "Evidence Gathering," *op. cit.* note 77, pp. 364-365, see Article 7.3 of the directive 2014/41/EU

[116] For example, in France, the receiving authority is directly the competent prosecutor or judge of instruction, Article 694-30 of the Code de procédure pénale. In Spain, the process is in between, since the orders must be sent to the public prosecution office, which can execute some of the orders, or will have to transmit to a judge those it cannot execute due to an impact on fundamental rights, Article 187.2 of the Ley 23/2014 de reconocimiento mutuo de resoluciones penales en la Unión Europea. In Romania,

knowledge regarding the competent executing authorities;[117] consequently, the current procedures are not as timely as expected.[118] Additionally, the lack of translation can result in unnecessary delays[119], as can the various channels available for the transmission such as mail, telecommunication, and the European Judicial Network system[120]. However, a major improvement to the Directive is to limit these delays to recognize[121] and execute the orders.[122] They are, however, only "*relative constraints*,"[123] because the executing authority can notify the issuing authority of a different time-lapse for both steps with no time limit.[124] Thus, the length of the procedure is still a "*relevant challenge*,"[125] especially since it seems inappropriate "*to capture electronic evidence*,"[126] due to the "*risk that data disappears or is altered*."[127]

294. From the most basic to the most sophisticated mutual assistance tools, these techniques do not appear to be capable of providing timely and efficient cooperation with digital actors to obtain data as evidence to prosecute cyber human trafficking.[128] In general, the traditional frameworks of mutual assistance are not adapted to gather digital data.[129] Therefore, innovative solutions should be considered to improve the repression of cyber trafficking.

European Investigation Orders for human trafficking cases will be recognized and carried out by the DIICOT, Article 330.2 of the Legea nr. 302 privind cooperarea judiciară internațională în materie penală, with a possible referral to the judge of rights and freedoms as needed, Article 333.1. However, assistance can also be provided by the specialized office of the Public Ministry, Article 330.3 and 4.

[117] Eurojust, "Report on Eurojust's casework in the field of the European Investigation Order," EU, November 2020, p. 30

[118] Through the central authority, see, for example, Article 331.5 of the Legea nr. 302 privind cooperarea judiciară internațională în materie penală; or with the assistance of Eurojust, Article 7.5 of the Directive 2014/41/EU

[119] Eurojust, *Report on the European Investigation Order*, *op. cit.* note 117, pp. 13-14

[120] *Ibid.* p. 29

[121] In general, 30 days after reception, Article 12.3 of the Directive 2014/41/EU

[122] In general, 90 days after recognition, Article 12.4 of the Directive 2014/41/EU

[123] M.-E. Morin, *Le système pénal de l'Union européenne*, *op. cit.* note 73, ¶ 476

[124] Article 12.5 and 6 of the Directive 2014/41/EU. Morever, the non-conformity with those delays is not an obstacle to the procedure, as underlined for the European Arrest Warrant, CJEU, *Minister for Justice and Equality v. Francis Lanigan*, July 16, 2015, C-237/15 PPU, ¶ 42, position that could be transposed to the European Investigation Order, M.-E. Morin, *Le système pénal de l'Union européenne*, *op. cit.* note 73, ¶ 476

[125] SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 25

[126] Europol, Eurojust, *Common challenges in combating cybercrime*, *op. cit.* note 46, p. 15

[127] S. Tosza, "All evidence is equal," *op. cit.* note 54, p. 169

[128] R. Malpani, *Legal Aspects of Trafficking for Forced Labour Purposes in Europe*, International Labour Office, 2006, pp. 19-21; Eurojust, "Report on Trafficking in Human Beings Best practice and issues in judicial cooperation," EU, February 2021, pp. 10-12

[129] R. Boos, *La lutte contre la cybercriminalité*, *op. cit.* note 63, p. 307; Europol, Eurojust, *Common challenges in combating cybercrime*, *op. cit.* note 46, p. 15. Arguing for the contrary, see S.V. Maymir, "Anchoring the need to revise cross-border access to e-evidence," *Internet Policy Review*, Alexander Von Humboldt Inst Internet & Soc, 2020, vol. 9, no. 3

§2. Innovative tools to cooperate with digital actors

295. To request data from digital actors, a variety of instruments have been developed that specifically consider the needs of prosecuting cybercrimes. The 2001 Budapest Convention on cybercrime was negotiated within the Council of Europe but is open for ratification globally, including in the United States and all EU member states, with the exception of Ireland.[130] The convention is deemed to be quite efficient and has been used as a model for other treaties or national reforms.[131] Thus, this text is of particular interest to improve cooperation with digital actors to repress human trafficking (I). Additionally, some national case law innovates new criteria to improve cooperation with digital actors (II). Although they are not dedicated to investigating trafficking, these tools are applicable, and in both cases, they redefine the principle of territoriality to reassert states' sovereignty.[132]

I. International tool to repress cybercrime

296. The scope of the Budapest Convention. At first glance, the Budapest Convention might appear not to be applicable to human trafficking investigations. However, cybercrime can encompass various meanings,[133] as the convention does not define it. In any case, all offenses linked to cybercrime, "*undermine the sovereignty of the state*."[134] Boos generally defines cybercrime as "*any illegal action whose purpose is to commit criminal offenses on or through a computer system interconnected to a*

[130] Therefore, it will be more interesting to require cooperation with American digital actors directly from their headquarters in the United States and not from their subsidiary or representation in Europe (Dublin).
[131] A. Jomni, "Le Conseil de l'Europe face aux défis de la lutte contre la cybercriminalité," *Revue de la gendarmerie nationale*, December 2018, no. 263, p. 7. See, for example, the 2014 African Union Convention on Cyber Security and Personal Data Protection, Cybercrime Convention Committee, *The Budapest Convention on Cybercrime*, *op. cit.* note 56, p. 15
[132] Another innovative tool might have been the use of joint investigation teams (a specific temporary entity to deal with a specific criminal case: law enforcement authorities from the various participating states collaborate directly without the need for mutual assistance processes). Yet they still rely on the preexisting digital investigative techniques, which are limited. Moreover, a joint investigation team cannot be built each time an authority needs data from a specific digital actor, or most of the cyber trafficking cases would need one with the US. Joint investigation teams are considered at Article 20 of the 2001 Second Additional Protocol to the 1959 Council of Europe Convention; Article 13 of the 2000 EU Convention, or, when non-applicable, the Council Framework Decision 2002/465/JHA on joint investigation teams; Article 5 of the 2003 EU-US agreement.
[133] For example, there is no unified definition shared by the various international organizations working on the subject, like the UNODC and the EU, R. Boos, *La lutte contre la cybercriminalité*, *op. cit.* note 63, p. 26; or by the literature, Conseil d'Etat, "Etude - Internet et les réseaux numériques," République française, November 30, 1997, p. 116
[134] J. Adams, M. Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies*, September 29, 2016, vol. 4, no. 6, p. 263

telecommunications network."[135] Thus, cybercrime is divided into two categories: "*computer-assisted crimes*" and "*computer-focused crimes*."[136] The latter defines cybercrime in a restrictive sense; the network or the device is the object of the offense.[137] The former accepts a broader definition of cybercrime: The device or the network is a tool, a means to commit "common" offenses.[138] As a result, cyber trafficking, or human trafficking facilitated by new technologies, falls under this second definition of cybercrime. Nonetheless, the Budapest Convention distinguishes between attacks against the network or its components[139]; and illegal content online,[140] which includes "*ordinary crimes that are frequently committed through the use of a computer system*."[141] However, the procedural provisions of the Budapest Convention go beyond this list of offenses; they apply to any "*other criminal offenses committed by means of a computer system*,"[142] including cyber trafficking.[143]

297. National orders. Once applicable, the Budapest Convention supplements

---

[135] R. Boos, *La lutte contre la cybercriminalité*, *op. cit.* note 63, p. 28

[136] S. Furnell, *Cybercrime: vandalizing the information society*, Addison-Wesley, A Pearson Education book, 1st ed., 2002, p. 22, cited in K.-S. Choi, "Cyber-Routine Activities Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization," *in* K. Jaishankar (ed.), *Cyber criminology: exploring Internet crimes and criminal behavior*, CRC Press, 2011, p. 230. Such division is also used by the GREVIO when considering the digital dimension of violence against women, Group of Experts on Action against Violence against Women and Domestic Violence, "General Recommendation No. 1 on the digital dimension of violence against women," Council of Europe, October 20, 2021, ¶¶ 22-23. Nevertheless, this division can be seen as purely formal since, in practice, both categories tend to combine to assist the commission of each other, S. El Zein, "L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie," *in* M.-C. Piatti (ed.), *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, Presses universitaires de Lyon, 2001, p. 164. For a summary of possible categorizations, see M.N. Solari-Merlo, "Análisis de los delitos informáticos. Una propuesta de clasificación," *Revista Aranzadi de Derecho y Proceso Penal*, December 2020, vol. 60

[137] R. Boos, *La lutte contre la cybercriminalité*, *op. cit.* note 63, p. 28. It includes, for example, breaches of automated data processing systems, or, in a common language, hacking.

[138] Conseil d'Etat, *Etude - Internet et les réseaux numériques*, *op. cit.* note 133, p. 116. Actually, "*Most of the 'cybercrime' we have seen so far is nothing more than the migration of real-world crimes into cyberspace*," S.W. Brenner, "Cybercrime: re-thinking crime control strategies," *in* Y. Jewkes (ed.), *Crime online*, Willan, 2007, p. 13

[139] Including "*offenses against the confidentiality, integrity and availability of computer data and systems*," Chapter II, Section 1, Title 1, Articles 2 to 6 of the Budapest Convention; and "*computer-related offenses*" (forgery and fraud of computer data or systems), Chapter II, Section 1, Title 2, Articles 7 and 8.

[140] Chapter II, Section 1, Titles 3 and 4 of the Budapest Convention. Those are offenses related to child pornography, Article 9; and to infringements of copyright and related rights, Article 10

[141] Council of Europe, "Explanatory Report to the Council of Europe Convention on Cybercrime," Council of Europe, 2001, ¶ 79. See also P. Lloria García, "Algunas reflexiones sobre la perspectiva de género y el poder de castigar del Estado," *Estudios Penales y Criminológicos*, June 15, 2020, vol. 40, pp. 504-505

[142] Article 14.2.b of the Budapest Convention

[143] It should be highlighted that the following round of evaluation by the GRETA underlines this link between the Warsaw Convention and the Budapest Convention, GRETA, "Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties. Fourth evaluation round. Thematic focus: Addressing vulnerabilities to

existing treaties[144] to improve "*the collection of evidence in electronic form of a criminal offense*."[145] To obtain digital evidence in any type of investigation, including to repress human trafficking, the Budapest Convention highlights the "*need for cooperation between States and private industry*."[146] Indeed, the states must create national measures to request traffic,[147] subscribers,[148] and computer data.[149] The convention relies on the criteria of presence in a national territory to require computer data and the offering of services[150] in a national territory to require subscriber data.[151] In both cases, the data must be in the "*physical possession*" or the remote control of the person.[152] Therefore, the convention "*rejects a data location-driven approach*":[153] Even a "*domestic power*"[154] can apply to a foreign digital actor. However, the convention provides, "*no enforcement mechanism in the receiving State*."[155]

298. International cooperation. Consequently, the convention innovates solutions to improve mutual assistance to obtain digital evidence. First, to secure a posterior request for data, states can request the preservation of stored computer data[156] and

trafficking in human beings," Council of Europe, June 30, 2023, ¶ 39, GRETA(2023)11. See also Cybercrime Convention Committee, "T-CY Guidance Note #13 The scope of procedural powers and of international co-operation provisions of the Budapest Convention," Council of Europe, June 27, 2023, pp. 4-5, T-CY(2023)6

[144] Preamble ¶ 13 and Article 27.1 of the Budapest Convention

[145] Articles 14.2.c, 23 and 25.1 of the Budapest Convention

[146] Paragraph 7 of the preamble of the Budapest Convention. The convention also recalls the need for cooperation with digital actors even for national digital investigative techniques, Articles 20.1.b and 21.1.b of the Budapest Convention, regarding real-time collection of traffic data and interception of content data (limited to a range of serious offenses). However, the collection and recording are limited to the national territory of the state, which can be difficult to define for interception of Internet content.

[147] However, the convention only provides for the disclosure of traffic data "*to identify the service providers and the path through which the communication was transmitted*," Article 13.1.b of the Budapest Convention

[148] Subscriber data can be of particular interest to obtain the subscriber's identity, address, or financial information. However, digital actors are not compelled to verify this identity. Moreover, the explanatory report highlights the limits of this article when the transmission of data to use the service is not mandatory, for instance, with prepaid mobile phone cards, which are used in some human trafficking cases, Council of Europe, *Explanatory Report to the Convention on Cybercrime*, *op. cit.* note 141, ¶ 181

[149] The explanatory report underlines that requiring data to digital actors may be more flexible compared to "*measures that are more intrusive or more onerous*," *Ibid.* ¶ 171

[150] Meaning that "*the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services); and the service provider has established a real and substantial connection to a Party*," Cybercrime Convention Committee, "T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)," Council of Europe, March 1, 2017, p. 8, T-CY(2015)16

[151] Article 18 of the Budapest Convention.

[152] Cybercrime Convention Committee, *T-CY Guidance Note #10*, *op. cit.* note 150, p. 7

[153] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 199

[154] Cybercrime Convention Committee, *T-CY Guidance Note #10*, *op. cit.* note 150, p. 3

[155] SIRIUS, *EU Digital Evidence Situation 2nd Annual Report*, *op. cit.* note 29, p. 15

[156] Article 29 of the Budapest Convention

the disclosure of traffic data to trace the communication.[157] These requests benefit from an advantageous framework with limited grounds for refusal.[158] Their transmission and execution can be directed to a specialized global network of law enforcement authorities that operates 24 hours a day, seven days a week.[159] However, these forms of assistance are not meant to obtain data; for the disclosure of stored computer data,[160] states will rely on the limited texts regarding classical mutual assistance.[161]

299. Thus, the convention dedicated to improving cooperation with digital actors for digital evidence does not allow for efficient data requests, even though its framework is applicable to human trafficking. Consequently, some states have attempted to implement new solutions to bypass mutual legal assistance.

II. Innovative national reforms

300. Faced with the limits of voluntary cooperation among digital actors and the inefficiency of mutual assistance frameworks, some countries have innovated solutions by distorting territoriality through case law and legislation. Going further than traditional criteria,[162] the United States and Belgium offer new solutions (A) that still face limits

---

[157] Article 30 of the Budapest Convention

[158] Classically, "*the request concerns […] a political offense or an offense connected with a political offense, or […] is likely to prejudice its sovereignty, security,* ordre public *or other essential interests*," Articles 29.5 and 30.2 of the Budapest Convention. Moreover, in general, the absence of dual criminality cannot be a ground for refusal of the preservation request, Article 29.3 and 4.

[159] Article 35.1.b of the Budapest Convention. Even though the 24/7 network might facilitate the collection of evidence, Article 35.1.c, the points of contact might be located in a police entity that does not have the competence to request specific kinds of data in the national framework.

[160] Article 31 of the Budapest Convention, as well as assistance for real-time collection of traffic data and interception of content data, Articles 33 and 34.

[161] In particular, grounds of refusal are defined by the states, Article 25.4 of the Budapest Convention, and the transmission of requests should be directed through central authorities, Article 27.9.

[162] Indeed, various locators can be used to attach a person to a state: the location of data, "*the location(s) of Internet end-user (s) or connected devices; the location(s) of the servers or devices that store or process the actual data; the locus of incorporation of the Internet companies that run the service(s) in question*," B. de L. Chapelle, P. Fehlinger, "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 729. For other criteria, see T. Christakis, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)*, SSRN Scholarly Paper, ID 3086820, CEIS & The Chertoff Group White Paper, Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection, November 29, 2017, p. 34. The first criterion has been criticized for a long time: It "*could be decided exclusively on the basis of economic considerations and change if less expensive options arise*," *Ibid.* p. 24. Accounts and data can also be "*moved from place to place, in many cases across international borders, for reasons of performance and efficiency*," according to the "*data shard*" model, J. Daskal, "Unpacking the CLOUD Act," *Eucrim*, 2018, no. 4, pp. 220-225. Location criteria are not usually known by law enforcement authorities, R. Bismuth, "Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ?," *Revue critique de droit*

(B).

A. National solutions to secure requests to digital actors

301. The American solution. In 2013, an American warrant[163] ordered Microsoft to disclose emails stored in Ireland.[164] In 2016, the 2nd Circuit Court of Appeals decided that the warrant had extraterritorial effect, as the violation of privacy occurred "*where the data was located*."[165] Consequently, a mutual assistance process was required.[166] In 2017, the case was forwarded to the US Supreme Court, but prior to the court's decision, the US government passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[167] which requires any digital actor with a US office[168] to disclose any type of data[169] in their "*possession, custody, or control, regardless of whether [it] is located within or outside of the [US]*."[170] The criterion is the accessibility of data in the United States. Additionally, the CLOUD Act introduces the possibility for the digital actor to contest such orders if the "*subscriber is not a [US] person and does not reside in the [United States]*,"[171] or if it "*would violate the laws of a qualifying foreign government*,"[172] meaning a country that has reached an agreement with the United

international privé, Dalloz, 2019, vol. 2019/3, no. 3, p. 683. Finally, the criterion of the headquarters of digital actors might be too restrictive to secure cooperation from American operators.

[163] Based on 18 USC § 2703 (Stored Communications Act)

[164] Since the Snowden scandals and the need to conform to the General Data Protection Regulation, Microsoft has built servers in Europe to store European data, T. Christakis, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence*, *op. cit.* note 162, p. 25

[165] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 188. Since the statute does not explicitly authorize extraterritorial effects, those are prohibited, US Supreme Court, *Morrisson and others v. National Australia Bank Ltd. and others*, June 24, 2010, no. 08–1191, *547 F. 3d 167*, cited in R. Gauvain et al., *Rétablir la souveraineté de la France et de l'Europe*, *op. cit.* note 47, p. 15

[166] And "*even if the crime, victim, and target of the investigation are all located*" in the United States, J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 188

[167] On the basis of this act, a new warrant was issued to Microsoft, which agreed to provide the data. The pending Microsoft case "*was dismissed as moot*," L. Siry, "Cloudy days ahead," *op. cit.* note 60, p. 237

[168] The CLOUD Act does not require the company to be a US national and applies to any digital actor based in the United States, M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data*, *op. cit.* note 112, p. 28; P. Jacob, "La compétence des États à l'égard des données numériques - Du nuage au brouillard… en attendant l'éclaircie ?," *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, no. 3, p. 671

[169] With a warrant for content and traffic data, 18 USC § 2703.a to c; without a warrant for subscriber data, 18 USC § 2703.c.1.E and §2703.c.2

[170] 18 USC §2713, see J. Daskal, "Unpacking the CLOUD Act," *op. cit.* note 162, pp. 220-225; S. Bilgic, "Something old, something new, and something moot: the privacy crisis under the cloud act," *Harvard Journal of Law & Technology*, 2018, vol. 32, no. 1, p. 333

[171] 18 USC § 2703.h.2.A.i

[172] 18 USC § 2703.h.2.A.ii. The court can also modify or quash the order "*based on the totality of the circumstances*", § 2703.h.2.B.ii, upon consideration of the criteria listed at § 2703.h.3, such as "*the location and nationality of the subscriber or customer*" or "*the nature and extent of the provider's ties to and presence in the [US]*."

States on the subject.[173] Indeed, a US warrant could contradict a foreign law on privacy, and these agreements are meant to avoid contradictions. They also secure qualifying foreign countries' requests for data on their nationals or residents from US digital actors[174] when investigating "*serious crime*,"[175] including human trafficking.[176] Through an agreement, the US Attorney General and Secretary of State certify a foreign state;[177] this avoids mutual assistance processes while securing requests for data.

302. The Belgium solution. Going further, Belgium developed a solution to request data from digital actors outside its territory.[178] The first case law of the Belgian *Cour de Cassation* regarded a 2007 request for subscriber data[179] from Yahoo!, but the company was fined for its refusal to cooperate.[180] Yahoo! disputed the fine, alleging, in particular, that the request should be sent to the United States through a mutual assistance process. However, the first court "*held that Yahoo! [was] 'commercially present' on a Belgian territory*."[181] Later, the *Cour de Cassation* ruled that disclosure obligations apply to "*any operator or provider that actively aims its economic activities*

[173] 18 USC § 2703.h.1. The first agreement adopted under this disposition is the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, October 3, 2019

[174] 18 USC § 2703.h.5.A. As well as interception of content data, 18 USC §2511.j (see also § 2520.d.3); voluntary disclosure of content data, § 2702.b.9, and other kinds of data, § 2702.c.7 (see also § 2707.e.3); and installation of a pen register or a trap and trace device, § 3121.a (see also § 3124.d and e). Those requests shall not directly or indirectly "*target a [US] person or a person located in the [US]*," 18 USC § 2523.b.4.A and B.

[175] 18 USC § 2523.b.4.D.i

[176] 18 USC § 1590.a. Serious crimes are defined as any "*offense punishable by a maximum term of imprisonment of more than one year*," 18 USC § 3156

[177] 18 USC § 2523.b. Such certification needs the verification of "*substantive and procedural protections for privacy and civil liberties in light of the data collection*," 18 USC § 2523.b.1, "*appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning [US] persons*," 18 USC § 2523.b.2, and the affordance of reciprocal rights, 18 USC § 2523.b.4.I.

[178] J. Daskal, "Unpacking the CLOUD Act," *op. cit.* note 162, pp. 220-225

[179] It was based on Article 46bis of the Belgian Code d'instruction criminelle, which allows the prosecutor to identify the subscriber or habitual user of a service.

[180] P.D. Hert, M. Kopcheva, "International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case," *Computer Law & Security Review*, Elsevier Limited, 2011, vol. 27, no. 3, p. 292

[181] Consequently, only a request for content data should have relied on a mutual assistance process, *Ibid.* p. 293. On the contrary, the Appeal court held that Yahoo! was not using its own infrastructure and therefore fell outside the scope of the statute, and that considering that its services are accessible through a computer screen in Belgium is not enough to deem the company present on the territory, *Ibid.* pp. 295-296. This application of the "viewable" criterion is inconsistent with a French decision involving the same operator, Tribunal de grande Instance de Paris, *Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" v. Yahoo ! Inc. et Yahoo France*, May 22, 2000, Ordonnance de référé; Cour d'appel de Paris, 11ème chambre, *Timothy K. et Yahoo! Inc v. Ministère public, Association Amicale des déportés d'Auschwitz et des Camps de Haute Silésie, et MRAP*, March 17, 2004

on Belgian consumers [by] participating actively [in …] to the Belgium's economic life."[182] As a result, legislators included in the 2016 law[183] this new criterion of offering of services to consumers in the Belgian territory.[184] New requests are applicable to the subscriber, location, and traffic data,[185] for the latter two, upon request of the judge of instruction, for offenses punishable by at least one year of imprisonment,[186] which include human trafficking.[187] Soon, another case applied this reform. After a request to Skype, the company argued that the transmission of content data should rely on a mutual assistance process.[188] Skype was fined for lack of cooperation,[189] and it filed a complaint to dispute the fine.[190] The *Cour de Cassation* applied its criterion from the Yahoo! case: The request is not extraterritorial, as it is located in the place of reception of the data.[191] Even for content data, mutual assistance is not necessary.[192] Thus, Belgium introduced a new solution to link digital actors to their territory: the market and the location of consumers.[193]

303. Both national solutions broaden the territoriality of national orders and avoid mutual legal assistance. However, these solutions highlight further problems.

---

[182] Cour de cassation (Belgium), *YAHOO ! Inc.*, December 1, 2015, P.13.2082.N, ¶¶ 7-9. In particular, the court mentions the domain name system, the language, and the targeted advertisements depending on the localization. Moreover, the court highlighted that it is not an extraterritorial power and does not hinder other states' sovereignty since it "*does not require the presence abroad of Belgian magistrates [n]either does the measure require any coercive measure with limited extent, material action to be taken abroad*," *Ibid.* ¶ 6

[183] Loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, December 25, 2016

[184] M. Giacometti, "Collecte transfrontalière de preuves numériques," *op. cit.* note 98, p. 322.

[185] Non-compliance with the order is punishable by a fine of 26 to 10,000 euros under Article 46bis of the Code d'instruction criminelle. The reform also considered the interception of communications, Article 90quater §2, as a subsidiary measure, Article 90ter §1, for a limitative list of offenses that includes human trafficking, Article 90quater 2§.22°

[186] Article 88bis of the Code d'instruction criminelle. In the case of a human trafficking investigation, the judge may request data from nine months prior to the request. The same sanction is provided as for Article 46bis.

[187] Article 433quinquies of the Belgian Code pénal

[188] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 194

[189] V. Franssen, "The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level Reports: Practitioner's Corner," *European Data Protection Law Review*, 2017, vol. 3, no. 4, p. 539

[190] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 194

[191] Cour de cassation (Belgium), *Skype*, February 19, 2019, P.17.1229.N, ¶ 2. The court adds that the communication is Belgian, and that the obligation does not require "*to have a registered office, infrastructure or physical presence in Belgium*."

[192] *Ibid.* ¶ 9

[193] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 195

B. Limits to new solutions to request data from digital actors

304. Facing data sovereignty. These new solutions raise certain problems, particularly those regarding sovereignty. Indeed, "*the adoption of the CLOUD Act has been seen as a violation of […] state sovereignty*."[194] Data sovereignty is closely linked with the protection of the privacy of the population of the state[195] and of trafficked victims in particular. Thus, by lessening the "*territorial nexus*,"[196] the CLOUD Act challenges the protection of human rights.[197] To protect data sovereignty, the right to privacy can be strengthened. However, a national safeguard does not consider foreign legal safeguards where the servers or the affected person are located.[198] The process lacks "*democratic accountability*"[199] in the other states involved. For example, the Fourth Amendment to the US Constitution regarding privacy protects only US citizens,[200] and the code does not provide strong guarantees to request data

[194] L. Siry, "Cloudy days ahead," *op. cit.* note 60, p. 241. It is particularly true for traffic, location, and content data that "*are likely to create strong sovereignty conflicts*," V. Franssen, "The Belgian Internet Investigatory Powers Act," *op. cit.* note 189, p. 541

[195] States have a "*legitimate sovereign interest in regulating access to data of a state's own nationals and residents*," J. Daskal, "Borders and Bits," *op. cit.* note 72, pp. 193-196

[196] That would mean developing the extraterritorial jurisdiction of one state, bypassing the classical rules of competence, V. Franssen, "The Belgian Internet Investigatory Powers Act," *op. cit.* note 189, p. 539

[197] J. Daskal, "Borders and Bits," *op. cit.* note 72, pp. 193-196

[198] In particular, the measure's notification to make the right to contest it effective, R. Bismuth, "Le Cloud Act face au projet européen e-evidence," *op. cit.* note 162, p. 685. In particular, the CLOUD Act does not provide for notification of the measure when concerning European citizens, L. Siry, "Cloudy days ahead," *op. cit.* note 60, p. 249

[199] J. Daskal, "Borders and Bits," *op. cit.* note 72, p. 181. As she underlines, "*the concerns are about what is accessed (and there is a real risk law enforcement access will not be sufficiently targeted), and the tools used to access it (given among other things the risk of network investigative techniques going awry), and not primarily about who is accessing the data*," *Ibid.* p. 207

[200] T. Christakis, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence*, *op. cit.* note 162, p. 31; P. Jacob, "La compétence des États à l'égard des données numériques," *op. cit.* note 168, p. 674

disclosure.[201]

305. Facing EU law.[202] As a solution to protect data sovereignty and privacy, the CLOUD Act faces the EU's General Data Protection Regulation (GDPR),[203] which limits cross-border transmission of data. In principle, a foreign order to disclose data

[201] The content of those executive agreements has been criticized, in particular regarding the European level of protection of personal data, R. Bismuth, "Le Cloud Act face au projet européen e-evidence," *op. cit.* note 162, p. 691. Orders can be produced for the investigation of any offense, and they only provide for oversight and not an individualized judicial review, S. Bilgic, "Something old, something new, and something moot," *op. cit.* note 170, p. 340. The only grounds for denying a request are a conflict with the law of a qualifying foreign government or the absence of a link between the person and the United States, J. Daskal, "Unpacking the CLOUD Act," *op. cit.* note 162, pp. 220-225. Considering that a US person is defined broadly: "*a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States*," 18 USC § 2523.a.2. Even if a country prohibits targeting individuals associated with it, it is difficult to analyze those links prior to obtaining the data, S. Bilgic, "Something old, something new, and something moot," *op. cit.* note 170, p. 338. Those weak legal safeguards could be specifically criticized regarding the ECHR case law on data transmission, ECHR, *Centrum För Rättvisa v. Sweden (2)*, May 25, 2021, no. 35252/08, ¶¶ 318-328; ECHR, *Big Brother Watch and others v. the United Kingdom (2)*, May 25, 2021, 58170/13, 62322/14 and 24960/15, ¶¶ 395-397

[202] Aside from the EU-level norms, states can use "blocking statutes," which prohibit companies from providing certain data to foreign counterparts. These statutes are in opposition to the new solutions investigated, J. Daskal, "Borders and Bits," *op. cit.* note 72, pp. 193-196, in particular the CLOUD Act when requesting data of European persons, T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, p. 32. They create a contradiction for digital actors: they might be obliged by a national law to provide for data while being prohibited from doing so according to another national law, K. Geens, "Défis de la société numérique : perspectives politiques," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 32; T. Christakis, "La communication aux autorités américaines de données sur la base du Cloud Act est-elle en conflit avec le règlement général sur la protection des données ?," *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, no. 3, p. 705. However, those laws are not always broad enough to protect personal data. For example, the French blocking provisions protects "*documents or information of an economic, commercial, industrial, financial or technical nature, the disclosure of which is likely to affect the sovereignty*," Article 1 of the Loi n° 68-678 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères (July 26, 1968). Similarly, see the Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Moreover, the French statute has only been applied once in 50 years, O. Boulon, "Une justice négociée," *in* A. Garapon, P. Servan-Schreiber (eds.), *Deals de justice: le marché américain de l'obéissance mondialisée*, Presses universitaires de France, 2013, pp. 75-76; R. Gauvain et al., *Rétablir la souveraineté de la France et de l'Europe*, *op. cit.* note 47, pp. 51-52.

[203] T. Christakis, F. Terpan, "EU–US negotiations on law enforcement access to data," *op. cit.* note 90, p. 6; F. G'Sell, "Remarques sur les aspects juridiques de la « souveraineté numérique »," *La revue des juristes de Sciences Po*, 2020, no. 19, p. 58. The Directive 2016/680 only considers the transmission of data between competent authorities, primarily law enforcement authorities, Article 39 of the Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data. However, in this situation, the transfer takes place between a digital actor and a foreign state: the GDPR is applicable, Article 2 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

must be "*based on an international agreement.*"[204] By derogation, other grounds for transfer are available, particularly when "*necessary for important reasons of public interest*,"[205] but these grounds must be interpreted narrowly.[206] According to the CJEU, the notion of "public interest" includes the prevention and investigation of terrorism and serious crimes,[207] including human trafficking.[208] However, this provision does not develop the legal safeguards for a transfer on this ground: the process for those transfers remains unclear.[209] Nonetheless, these debates hide the fact that the new American statute is the most problematic, as it prohibits digital actors from providing data for European investigations, especially human trafficking, in the absence of an executive agreement.

306. The inadequacy of executive agreements. The executive agreements introduced by the CLOUD Act facilitate data transfer by securing direct communications, but they may also be seen as the US "*impos[ing] its law*."[210] This situation creates a distinction between qualifying foreign governments that will have easy access to data and those that will not and will continue to face challenges in obtaining data while the United States can request data disclosure. This division mostly depends on the will of the US government. Political considerations are designed to be

[204] Article 48 of the GDPR, in particular, in the absence of an adequacy decision, Article 45. With respect to the United States, the two adequacy decisions have been annulled by the CJEU. The Safe Harbor (Commission Decision 2000/520/EC) was invalidated by CJEU, *Maximillian Schrems v. Data Protection Commissioner (Schrems I)*, October 6, 2015, C-362/14; and the Privacy Shield (Commission Implementing Decision (EU) 2016/1250) by the CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*, July 16, 2020, C-311/18. A new draft has been published by the European Commission, Draft Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, December 13, 2022 The processing also must be "*necessary for compliance with a legal obligation to which the controller is subject; [or] in order to protect the vital interests of the data subject or of another natural person*," Article 6.1.c and d.

[205] Article 49.1.d of the GDPR, European Data Protection Supervisor, European Data Protection Board, "Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence," EU, July 10, 2019, p. 3

[206] T. Christakis, "La communication aux autorités américaines de données sur la base du Cloud Act," *op. cit.* note 202, p. 701

[207] CJEU, *Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a. (C-594/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána and Ireland*, April 8, 2014, C- 293/12 and C- 594/12, ¶ 42. Later, the CJEU mentions "*terrorist offenses and serious transnational crime*," CJEU, *Envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, July 26, 2017, Opinion 1/15, ¶¶ 148-151

[208] Article 83.1 of the Treaty on the Functioning of the EU

[209] T. Christakis, "La communication aux autorités américaines de données sur la base du Cloud Act," *op. cit.* note 202, p. 699

[210] T. Christakis, *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence*, *op. cit.* note 162, p. 35

involved in the certification process. The United States could certify "*both good and bad human rights records*,"[211] opening the use of American digital actors' data for questionable aims: when investigating trafficking, for example, to repatriate victims without offering them protection or prosecuting them. On the contrary, if the United States only "*privilege[s] Western democracies and leave[s] the majority of countries in the [mutual legal assistance treaties] world*,"[212] these latter countries may develop data location requirements, impeding access to such data.

307. Conclusion of the section: the "*jungle*"[213] of cross-border evidence. Through cooperation between states and between states and digital actors, all examined frameworks create multiple texts regarding requests for data. [214] Thus, multiple solutions exist to request data from digital actors for human trafficking investigations. However, they all face numerous limits, partly because they are not adapted to the reality of cyberspace or because they question the protection of other issues, such as human rights and sovereignty.[215] Through national and supranational solutions, digital actors are set aside and must comply with possibly contradictory regulations.[216] To bypass actual challenges, the later reforms recognized increased autonomy for digital actors, offering a pragmatic approach to their own sovereignty.

Section 2. Autonomous cooperation with digital actors to repress cyber trafficking

308. Sovereignty as participation. The cooperation with digital actors through states is not adapted to current needs.[217] States lack a "*sovereign authority with the power to compel obedience among*"[218] international actors who possess data that are needed to investigate cyber trafficking. Slaughter defines the evolution of sovereignty as participation: "*to engage with each other in networks that would strengthen [states] and improve their ability to perform their designated government tasks individually and collectively*."[219] Nonetheless, those networks might need to be extended to include

[211] S. Bilgic, "Something old, something new, and something moot," *op. cit.* note 170, pp. 346-347
[212] *Ibid.* p. 345
[213] Cybercrime Convention Committee, *Transborder access to data and jurisdiction*, *op. cit.* note 46, p. 7
[214] This lack of harmonization at national and international levels does not favor legal certainty.
[215] P. Jacob, "La compétence des États à l'égard des données numériques," *op. cit.* note 168, p. 668
[216] V. Franssen, "The Belgian Internet Investigatory Powers Act," *op. cit.* note 189, p. 540
[217] F. Vadillo, "Techniques d'enquête numérique judiciaire : les défis d'une survie dans la modernité," *Enjeux numériques*, Annales des mines, September 2018, no. 3, p. 60
[218] D.G. Post, "Governing Cyberspace," *Wayne Law Review*, 1996, vol. 43, no. 1, pp. 170-171
[219] A.-M. Slaughter, *A new world order*, Princeton University Press, 2004, p. 34

private entities. The participation of digital actors can be divided[220] between internal and external sovereignty.[221] The former rests on their power over subjects through legitimate coercion and the positive exercise of "*supreme power*,"[222] while the latter lies in an autonomy at the international level between all owners of sovereignty through the negative exclusion of "*a superior power to [the] State*."[223] In the end, "*internal supremacy and external autonomy are two sides of the same coin*."[224]

309. Therefore, recent solutions regarding direct cooperation between states and digital actors, "*go beyond the notions of non-state-centered systems of coordination*."[225] Indeed, some rules or techniques needed to obtain data have been established by digital actors, while the state has been absent. Thus, digital actors exercise a pragmatic internal sovereignty, as "*the sovereign [state] seems to be overwhelmed*"[226] (§2). Additionally, external sovereignty is facing a timid legal recognition through new procedures to obtain data (§1).

§1. Explicit recognition of external sovereignty of digital actors

310. The birth of digital actors' external sovereignty is exemplified by the latest EU and Council of Europe texts on the procurement of data, which provide an insight into the not-so-recent powers of digital actors, by "legalizing" their current voluntary cooperation with states. Such autonomy can be underlined from both a formal (II) and a material perspective (III). To begin with, the concept of external sovereignty should be developed (I).

[220] Numerous other kinds of sovereignty classifications have been theorized, see, for example, B.H. Bratton, *The stack: on software and sovereignty*, MIT Press, Software studies, 2015, p. 56
[221] K. Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet*, 2012, vol. 4, no. 3-4, p. 53
[222] O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, pp. 15-16
[223] T. Christakis, *"European Digital Sovereignty," op. cit.* note 202, p. 5; J. Combacau, S. Sur, *Droit international public*, LGDJ, 2014, p. 236. The former rests on a vertical application of coercion and public authority, while the latter supposes a horizontal protection of each other's sovereignty, J. Adams, M. Albakajai, "Cyberspace," *op. cit.* note 134, p. 260
[224] J.L. Cohen, *Globalization and sovereignty: rethinking legality, legitimacy and constitutionalism*, Cambridge University Press, 2012, p. 27. See also P. Mortier, *Les métamorphoses de la souveraineté*, Thesis, Université d'Angers, January 1, 2011, ¶ 139
[225] S. Sassen, *Losing control: sovereignty in an age of globalization*, Columbia University Press, University Seminars: Leonard Hastings Schoff Memorial Lectures, 1996, p. 14
[226] M. Delmas-Marty, *Libertés et sûreté dans un monde dangereux*, Seuil, La couleur des idées, Éditions du seuil, 2010, pp. 196-197

I. Concept of external sovereignty

311. Permanent Court of International Justice position. The basis of external sovereignty traditionally rests on the Wimbledon and Lotus decisions from the Permanent Court of International Justice. The former decision,[227] which was made in 1923, recognizes the rights of sovereigns to interact in the international community without questions about their sovereignty. Consequently, the content of sovereign powers depends on the framework of the international community.[228] Going further, the Lotus decision[229] underlines that, inside its territory, the state is internally sovereign. Outside, it is sovereign as well, as it can negotiate its powers outside its territory with other states. Without treaties, the "*principle of mutual exclusion is the essence of external sovereignty*":[230] autonomy is "*inviolable*."[231]

312. Criticisms. However, these decisions are based on one criterion: the will of the sovereigns.[232] Today, the notion of consent is criticized due to "*the interdependence of states*."[233] Individual will is still limited by the will of the other sovereigns[234] and by "*group logic*" due to the increasing "*collective dimension of international life*."[235] However, the processes framing international law did not fundamentally change; external sovereignty shifted from an individualistic perspective (a state's sovereignty) to a pluralistic perspective (states' sovereignty).[236] Thus, sovereignty continues to rest with states, the origin of "*all international normativity*."[237] Other actors, such as non-governmental and business ones, might produce texts, but the source of international obligations remains treaties that have been ratified by the

---

[227] Permanent Court of International Justice, *Wimbledon*, August 17, 1923
[228] J.-D. Mouton, "L'état selon le droit international - diversité et unité," *in* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 91
[229] Permanent Court of International Justice, *Lotus*, September 7, 1927, no. 9, pp. 17-18
[230] K. Irion, "Government Cloud Computing and National Data Sovereignty," *op. cit.* note 221, p. 53
[231] J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018, p. 11
[232] L. Bal, *Le mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Thesis, Université de Strasbourg, February 3, 2012, n. 52
[233] J. Charpentier, "Le phénomène étatique à travers les grandes mutations politiques contemporaines," *in* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 31
[234] L. Bal, *Le mythe de la souveraineté en droit international*, *op. cit.* note 232, p. 82. As such, the equality between sovereigns is a legal fiction. See, for example, the permanent members of the United Nations Security Council, or the different weight in negotiations depending on economic or military power, *Ibid.* p. 217
[235] L. Bal, *Le mythe de la souveraineté en droit international*, *op. cit.* note 232, p. 78
[236] *Ibid.* p. 369
[237] *Ibid.* p. 114

"*privileged circle*" of states.[238] Nevertheless, it is not yet clear if states are the only actors who are involved in the creation of international law. Indeed, "*the contemporary state is no longer the sole expression of political power*."[239]

313. Diplomatic sovereignty. Some authors add, as an element of sovereignty, the power "*to represent the [sovereign] in the international environment*."[240] The diplomatic scene that once faced terrestrial and maritime control[241] is now turning to "*Internet domination*."[242] States are no longer the only ones to use diplomacy to extend their power in cyberspace.[243] The negotiation processes for data requests, although primarily interstate, highlight the participation of digital actors.[244] The Council of Europe negotiated the Second Additional Protocol to the Budapest Convention with "c*lose interaction with civil society, data protection organizations, and industry*."[245] At the EU level, the electronic evidence package included bilateral meetings with Microsoft, Apple, Google, Twitter, and Facebook.[246] In general, according to a 2021 report, "*612 companies, groups, and business associations [are] lobbying the EU's digital economy policies [and] spend over € 97 million annually lobbying the EU institutions. This makes tech the biggest lobby sector in the EU*."[247] Therefore, digital actors, and "*transnational*

[238] *Ibid.* p. 46
[239] *Ibid.* p. 344
[240] W.P. Nagan, C. Hammer, "The Changing Character of Sovereignty in International Law and International Relations," *Columbia Journal of Transnational Law*, 2004, vol. 43, pp. 150-151; J.-P. Queneudec, "Conclusions," *in* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 312
[241] P. Bellanger, "De la souveraineté numérique," *Le débat*, Gallimard, 2012, vol. 2012/3, no. 170, p. 153
[242] Y. Poullet, "Quelques réflexions d'avant-propos," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 8
[243] A. Desforges, "Les stratégies européennes dans le cyberespace," *in* A. Blandin-Obernesser (ed.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 83
[244] In 2017, "*Denmark announced the appointment of an ambassador to the global digital giants*," P. Türk, "La 'souveraineté numérique' : un concept pertinent en droit constitutionnel ?," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 19; followed by Austria in 2020; and by the EU in 2022, S. Feingold, "Why the European Union is opening a Silicon Valley 'embassy,'" *World Economic Forum*, August 16, 2022, online https://www.weforum.org/agenda/2022/08/why-the-european-union-is-opening-a-silicon-valley-embassy/ (retrieved on August 23, 2022). "*Techplomacy*" is therefore in development, C. Blume, M. Rauchbauer, "How to Be a Digital Humanist in International Relations: Cultural Tech Diplomacy Challenges Silicon Valley," *in* H. Werthner et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, p. 104
[245] Cybercrime Convention Committee, "Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime Workplan and working methods," Council of Europe, November 29, 2017, p. 3, T-CY (2017)20. Indeed, six rounds of consultations with stakeholders were carried out, in which participants included, for example, the European Association of European Internet Services Providers Associations, Kaspersky, and Facebook.
[246] European Commission, *Working document impact assessment accompanying the e-evidence proposals*, *op. cit.* note 48, p. 140
[247] M. Bank et al., *The lobby network: big tech's web of influence in the EU*, Corporate Europe Observatory, LobbyControl e.V., August 2021, p. 6

organizations are autonomous or quasi-autonomous actors in world politics."[248]

314. External sovereignty rests not only on the process of creating international law and the autonomy to join a treaty but also on the subjects of international obligations. Classically, these subjects are the states, but the new frameworks for obtaining digital evidence are modifying these classical rules.

II. A procedural external sovereignty

315. An original approach. The Council of Europe first started working on cross-border evidence,[249] and as soon as the GDPR was published in 2016, the EU Council called for an EU instrument on the same topic.[250] These texts are meant to resolve the limits to the current cooperation systems,[251] especially when they are voluntarily based, which are deemed dangerous for fundamental rights and national sovereignties.[252] The Second Additional Protocol to the Budapest Convention[253] has been open to for ratification since May 2022, and the E-evidence package was adopted by the EU in July 2023 after 7 years of negotiation.[254] Both instruments offer original

[248] S.J. Kobrin, "Sovereignty@Bay: Globalization, Multinational Enterprise, and the International Political System," *in* A.M. Rugman, T. Brewer (eds.), *The Oxford Handbook of International Business*, Oxford University Press, September 2, 2009, p. 24

[249] While the EU was negotiating the update of data protection frameworks (the GDPR and the Directive 2016/680), the Council of Europe established two successive working groups since 2012, resulting in the mandate to prepare a second protocol to the Budapest Convention in 2017, Council of Europe, "Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques : Vers un protocole à la Convention de Budapest," September 5, 2019

[250] EU Council, "Council conclusions on improving criminal justice in cyberspace," EU, June 9, 2016, p. 4. Framed in the Area of Freedom, Security and Justice, Article 82 of the Treaty on the Functioning of the EU

[251] Cybercrime Convention Committee, "Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol version 3," Council of Europe, May 28, 2021, ¶ 94

[252] European Commission, "Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime," EU, January 26, 2001, p. 25

[253] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, Council of Europe

[254] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (E-evidence regulation); and the Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. The regulation defines electronic evidence depending on the kind of data requested, Article 3.8. A broader definition could include any "*electronic means that allows proving relevant facts for the process, whether they are physical or electronic facts, and that is composed of two elements necessary for its existence, which determine the specialty of electronic evidence in relation to other means of proof a technical element that will refer either to a hardware in the judicial venue or to an electronic channel when it is presented through a computerized procedural management system and a logical element or*

procedures. Cooperation does not go through two states to obtain data from a digital actor; instead, the texts recognize a direct cooperation between the sending state and the digital actor. This process bypasses the classical sovereignty of the state in which the data is located while recognizing the autonomy of digital actors.[255]

316. General frameworks. The Second Additional Protocol requires states to create legal provisions "*to empower [their] competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party*"[256] and to compel that party's service providers to disclose data.[257] The order might be applicable for any type of offense, depending on the limits set by the states,[258] and these limits can restrict its production "*by, or under the supervision of, a prosecutor or other judicial authority*."[259] However, the Budapest Second Additional Protocol is limited to subscriber data;[260] for other types of data, states will rely on the classical mutual assistance procedures.[261] As law enforcement authorities can simultaneously request various types of data, classical procedures will be more efficient.[262] The EU E-evidence regulation means to enable member states to " *order a service provider offering services in the Union and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of data*."[263] The regulation mainly creates the European Production Order. Regarding subscriber and access data,[264] it is issued by a judicial authority or a prosecutor,[265] while regarding traffic and

software that will have an intangible nature," F. Bueno de Mata, "Análisis crítico de las futuras órdenes europeas en materia de prueba electrónica," *in* F. Bueno de Mata, I. González Pulido (eds.), *La cooperación procesal internacional en la sociedad del conocimiento*, Atelier Libros Jurídicos, Processus iudicii no. 59, 2019, p. 326

[255] S. Tosza, "Cross-border gathering of electronic evidence," *op. cit.* note 42, p. 278

[256] Article 7.1 of the Budapest Protocol

[257] Article 7.2.a of the Budapest Protocol, see also Cybercrime Convention Committee, *Draft Protocol version 3*, *op. cit.* note 251, ¶ 100. Unfortunately, those provisions are not preserved from possible reserve, as parties might declare not applying it, Article 7.9.a

[258] This may or may not include human trafficking.

[259] Article 7.2.b of the Budapest Protocol

[260] Article 18.3 of the Budapest Convention; Article 6 of the Budapest Protocol also takes domain name registration information into account. However, it is the most requested kind of data, Cybercrime Convention Committee, "Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence," Council of Europe, 2021, ¶ 92

[261] Updated by the Budapest Protocol, Article 8 for subscriber and traffic data; Article 9 for expedited disclosure of stored computer data in an emergency

[262] Cybercrime Convention Committee, *Draft Protocol version 3*, *op. cit.* note 251, ¶ 125

[263] Article 1.1 of the E-evidence regulation

[264] Article 3.9 and 10 of the E-evidence regulation

[265] Article 4.1 of the E-evidence regulation, or any other competent authority and validated by a judicial authority or a prosecutor.

content data,[266] it is issued by a judicial authority, or another authority, including a prosecutor, and then validated by a judicial authority.[267] The order is "*addressed directly to the designated establishment or to the legal representative designated by the service provider*" or, in emergency cases with a lack of response, "*to any other establishment or legal representative of the service provider in the Union*."[268] Consequently, the order must "*be treated, in essence, as an order in the country where the request is being sent*."[269] For subscriber and identification data, an order "*may be issued for all criminal offenses*," while an order on traffic and content data may be issued "*for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years*,"[270] which usually includes human trafficking.

317. Addressees. A core element is the definition of digital actors. The Budapest Second Additional Protocol uses the definition of the main convention and includes entities providing "*the ability to communicate by means of a computer system*" and entities processing and storing data "*on behalf of such communication service*."[271] Broadly interpreted,[272] most digital actors fit this definition, but it seems too restrictive to face the evolution of communication technologies. The EU definition is more developed. It includes electronic communications services,[273] *"internet domain name*

[266] Article 3.11 and 12 of the E-evidence regulation
[267] Article 4.2 of the E-evidence regulation. For instance, unlike the European arrest warrant, which requires the issuing authority to be independent of the executive power (CJEU, *Minister for Justice and Equality v. PF*, May 27, 2019, C-509/18, ¶ 57; CJEU, *Minister for Justice and Equality v. OG and PI*, May 27, 2019, C-508/18 and C-82/19 PPU, ¶ 90; CJEU, *JR and YC*, December 12, 2019, C-566/19 PPU and C-626/19 PPU, ¶ 58), the CJEU confirmed for the European investigation order that is might be issued by any prosecutor, CJEU, *Criminal proceedings against A and Others*, December 8, 2020, C-584/19, ¶ 75
[268] Article 7.1 and 2 of the E-evidence regulation
[269] J. Daskal, D. Kennedy-Mayo, "Budapest Convention: What is it and How is it Being Updated?," *Cross-Border Data Forum*, July 2, 2020, online https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/ (retrieved on April 11, 2021)
[270] Article 5.3 and 4 of the E-evidence regulation proposal, the latter of which also adds a list of specific offenses "*if they are wholly or partly committed by means of an information system*," when harmonized by a directive. However, it does not include the offense of human trafficking. The threshold of three years of imprisonment has been criticized as too low, M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data*, *op. cit.* note 112, pp. 35-36, and as challenging an harmonized application of the instrument due to different national penalizations of the same offense, H. Christodoulou, L. Gaurier, A. Mornet, "La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?," *European Papers - A Journal on Law and Integration*, European Papers (www.europeanpapers.eu), June 30, 2021, vol. 2021 6, no. 1, p. 438
[271] Article 3.1 of the Budapest Protocol and Article 1.c of the Convention
[272] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, *op. cit.* note 141, ¶¶ 26-27
[273] Provision of "'*Internet access service*,' '*interpersonal communications service*'" and "*services consisting wholly or mainly in the conveyance of signals*," Article 2.4 of the Directive (EU) 2018/1972 establishing the European Electronic Communications Code

and IP numbering services," and information society services[274] that "*enable their users to communicate with each other*" or "*make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user*."[275] In any case, digital actors are still linked to a state.[276] In the Budapest Second Additional Protocol, digital actors are to be located, "*in the territory of another Party*."[277] It remains to be seen if this notion will be restrictively interpreted as the location of a headquarters or broadly as any type of territorial link. On the contrary, the EU goes further, as the regulation "*applies to service providers which offer services in the Union*."[278] This criterion's scope is broad enough to encompass all necessary digital actors.

318. Procedure. The Budapest Second Additional Protocol establishes a maximal limit for answers of 30 days, which is seen as too long due to the volatility of data.[279] Conversely, the EU requires that the order be executed within 10 days.[280] These deadlines are "*much shorter than, for instance, for the [European Investigation Order]*."[281] Additionally, the Budapest Convention allows for digital transmission of the requests.[282] On the contrary, the E-evidence regulation mandates the transmission of requests and information "*through a secure and reliable decentralized IT system*."[283] In response, the EU developed the e-CODEX platform, "*a decentralized and*

[274] Meaning "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*," Article 1.1.b of the Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services
[275] Article 3.3 of the E-evidence regulation
[276] P. Jacob, "La compétence des États à l'égard des données numériques," *op. cit.* note 168, p. 670
[277] Article 7.1 of the Budapest Protocol. Therefore, "*The service provider [must] be physically present*" in the territory of the receiving state, Cybercrime Convention Committee, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime*, *op. cit.* note 260, ¶ 99
[278] Article 2.1 of the E-evidence Regulation. It means that the provider enables " *natural or legal persons in a Member State to use [its] services*" and has "*a substantial connection based on specific factual criteria to [this member state]; such a substantial connection is to be considered to exist where the service provider has an establishment in a Member State, or, in the absence of such an establishment, where there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States*," Article 3.4. This interpretation of connection is harmonized with the one in the GDPR, P. Jacob, "La compétence des États à l'égard des données numériques," *op. cit.* note 168, p. 673
[279] Article 7.7 of the Budapest Protocol
[280] 96 or eight hours in case of emergency, Article 10.2 and 4 of the E-evidence regulation; Article 10.6 also sets a timeframe to request further information to execute the order. However, to inform them that it will not be executed, the provision only considers answering "*without undue delay*," Article 10.7
[281] S. Tosza, "Cross-border gathering of electronic evidence," *op. cit.* note 42, p. 281
[282] Article 7.6 of the Budapest Protocol
[283] Article 19.1 of the E-evidence regulation. If not possible, "*the transmission shall be carried out by the most appropriate alternative means, taking into account the need to ensure an exchange of information which is swift, secure and reliable, and allows the recipient to establish authenticity*," Article 19.5

interoperable system for cross-border communication for the purpose of facilitating the electronic exchange of data"[284] to harmonize the various channels for data transmission. However, this tool has still to be fully implemented. Meanwhile, law enforcement authorities rely on digital actors' procedures, underscoring their autonomy to shape the process of requesting evidence.

319. The recognition of digital actors' sovereignty is still limited. In the Council of Europe framework, both the scope and procedure of the text offer little improvement: It continues to rely on territoriality. On the contrary, the EU regulation goes further. However, in both cases, the texts frame new obligations for digital actors, recognizing their coercion powers, regarding the procedure and the content of requests.

III. A material external sovereignty

320. **The role of third states.** Traditionally, external sovereignty results in the control of foreign acts in international judicial cooperation procedures. However, in the new texts, cooperation goes directly from a state to a digital actor, while, other states might have an interest in protecting the privacy of the requested data. The Budapest Second Additional Protocol protects the sovereignty of third states: It is not applicable as such, and needs a national transposition. Consequently, the state, "*when an order is issued […] to a service provider in its territory, […can require] simultaneous notification of the order*."[285] This process degrades the goal of quick cooperation, so the Council of Europe highlighted that it should be limited to "*identified circumstances*."[286] Nonetheless, when the state is not notified, the digital actor will need to check on grounds for refusal. Under the E-evidence regulation, the issuing authority must notify the enforcing state[287] of requests regarding traffic and content

[284] Article 3.1 of the Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerized system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system)

[285] Article 7.5.a of the Budapest Protocol, in particular to check grounds of refusal, in particular if the "*disclosure may prejudice criminal investigations*," Article 7.5.c.i (which cannot be known by the digital actor), or the other grounds set by national law, Article 7.5.c.ii; those grounds are limited in the Convention (political offense and prejudice to sovereignty, Article 27.4). The principle of dual criminality is more flexible, see Article 5.6 of the Protocol.

[286] Cybercrime Convention Committee, *Draft Protocol version 3*, *op. cit.* note 251, ¶ 108

[287] Meaning, "*the Member State in which the designated establishment is established or the legal representative resides and to which a European Production Order and an EPOC or a European Preservation Order and an EPOC-PR are transmitted by the issuing authority for notification or for enforcement in accordance with this Regulation*," Article 3.16 of the E-evidence regulation. However, it should be noted that the enforcing state might be different from the affected state, T. Christakis, "Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament's E-Evidence

data, unless "*there are reasonable grounds to believe that: (a) the offense has been committed, is being committed, or is likely to be committed in the issuing State; and (b) the person whose data are requested resides in the issuing State*."[288] When this notification is made, the enforcing state must quickly assess the order, and its grounds for refusing its enforcement are limited. It should be mentioned that the execution of the request can be refused when, "*in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right.*"[289] In the absence of notification, in practice, the digital actor will verify the content, scope, and authorization of the order, with little grounds for refusal.[290] The original proposal provided a wider margin of appreciation to digital actors. In particular, they were to refuse execution if the order "*manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive*."[291] In both versions, the manifest characteristic of such a violation is not defined and could be difficult to assess due to the limited information in the order certificate.[292] Finally, the enforcing state also has a strong role in case of the lack of compliance of digital actors: Consequently, the issuing authority will request the

Draft Report," *Cross-Border Data Forum*, January 7, 2020, online https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/ (retrieved on April 12, 2021)

[288] Article 8.1 and 2 of the E-evidence regulation. The issuing authority also must notify the concerned person, Article 13.1, although no delay is set. This amendment was meant to reduce the weaknesses of the original proposal, M. Rojszczak, "e-Evidence Cooperation in Criminal Matters from an EU Perspective," *Modern Law Review*, Wiley, July 2022, vol. 85, no. 4, pp. 1010-1012

[289] The other grounds for refusal are the followings: when the data "*is protected by immunities and privileges granted under the law of the enforcing State, […] or the data requested is covered by rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media*"; when the enforcement "*would be contrary to the principle of* ne bis in idem"; or "*the conduct for which the order has been issued does not constitute an offense under the law of the enforcing State, unless it concerns an offense listed within the categories of offenses set out in Annex IV*," which includes human trafficking, Article 12.1 of the E-evidence regulation

[290] Incomplete orders do not imply refusal of execution but a request for information, Article 10.6 of the E-evidence regulation. The digital actor must inform states' authorities if the order "*could interfere with immunities or privileges, or rules on the determination or limitation of criminal liability that relate to the freedom of press or the freedom of expression in other media in the enforcing State*," Article 10.5. Moreover, the addressee might refuse to execute the order due to a conflict "*with the applicable law of a third country*," Article 17.1 (for example, the US legislation protecting the privacy of its citizens). The case will then be assessed by the issuing authority and, if necessary, by a competent court, Article 17.3 and 4.

[291] Article 9.5 of the E-evidence regulation as in the original proposal of the European Commission, Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final (2018).

[292] M. Corhay, "Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal," *European Papers - A Journal on Law and Integration*, European Papers (www.europeanpapers.eu), June 30, 2021, vol. 2021 6, no. 1, p. 464

enforcing state to enforce the order.[293]

321. Critics. The margin of appreciation of digital actors regarding the conformity and legality of the orders varies between texts and will be different depending on countries' transpositions. Such a private assessment of orders has been highly criticized as a privatization of the state's sovereignty: "*It appears unrealistic to expect that private companies will effectively engage in [these types] of sensitive and complex legal assessments*."[294] The authors, in particular, doubt that digital actors have enough information to make these assessments,[295] which might be why the final text of the E-evidence regulation broadly limited digital actors' possible grounds for refusal. Their grounds for refusal are not even a full power to deny the execution of the order, but a mere request to reconsider its execution, as the final assessment is made by a state. Nonetheless, it remains that part of this assessment is still already checked voluntarily by digital actors. They act as "*extended arms of law enforcement*"[296] by executing judicial cooperation and by being included as main addresses of the texts, while the enforcing state acts as a mere intermediary. Thus, in assessing its content, digital actors will produce an autonomous interpretation of criteria and guarantees. States face a "*reallocation of protective functions*,"[297] as they cannot review all orders.[298]. Consequently, this framework supports mutual trust with digital actors to assess data request orders.

322. Mutual trust and unilateral recognition. The EU text might create a new level of mutual recognition.[299] Recognition is almost automatic, although the enforcing state can be involved in the procedure. However, "*one may question whether there is still*

[293] Article 16 of the E-evidence regulation
[294] M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data*, *op. cit.* note 112, p. 40; C.-D. Bulea, "Cooperarea judiciară în materie penală şi respectarea drepturilor omului. Probleme actuale. Probele electronice," *Caiete de drept penal*, 2021, vol. XVII, no. 1, p. 85
[295] J. Daskal, D. Kennedy-Mayo, *Budapest Convention*, *op. cit.* note 269 However, it can be highlighted that the European Production Order Certificate has to include "*grounds for the necessity and proportionality of the measure or further details about the investigations*," Article 5.5.i and Annex I Section M of the E-evidence regulation
[296] S. Tosza, "All evidence is equal," *op. cit.* note 54, p. 182. Those evolutions could appear "*to be at odds with the principles of corporate social responsibility emerging under international and EU law*," M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data*, *op. cit.* note 112, p. 40. For more detail see *infra* Part 2. Title 2. Chapter 1.
[297] T. Christakis, "E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead," *Cross-Border Data Forum*, January 14, 2019, online https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/ (retrieved on April 12, 2021)
[298] J. Daskal, D. Kennedy-Mayo, *Budapest Convention*, *op. cit.* note 269
[299] Article 82 of the Treaty on the Functioning of the EU

any recognition since there is no authority to actively recognize the order."[300] The issuing state unilaterally requests data abroad,[301] which is a proof of mutual trust in the judicial systems of each member state[302] through the presumption of equivalent protection.[303] Nonetheless, this presumption is not automatic and can be discussed regarding fundamental rights.[304] The CJEU established a "*two-step procedure*," in which the "*authority must, first of all, make a finding of general or systemic deficiencies in the protections […] and, then, seek all necessary supplementary information from the issuing […] authority as to the protections for the individual concerned*."[305] However, under the E-evidence regulation, those verifications will not be undertaken by member states but by digital actors.[306] Mutual trust is then directed toward states and private entities, creating "*a completely new model of cooperation in criminal matters with a significant role of a private actor*."[307] Part of the doctrine has been qualifying this evolution as a privatization of mutual trust,[308] and at least it has

[300] S. Tosza, "All evidence is equal," *op. cit.* note 54, p. 177

[301] It has also been argued that this instrument meant that the issuing authorities would be able to protect the interests of the other member states, proving "*a high level of mutual trust*," but not "*an absolute guarantee*," T. Christakis, *E-Evidence in a Nutshell*, *op. cit.* note 297. However, it should be noted that "*each of the Member States prescribes to the same European legal framework for human rights, and in particular privacy and data protection*": Insecurities may stem primarily from third countries, specifically the CLOUD Act, L. Siry, "Cloudy days ahead," *op. cit.* note 60, p. 246.

[302] C.-D. Bulea, "Probele electronice," *op. cit.* note 294, p. 75

[303] ECHR, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Irlande*, June 30, 2005, no. 45036/98, ¶¶ 105-106; ECHR, *Michaud v. France*, December 6, 2012, no. 12323/11, ¶¶ 102-111; ECHR, *Avotiņš v. Latvia*, May 23, 2016, no. 17502/07, ¶¶ 101-104; ECHR, *Bivolaru and Moldovan v. France*, March 25, 2021, 40324/16 and 12623/17, ¶¶ 96-103

[304] The case law of the CJEU evolved on that point. In the beginning, recognition was automatic, even when facing fundamental rights, CJEU, *Proceedings relating to the execution of European arrest warrants issued against Ciprian Vasile Radu*, January 29, 2013, C-396/11; CJEU, *Stefano Melloni v. Ministerio Fiscal*, February 26, 2013, C- 399/11. It changed its position three years later to assess that fundamental rights should be taken into account during the recognition process, CJEU, *Pál Aranyosi and Robert Căldăraru v. Generalstaatsanwaltschaft Bremen*, April 5, 2016, C-404/15 and C-659/15 PPU. See also D. Fransen, "Face à l'internationalisation : existe-t-il des compétences irréductibles du juge interne ?," *in* Société française pour le droit international, M. Ubéda-Saillard (eds.), *La souveraineté pénale de l'État au XXIème siècle*, Éditions Pedone, 2018, pp. 168-169; C.-D. Bulea, "Probele electronice," *op. cit.* note 294, pp. 76-77

[305] CJEU, *Aranyosi and Căldăraru*, *op. cit.* note 304, ¶ 104; M. Stefan, G. González Fuster, *Cross-border Access to Electronic Data*, *op. cit.* note 112, p. 9

[306] For example, regarding in particular the E-evidence regulation, it has been argued that the sanctions are too heavy to consider that the verification will be done correctly, T. Christakis, *Lost in Notification?*, *op. cit.* note 287

[307] S. Tosza, *Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations*, SSRN Scholarly Paper, ID 3517878, Rochester, NY, Social Science Research Network, September 19, 2019, p. 20

[308] A. Tinoco Pastrana, "Las órdenes europeas de entrega y conservación: La futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea," *Cuadernos de política criminal*, Dykinson, 2021, no. 135, p. 216; V. Mitsilegas, "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence," *Maastricht Journal of European and Comparative Law*, SAGE Publications Ltd, June 1, 2018, vol. 25, no. 3, pp. 263-265

"*undergone a metamorphosis*."[309]

323. While European frameworks build an embryonic external sovereignty for digital actors, framing data requests also highlights the existence of their internal sovereignty.

§2. Implicit delegation of internal sovereignty

324. Through their own type of external sovereignty, digital actors contribute to international relations and obtain new obligations to cooperate with states. They do not define the content of the law, but they will concur in its interpretation. Digital actors can even create their own norm in a new form of internal sovereignty. In particular, they have a major role in framing cyberspace,[310] making it indispensable to exercise fundamental rights.[311] Most technical rules come from digital actors,[312] and some technical regulations of cyberspace directly affect law enforcement authorities when they collect or request data, especially to investigate cyber trafficking. Thus, digital coercion of digital actors is demonstrated by their implementation of code rather than law (I). Additionally, the digital actors rule autonomously, facing the failure of the state to regulate data conservation (II) and the absence of the regulation of encryption (III).

I. The concept of internal sovereignty

325. Dividing the production of norms among sovereigns. Bodin recognized the need for the sovereign to be independent from other sovereigns and to monopolize "*the power to enact positive law*."[313] Bodin lists "marks" of sovereignty[314] as parts of

[309] H. Christodoulou, L. Gaurier, A. Mornet, "La proposition e-evidence," *op. cit.* note 270, p. 434
[310] M. Palacio, "Protection et surveillance augmentées Le nouveau paradigme sécurité et liberté," *Cahiers de la sécurité et de la justice*, INHESJ, Deuxième trimestre 2019, no. 47, p. 11. Indeed, cyberspace is "*to a large extent, a creation of the private sector,*" N. Choucri, D.D. Clark, "Who controls cyberspace?," *Bulletin of the Atomic Scientists*, SAGE Publications, September 1, 2013, vol. 69, no. 5, p. 23. Up to the point of naming part of cyberspaces "*cyber baronnies*," X. Raufer, *Cyber-criminologie*, CNRS Éditions, 2015, p. 18; or arguing for the "*"colonization" of the European digital market by major American platforms*," B. Thieulin, *Towards a European digital sovereignty policy*, Opinion of the Economic, Social and Environmental Council, France, March 13, 2019, p. 8
[311] See, for example, Human Rights Council, "Resolution 20/8. The promotion, protection and enjoyment of human rights on the Internet," UN, July 16, 2012, A/HRC/RES/20/8; Human Rights Council, "Resolution 26/13. The promotion, protection and enjoyment of human rights on the Internet," UN, July 14, 2014, A/HRC/RES/26/13; and ECHR, *Ahmet Yildrim v. Turkey*, December 18, 2012, no. 3111/10, ¶ 54
[312] M. Alauzen, "L'Etat plateforme et l'identification numérique des usagers - Le processus de conception de FranceConnect," *Réseaux*, La Découverte, 2019, vol. 2019/1, no. 213, p. 2025
[313] P. Mortier, *Les métamorphoses de la souveraineté*, *op. cit.* note 224, ¶ 15
[314] Making war or peace, controlling currency, etc., J. Bodin, *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie no. 4619, 1993, p. 101

the exclusive domain of the state. However, this listing is a "*very subjective method*."[315] Facing this "*multiplicity of powers*," there is still "*a common point of origin*":[316] the law. Bodin affirms that all marks are "*included under the power of giving the law*."[317] Today, the "*modern Sovereign is foremost a King–Legislator*,"[318] and the sovereign's power will be exercised through the law.[319] In states framed by the rule of law, the ways to ensure obedience to the law are also regulated by it.[320] Similarly, according to Weber, the monopoly of violence entails first being able to decide what is licit and what is not[321] and then using coercion to ensure compliance with the rules.[322] When the monopoly is owned by the state, the coercion rests on a legal legitimacy: The state, "*authorizes acts of coercion by means of prescriptions. In other words, the State is that political form which acts in the legal form*."[323] Later, Kelsen equates legitimacy with legality, as a legal translation of Weber's sociological definition.[324] Coercion might exist

[315] D. Baranger, "The apparition of sovereignty," *in* H. Kalmo, Q. Skinner (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 53. It depends on time, places, and the one writing the list and its objectives, M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020, p. 84. For example, Herzog considers the monopoly of legitimate coercion and the promulgation of law to be part of the state's exclusive competences rather than the definition of its sovereignty. For him, it is similar to controlling the money supply or declaring war, D. Herzog, *Sovereignty, RIP*, Yale University Press, 2020, p. 279

[316] H. Kalmo, Q. Skinner, "Introduction : a concept in fragments," *in* H. Kalmo, Q. Skinner (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 14

[317] J. Bodin, *Les six livres de la République*, *op. cit.* note 314, p. 101. For Bodin, the law is a unilateral norm, produced by an entity that is not the addressee of the text and promulgated without the consent of the subjects of the sovereign, O. Beaud, *La puissance de l'Etat*, *op. cit.* note 222, pp. 69-74. Beaud also considers internal sovereignty as unilateral acts "*which translate a relationship of subordination between the author and the addressee of the norm*," L. Bal, *Le mythe de la souveraineté en droit international*, *op. cit.* note 232, p. 23

[318] O. Beaud, *La puissance de l'Etat*, *op. cit.* note 222, p. 44. Including the creation and suppression of norms depending on the underlying human will, *Ibid.* p. 97; F. Brunet, "La contrainte du droit," *Pouvoirs*, April 27, 2021, vol. N° 177, no. 2, p. 72

[319] O. Beaud, "Le Souverain," *Pouvoirs*, 1993, no. 67, p. 34

[320] M. Foucault et al., *Sécurité, territoire, population: cours au Collège de France, 1977-1978*, Seuil : Gallimard, Hautes études, 2004, p. 102. It is especially true in criminal procedure, where the principles of fair trial and legality are applied.

[321] Conseil d'État (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 2, p. 219, 11è conférence, Denys de Béchillon

[322] J. Chevallier, C. Jacques, *L'État post-moderne*, LGDJ, 4th ed., 2017, pp. 12, 22-23

[323] M. Troper, "Le monopole de la contrainte légitime," *Lignes*, Éditions Hazan, 1995, vol. n° 25, no. 2, p. 43. However, Weber only considers the internal legitimacy, meaning, the respect of the norms set by the system to produce this coercion, B. Mazabraud, "Foucault, le droit et les dispositifs de pouvoir," *Cites*, October 11, 2010, vol. n° 42, no. 2, p. 141. But legal legitimacy also relies on an external perspective: the conformity to general norms or values not set by the system, M. Troper, "Le monopole de la contrainte légitime," p. 38. Foucault argues that those norms coming from outside the legal system come from other "structures of power" that produce norms in different ways. For example, the discipline structure "*consists in setting an optimal model, then developing training and control techniques in order to make human behaviors conform to this model (the normal)*," B. Mazabraud, "Foucault, le droit et les dispositifs de pouvoir," pp. 173-174.

[324] M. Troper, "Le monopole de la contrainte légitime," *op. cit.* note 323, p. 36

outside the state, but the state has the "*exclusive right to prescribe or permit and therefore prohibit violence*."[325] Nevertheless, the production of norms by a single entity, the state, is a fiction. First, inside the state, various institutions produce norms. At the top, constitutional control limits the production of laws, and at the bottom, territorial collectivities can have powers of regulation,[326] and independent administrative and technical entities will produce their own set of rules.[327] Second, the law is influenced by norms from outside the state through international and European laws and jurisprudence, although they indirectly derive from the states. The international community, such as commercial actors and expert groups also produces norms. The classical pyramid of norms limited to the sovereign state is becoming a network connected to various sources of norm production.[328]

326. Coercion in cyberspace. This "*network-like structure*"[329] and "*'liquid' forms of law*"[330] are particularly adapted to cyberspace.[331] Norms come from various states, all equal in their external sovereignty: There cannot be a hierarchical setting. However, the state regulation is not adapted to this global phenomenon.[332] Online, imperfection of information about the user, location, or network use may prevent states from enforcing their coercion.[333] Technologies to lessen anonymity and increase traceability lie in the hands of digital actors.[334] Therefore, applying digital coercion does not depend primarily on state law any longer but on what Lessig calls the code, "*the instructions embedded in the software or hardware that makes cyberspace what it is*."[335] As the

---

[325] *Ibid.* p. 40
[326] M. Van de Kerchove, "Eclatement et recomposition du droit pénal," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000, p. 6
[327] M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique*, Michalon Editions, 2010, p. 64
[328] F. Ost, M. van de Kerchove, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications des facultés universitaires Saint-Louis, 2010, p. 26
[329] R.E. Kostoris, "European Law and Criminal Justice," *in* R.E. Kostoris (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, p. 57
[330] M. Kettemann, *The normative order of the internet*, *op. cit.* note 315, p. 237
[331] B. Barraud, *Le renouvellement des sources du droit - Illustrations en droit de la communication par internet*, Thesis, Université d'Aix Marseille, July 1, 2016, p. 307
[332] D.R. Johnson, D. Post, "Law and Borders - The Rise of Law in Cyberspace," *Stanford Law Review*, May 1996, vol. 48, no. 5, p. 1370. For instance, "*The technology of the medium, the geographical distribution of its users, and the nature of its content all make the Internet specially resistant to state regulation*," J. Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," *University of Cincinnati Law Review*, January 1, 1997, vol. 66, p. 183. Going further, one author argued that "*The nature and logic of the Internet would contradict the nature and logic of the modern law-state*," B. Barraud, *Le renouvellement des sources du droit*, *op. cit.* note 331, p. 9
[333] L. Lessig, *Code*, Basic Books, 2nd ed., 2006, p. 35
[334] *Ibid.* pp. 46-49, 57-58
[335] *Ibid.* p. 121. However, Lessig recognized that the code is not the only source of norms in the cyberspace, and that it also relies on state laws and social norms, L. Lessig, "Reading The Constitution in Cyberspace," *Emory Law Journal*, 1996, vol. 45, no. 3, p. 29

intervention of the state in cyberspace is limited, "*the State as a whole [is] challenged by the Internet*."[336] States and digital actors might be competing for digital coercion,[337] because digital actors define the code, which is difficult to change by producing state law.[338] Digital actors' powers would then be challenged by "*resovereignization of the Internet characterized by a nationalization of oversight over global public policy issues of the Internet, [and] state-led initiatives on sectorial issues*."[339] However, by recognizing the sovereignty of digital actors, this competition is lessened. Instead of attempting, to regulate cyberspace, to no avail, state sovereignty can become "passive sovereignty," creating "*strong interconnections to provide a governance structure*."[340] Subsidiarity, as practiced within the EU, could be applied to these relationships. Digital actors will build norms in the first place, according to the notion of proximity, and states would intervene when the code is insufficient to protect the rule of law. This collaboration is based on collaboration rather than on competition.[341]

327. Nevertheless, the framework for data requests highlights that states attempt to intervene, without success. Thus, digital actors' internal autonomy is exemplified through the prism of data conservation and encryption, two frameworks necessary to efficiently investigate cyber trafficking.

II. Regulation by digital actors due to the incapacity of the states

328. Data conservation and human trafficking. Before data are requested, the question of their conservation is necessary.[342] Data retention or conservation *"means the collection and storage of personal data for an undetermined purpose in the event that it should ever be needed for not-yet specified future use*."[343] Indeed, "*non-state*

---

[336] B. Barraud, *Le renouvellement des sources du droit*, *op. cit.* note 331, p. 587
[337] *Ibid.* p. 590
[338] J.R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology," *Texas Law Review*, 1998, vol. 76, no. 3, p. 582; L. Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review*, The Harvard Law Review Association, 1999, vol. 113, no. 2, pp. 534-535
[339] M. Kettemann, *The normative order of the internet*, *op. cit.* note 315, p. 173
[340] J.A. Lewis, "Sovereignty and the Role of Government in Cyberspace," *The Brown Journal of World Affairs*, Brown Journal of World Affairs, 2010, vol. 16, no. 2, p. 62
[341] J. Chevallier, C. Jacques, *L'État post-moderne*, *op. cit.* note 322, p. 64
[342] On the link between both topics, K. Ligeti, G. Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence: Beyond Mutual Recognition?," *in* R. Kert, A. Lehner (eds.), *Vielfalt des Strafrechts im internationalen Kontext. Festschrift für Frank Höpfel zum 65. Geburtstag*, NWV Verlag, 1st ed., January 19, 2018, p. 643
[343] M. Albers, "Data Retention in Germany," *in* M. Zubik, J. Podkowik, R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, p. 117

actors potentially have access to a gold mine of information,"[344] but this gold mine is useful only if it is conserved. This topic is important in investigating human trafficking.[345] Some digital services used by traffickers are known for the ephemeral availability of data, such as Snapchat,[346] or for temporary content, such as Instagram stories.[347] Thus, data conservation is a core issue.[348] However, data conservation should consider international texts and human rights,[349] particularly trafficked victims.[350] There is a need for "*balance [between] human protection from exploitation and human protection from invasion of privacy*."[351]

329. Data conservation in the EU. In the EU, the principle is the minimization of data conservation.[352] The Directive 2006/24 created an exception, after the 2005 London bombings,[353] by obliging digital actors to retain traffic and location data and

[344] A. Beduschi, "The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law," *Georgetown Journal of International Law*, 2018, vol. 49, no. 3, p. 1015
[345] Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, "Final Report," Committee for Equality between Women and Men, Council of Europe, September 16, 2003, pp. 74-77, EG-S-NT (2002) 9 rev.. The report emphasizes the importance of traffic data in identifying the individuals. One author also highlights the need for a regulation about data storage, especially due to the "*important degree of volatility of digital evidence*," A. Sykiotou, "Cyber trafficking: recruiting victims of human trafficking through the net," *in* N.E. Kourakēs, C.D. Spinellis (eds.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017, p. 1566
[346] J. Stearns, "Street Gangs and Human Trafficking," *in* M. Palmiotto (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 153
[347] B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de mineures – Quelles réalités sociales et juridiques ?*, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020, p. 20
[348] Committee of Ministers, "Recommendation No. R (87) 15 regulating the use of personal data in the police sector," Council of Europe, September 17, 1987, ¶ 3, recommendation that is now "*part of the Schengen acquis*," S. Şandru, "About Data Protection and Data Retention in Romania," *Masaryk University Journal of Law and Technology*, November 29, 2013, vol. 7, no. 2, p. 388
[349] Inter-agency coordination group against trafficking in persons, *Human trafficking and technology: trends, challenges and opportunities*, Issue Brief, no. 7, UN, 2019, p. 5; S. Milivojević, "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, p. 37
[350] Article 11 of the Warsaw Convention
[351] F. Gerry QC, J. Muraszkiewicz, N. Vavoula, "The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns," *Computer Law & Security Review*, April 2016, vol. 32, no. 2, p. 210
[352] Article 5.1.e of the GPDR. In particular, traffic data "*must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication*," Article 6 of the Directive 2002/58
[353] B. Grabowska-Moroz, "Data Retention in the European Union," *in* M. Zubik, J. Podkowik, R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, p. 3

"*data necessary to identify the subscriber*,"[354] for six months to two years.[355] Criticized since its negotiation,[356] this obligation, it was challenged before the CJEU.[357] The 2014 Digital Rights Ireland decision[358] annulled the text, finding that the obligation was disproportionate due to the general personal and data scope, the lack of definition of the material and temporal scopes, and of guarantees regarding access, use, and erasure.[359] However, the court decision was criticized as undermining the capabilities of law enforcement authorities;[360] it recognized the national trends to declare unconstitutional transposing laws, led by Romania, while the French institutions are resisting the annulment.[361] This heterogeneity "*may limit the effectiveness of mutual legal assistance*."[362] For this reason, the code established by digital actors seems to permit preservation orders only.

330. The Romania framework. Classically, "*national courts have no jurisdiction to declare that acts of [the EU] are invalid*."[363] However, in 2009, the Romanian *Curtea Constituţională*[364] was the first European court to declare unconstitutional the

[354] Article 3 of the Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks; E. Kosta, "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection," *SCRIPTed*, October 4, 2013, vol. 10, no. 3, p. 342. Except for content data, Article 5.2

[355] Article 6 of the Directive 2006/24

[356] Cybercrime Programme Office of the Council of Europe, "Data retention in the States Parties to the Budapest Convention on Cybercrime Survey report 2020," Council of Europe, 2020, p. 8

[357] First, on the ground that the directive was not adopted on the correct basis, ECJ, *Ireland v. European Parliament and Council of the European Union*, February 10, 2009, C-301/06. See also B. Grabowska-Moroz, "Data Retention in the European Union," *op. cit.* note 353, pp. 4-5

[358] CJEU, *Digital Rights Ireland*, *op. cit.* note 207

[359] D. Cohen, "Le juge européen et les données personnelles," *in* Collectif (ed.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 260; F. Coudert, F. Verbruggen, "Conservation des données de communications électroniques en Belgique : un juste équilibre ?," *in* V. Franssen, D. Flore, F. Stasiak (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 248

[360] Europol, "Internet organised crime threat assessment," EU, 2019, p. 56; M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 142; Europol, Eurojust, *Common challenges in combating cybercrime*, *op. cit.* note 46, p. 5

[361] No question has arisen for now with the Spanish framework, which won't be studied. The applicable frameworks are the Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones and Article 588 ter j of the Ley de Enjuiciamiento Criminal for access by law enforcement authorities (upon judicial authorization).

[362] M. Quéméner, *Le droit face à la disruption numérique*, *op. cit.* note 360, p. 139

[363] ECJ, *Foto-Frost v. Hauptzollamt Lübeck-Ost*, October 22, 1987, C-314/85, ¶ 20

[364] Curtea Constituţională, *Decizia referitoare la excepţia de neconstituţionalitate a prevederilor Legii nr.298/2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, precum şi pentru modificarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice*, October 8, 2009, no. 1298/2008, p. 200. Considering the history of Romania, after the end of the dictatorship, the country has a strong interest in protecting human rights. Furthermore, as one of the last countries to join the EU, it also has a political interest in supporting European values to ensure, for instance, its entrance into the Schengen area.

transposing law[365] of the 2006 directive. This decision, however, does not refer to the EU framework. It considered "*the very nature of [bulk] data retention as a measure infringing the right to privacy*,"[366] using a general reasoning.[367] Specifically, the court criticized the lack of definitions ("related data," "threats to national security") and the lack of legal safeguards (particularly regarding the access to data), the general personal scope (all the physical and legal persons in their quality as users), and the continuous retention without a specific cause. The government then transposed the 2006 directive for a second time in 2012,[368] and this law was also declared unconstitutional in 2014.[369] The court particularly objected to the broad personal and material scopes regarding offenses,[370] the lack of a definition of "related data,"[371] notification of the affected person,[372] and safeguards regarding access to and use of data.[373] Consequently, the current framework provides for the possibility to request

[365] Lege 298/2008 privind reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, setting a retention obligation of traffic and location data for six months; also called the "*Big Brother law*," S. Şandru, "Data Retention in Romania," *in* M. Zubik, J. Podkowik, R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, p. 192

[366] E. Kosta, "The Way to Luxemburg," *op. cit.* note 354, p. 349. It should be underlined that the Romanian right to privacy not only protects citizens, "*having in mind that the right to privacy has to be ensured to every individual, regardless of the nature of his/her relationship with the Romanian State*," S. Şandru, "About Data Protection and Data Retention in Romania," *op. cit.* note 348, p. 384

[367] Other national courts only declared invalid certain provisions of the transposing laws, E. Kosta, "The Way to Luxemburg," *op. cit.* note 354, p. 359. For instance, the German decisions focus on access and use, K. de Vries et al., *The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)*, CEPS Liberty and Security in Europe, Centre for European Policy Studies, May 2010; and the Belgian court criticized the length of the offenses list that allowed data retention, C. Van de Heyning, "Data Retention in Belgium," *in* M. Zubik, J. Podkowik, R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 53-74. Nor does the CJEU question the idea of data retention, M. Zubik, J. Podkowik, R. Rybski, "Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remarks," *in* M. Zubik, J. Podkowik, R. Rybski (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, p. 238

[368] Lege 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice

[369] See S. Şandru, "Data Retention in Romania," *op. cit.* note 365, p. 199

[370] Curtea Constituţională, *Decizia referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr.82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice și ale art.152 din Codul de procedură penală*, July 8, 2014, no. 440/014, ¶ 49

[371] *Ibid.* ¶ 50

[372] *Ibid.* ¶ 55

[373] *Ibid.* ¶ 57, in particular by intelligence authorities, *Ibid.* ¶ 63

data only from digital actors,[374] who are then responsible for defining their own rules for data retention.

331. Posterior CJEU case laws. After the Digital Rights Ireland decision, the CJEU continued to frame data retention. In particular, the "*revolutionary*"[375] Tele2 2016 decision explicitly prohibits the "*general and indiscriminate retention*" of data,[376] requiring targeted[377] conservations only for serious crimes[378] and access upon authorization by an independent institution.[379] Later, the French legislation was challenged by the CJEU. Regarding the retention of traffic and location data to investigate serious crimes, the court highlighted the need for targeted retention "*on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion*."[380]

332. The French framework. At that time, French law provided for the general conservation of data related to the identification of users, traffic, and location data for the investigation of criminal offenses. [381] After the decision of the CJEU, the *Conseil d'Etat* deemed the regime almost completely valid. It argued that the entire regime was valid because of current (terrorist) threats to national security,[382] except that this

[374] Lege 235/2015 pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, introducing Article 12^1 on access to data by authorities; and Article 152 of the Codul de Procedură Penală, S. Şandru, "Data Retention in Romania," *op. cit.* note 365, p. 200

[375] B. Grabowska-Moroz, "Data Retention in the European Union," *op. cit.* note 353, p. 12

[376] CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen*, December 21, 2016, C-203/15 and C-698/15, ¶ 112. Lately recalled by CJEU, *G.D. v. An Garda Síochána*, *op. cit.* note 17

[377] The technical options for limiting data retention have been criticized for failing to account for reality, B. Grabowska-Moroz, "Data Retention in the European Union," *op. cit.* note 353, p. 13

[378] F. Coudert, F. Verbruggen, "Conservation des données de communications électroniques en Belgique," *op. cit.* note 359, p. 255

[379] F. Molins, "La protection des citoyens européens dans un monde ultra-connecté," *Question d'Europe*, Fondation Robert Schuman, April 8, 2019, no. 510, p. 2

[380] However, such retention does not need to be targeted when considering "*genuine and present or foreseeable*" serious threats to national security, "*where the decision […] is subject to [independent and] effective review*," CJEU, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs v. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées ; and Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministres*, October 6, 2020, C-511/18, C-512/18, C-520/18, ¶ 168. On the contrary, retention of identification data, particularly IP addresses, was deemed unnecessary to limit to serious crimes or targeted individuals, *Ibid.* ¶ 159. Therefore, the court creates a criticized "*retention scale*," J. Sirinelli, "La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite," *Revue trimestrielle de droit européen*, 2021, pp. 316-321

[381] Articles L34-1 and R10-13 of the Code des postes et des communications électroniques (old version); see also Article 6.II of the Loi n° 2004-575 pour la confiance dans l'économie numérique

[382] Conseil d'Etat, *French Data Network et autres*, April 21, 2021, no. 397844, 397851, 393099, 394922, 424717, 424718, ¶ 44. However, the justification resting on a state of emergency that is prolonged is highly criticized in relation to the preservation of the rule of law, J. Chevallier, *L'État de droit*, LGDJ, Clefs, 6th ed., 2017, pp. 85, 141-142

general conservation of data[383] should be limited to the objectives of protecting national security[384] and that the threats should be reassessed on a regular basis.[385] Since targeted retention efforts are not considered efficient by the CJEU, [386] mandatory general conservation is justified by threats to national security. As a result, digital actors must save all data. When some of it would be useful for a criminal investigation, law enforcement authorities can therefore produce a preservation order or a request for data. As a result, the legal reform went further than the *Conseil d'Etat*'s requirements, recognizing that its decision did not conform to CJEU case law. Under the current texts, digital actors must retain data linked to the identity of users for up to five years after the end of the contract, and all other information and transaction data for up to one year after the contract's end.[387] For transmission to law enforcement authorities who are investigating serious offenses, digital agents must retain for one year "*technical data to identify the source of the connection or data relating to the terminal equipment used*."[388] However, even this reform does not conform to the CJEU decision, particularly since it does not consider the notion of "serious offenses." Therefore, further interpretations will be needed.[389]

333. From conservation to preservation. Data conservation rests in the hands of digital actors, due to the invalidation of the EU framework and national ones and the instability of those still existing. Even in France, the law seems to be a legal consecration only of the data already conserved by digital actors, that are essential to

[383] Except for the conservation of IP addresses, that can be allowed for a certain time for the objective of investigating any offenses, Conseil d'Etat, *French Data Network et autres*, *op. cit.* note 382, ¶¶ 39-40; or for an indefinite time when considering the objective of national security, *Ibid.* ¶ 35
[384] Conseil d'Etat, *French Data Network et autres*, *op. cit.* note 382, ¶¶ 59-60
[385] *Ibid.* ¶ 46
[386] From a public law perspective, various authors argue that this decision is another example of the resistance of the Conseil d'Etat against EU law, J. Teyssedre, "Le droit de l'Union européenne de la protection des données dans le prétoire du Conseil d'État : quels enjeux ?," *Revue trimestrielle de droit européen*, 2021, p. 334; J. Sirinelli, "La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite," *op. cit.* note 380, p. 313; M.-C. de Montecler, "Conservation des données : la guerre des juges n'aura pas lieu," *Dalloz Actualité*, Dalloz, April 26, 2021; L. Azoulai, D. Ritleng, "« L'État, c'est moi ». Le Conseil d'État, la sécurité et la conservation des données," *Revue trimestrielle de droit européen*, 2021, pp. 351-358. The lack of reference to fundamental rights was also criticized, *Ibid.* p. 360
[387] Article L34-1.II bis.1° and 2° of the Code des postes et des communications électroniques; the data to be conserved is detailed at Article R-10.13.
[388] Article L34-1.II bis.3° of the Code des postes et des communications électroniques. Finally, when considering a serious threat against national security, the prime minister can mandate digital actors to conserve traffic and location data for one year, Article L34-1.III; injunction produced by the Décret n° 2021-1363
[389] L. Azoulai, D. Ritleng, "« L'État, c'est moi »," *op. cit.* note 386, p. 359

the survival of their economic model.[390] In that sense, the technical code regulating data "*can be subsequently used both for commercial purposes and as a result of requests and fishing operations or data mining by law enforcement authorities or national security services*."[391] As a result, to ensure data availability, law enforcement officials can request data preservation (or "rapid conservation"), which means protecting previously retained data from "*anything that would cause its current quality or condition to change or deteriorate*."[392] This framework "*avoid[s] the blanket intrusion into privacy of population-wide data retention laws*,"[393] while recognizing that conservation is handled by digital actors.[394] National and international preservation orders have been harmonized by the Budapest Convention,[395] although they seem to be of limited application, especially at the international level, because of the need to rely on the complex system of mutual assistance.[396]

334. Even when law enforcement authorities can request retained data from digital actors to investigate cyber trafficking, these data might be encrypted, which highlights a different perspective on digital actors' internal sovereignty.

III. Regulation by digital actors in the absence of the states

335. "Janus-faced"[397] encryption. The cryptography discipline aims to modify data "*to hide [their] information content, establish [their] authenticity, prevent [their] undetected modification, prevent [their] repudiation, or prevent [their] unauthorized*

[390] K. Douplitzky, "Le commerce du moi, modèle économique du profilage," *Hermes, La Revue*, C.N.R.S. Editions, 2009, vol. 53, no. 1, p. 115
[391] Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines," European advisory body on data protection and privacy, April 4, 2008, p. 7, 00737/EN WP 148
[392] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, *op. cit.* note 141, ¶ 151
[393] I. Brown, "Communications Data Retention in an Evolving Internet," *International Journal of Law and Information Technology*, July 5, 2010, vol. 19, no. 2, p. 106
[394] It is very clear in the E-evidence regulation: prior erasure of data is a reason for non-execution, Article 10.7
[395] Articles 16 and 29 of the Budapest Convention. See also Article 588 octies of the Ley de Enjuiciamiento Criminal regarding a preservation order of 90 days produced by the prosecutor or police officer without any limitation in the kind of preserved data; Article 154 of the Codul de Procedură Penală, regarding a preservation order of 60 days produced by the prosecutor without any limitation in the kind of preserved data; Articles 60-2¶2, 77-1-2¶2 and 99-4¶2, regarding a preservation order of 1 year upon authorization of the judge of liberties and custody or the judge of instruction, but this regime is limited to preservation of the "*content of the information consulted by the users*."
[396] Cybercrime Convention Committee, "Assessment Report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime," Council of Europe, January 25, 2013, pp. 10, 18, 28-29, 44, T-CY (2012)10 REV
[397] L. Lessig, *Code*, *op. cit.* note 333, p. 53

use."[398] In particular, encryption is designed to "*produce unintelligible data (encrypted data) to ensure [their] confidentiality*":[399] Any person without knowledge of or access to the encryption key will be unable to read the data. Obtaining the data without this key requires decoding, or cracking the encryption. This discipline supports "good" objectives, such as the confidentiality of communications; it allows trust in cyberspace and the protection of fundamental rights.[400] Thus, "*encryption is an essential element of our digitalized democracies*,"[401] linked to data sovereignty.[402] However, encryption lies mainly in the hands of digital actors, due to a current general lack of regulation.[403] Nonetheless, encryption can also serve criminal uses.[404]

336. Misuse of encryption: human trafficking. Increasingly, the efficiency of digital investigative techniques is questioned due to the criminal use of encryption,[405] by traffickers in particular.[406] In 2021, the UNODC called for better partnerships with

[398] OECD, "Recommendation of the Council concerning Guidelines for Cryptography Policy," OECD, 2020, p. 3, OECD/LEGAL/0289
[399] *Ibid.* p. 9
[400] L. Lessig, *Code*, *op. cit.* note 333, p. 54; OECD, *Recommendation of the Council concerning Guidelines for Cryptography Policy*, *op. cit.* note 398, p. 5; European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025," EU, April 14, 2021, p. 26, COM(2021) 170 final. It can, for instance, enhance medical secrecy or protect whistleblowers' data (as well as the privacy of every person), E. Netter, *Numérique et grandes notions du droit privé*, Thesis, Université de Picardie - Jules Verne, November 20, 2017, ¶ 85
[401] Europol, Eurojust, *Common challenges in combating cybercrime*, *op. cit.* note 46, p. 10
[402] P. Bellanger, "Les données personnelles : une question de souveraineté," *Le débat*, Gallimard, 2015, vol. 2015/1, no. 183, pp. 21-22
[403] Indeed, cryptography was limited to states' military and diplomacy domains until the 1990s, C. Féral-Schuhl, *Cyberdroit: le droit à l'épreuve de l'Internet*, Praxis Dalloz, Dalloz, 2020, pp. 1193-1195. During the cold war, cryptography was regarded as a war weapon, and its import and exportation were strictly controlled, I. Roujou De Boubée, "Cryptographie : ses nécessités, ses dérives," *in* M.-C. Piatti (ed.), *Les libertés individuelles à l'épreuve des nouvelles technologies de l'information*, Presses universitaires de Lyon, 2001, p. 125. On the contrary, the law in France also restricted the use of encryption, *Ibid.* p. 137. See Article 28 of the Loi n° 90-1170 sur la réglementation des télécommunications (1990 version). Later on, a special regime was created to entrust encryption keys to a third party, see Article 28 of the Loi n° 90-1170 (1996 version). However, due to a lack of technical efficiency, the regime was finally completely suppressed in 2004, establishing the entire free use of encryption, Conseil d'Etat, *Etude - Internet et les réseaux numériques*, *op. cit.* note 133, p. 69, Articles 30.I and 40 of the Loi n° 2004-575 pour la confiance dans l'économie numérique.
[404] E. Netter, *Numérique et grandes notions du droit privé*, *op. cit.* note 400, ¶ 40
[405] Europol, Eurojust, *Common challenges in combating cybercrime*, *op. cit.* note 46, pp. 10, 13; OECD, *Recommendation of the Council concerning Guidelines for Cryptography Policy*, *op. cit.* note 398, p. 6; K. Ligeti, G. Robinson, "Enhanced cooperation in criminal matters," *op. cit.* note 342, p. 628. This challenge has been underlined since 1995 by the Council of Europe, Committee of Ministers, "Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology," Council of Europe, September 11, 1995, ¶ 14 (annex). However, metadata is usually not encrypted, which could be important for law enforcement authorities, S. Woolley, J. Gursky, *Countering disinformation and protecting democratic communication on encrypted messaging applications*, Brookings institution, June 11, 2021, p. 1
[406] GRETA, *Online and technology-facilitated trafficking in human beings. Full report*, *op. cit.* note 61, pp. 44-46

private actors on that topic to investigate human trafficking,[407] although it had been mentioned since 2003.[408] Today, encryption is embedded in many services used by everyday people as well as traffickers and victims. Specific examples are provided with not-so-well-known applications such as Loki or Wickr,[409] but most common tools of communication are now encrypted, such as WhatsApp. This, therefore poses a challenge for the investigation of cyber trafficking.[410] However, the law should neither prohibit nor weaken encryption as a tool useful for the rule of law, while strengthening the powers of law enforcement authorities to support efficient investigations.[411]

337. **Bypassing encryption.** The first solution is to bypass encryption, by finding another way to access the intelligible data.[412] Through the use of legal hacking, a password, or direct participation directly in the communication through cyber-infiltration, encryption is no longer a challenge. Due to the limitations of these techniques, law enforcement authorities can also require the "*access key to be handed*

[407] UNODC, *Global report on trafficking in persons 2020*, UN, January 2021, p. 19. Europol is also calling for more training on encryption to achieve the same goal, Europol, "Intelligence Notification 15/2014 Trafficking in human beings and the internet," EU, October 2014, p. 3

[408] Although the broadness of encryption tools was questioned, Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation, *Final Report*, *op. cit.* note 345, pp. 63, 71-72

[409] J. van Rij, R. McAlister, "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1694

[410] UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," Austria Center Vienna, UNODC, UN, February 2008, p. 4; I. Chatzis, "Traite, esclavage et travail forcé au XXIe siècle : un état des lieux," *Diplomatie*, December 2020, no. 106, p. 44, and in particular for online sexual exploitation of children that might be connected to human trafficking offenses, see Department of State, "Trafficking in persons report," US, June 2017, p. 32; Europol, "Internet organised crime threat assessment," EU, 2021, p. 26

[411] E. Netter, *Numérique et grandes notions du droit privé*, *op. cit.* note 400, ¶ 86

[412] F. Tréguer, "Anonymat et chiffrement, composantes essentielles de la liberté de communication," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 321

over,"[413] as in the French[414] or Spanish[415] laws. However, the current state of the law does not include requests to digital actors to decrypt the data. However, those who use encryption may not be the ones who built it and, thus, they lack the knowledge to decrypt it.[416] Additionally, end-to-end encryption, now "*a standard security feature for many communication channels*,"[417] encrypts the data before it they leave their origin and decrypts them after they arrive at their destination.[418] Simply put, even the digital actor transmitting the data cannot access its intelligible version and does not have access to the encryption key. The actor may code the technique, but its functioning is autonomous.

338. Cracking encryption. Another solution arises: cracking encryption. The French law allows any person to request technical operations to obtain clear data, including by cracking encryption, or state the means protected by national defense secrecy when the offense is punishable by at least two years or more of imprisonment,

[413] Remote searches are especially mentioned in countries without specific encryption legislation, such as Spain and Romania, Europol, Eurojust, "Second report of the observatory function on encryption - Joint report," EU, 2020, p. 12

[414] The French legislator created a particular offense in 2001, to sanction the lack of transmission upon request of a known encryption key used for criminal purposes, Article 434-15-2 of the Code pénal, introduced by the Loi n° 2001-1062 relative à la sécurité quotidienne (sanction of up to three years of imprisonment and a fine of up to 270,000 €). The same law introduced another obligation for those offering encryption: to hand over the keys to law enforcement authorities, subject to a lesser sanction. However, such provision was repealed a few years later (Article 11-1 of the Loi n°91-646 relative au secret des correspondances émises par la voie des communications électroniques, repealed by the Ordonnance n° 2012-351 relative à la partie législative du code de la sécurité intérieure). This provision was deemed valid even when requesting the key from the suspect, Conseil constitutionnel, *M. Malek B. [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]*, March 30, 2018, 2018-696 QPC; and was extended to the transmission of the unlocking code of a phone, Cour de Cassation, Chambre criminelle, October 13, 2020, no. 20-80150; A. Lepage, "Un an de droit pénal du numérique (Octobre 2019 – Octobre 2020)," *Droit pénal*, LexisNexis, December 2012, no. 12, ¶¶ 8-10; Cour de Cassation, Assemblée plénière, November 7, 2022, no. 21-83146; R. Ollard, "Un an de droit pénal du numérique (Octobre 2021 – Octobre 2022)," *Droit pénal*, LexisNexis, December 2022, no. 12, ¶ 6; J.-Y. Maréchal, "Le refus de communiquer le code de déverrouillage d'un téléphone portable utilisé pour commettre une infraction peut constituer un délit," *La Semaine Juridique Edition Générale*, LexisNexis, November 14, 2022, no. 45, p. 1258; Cour de cassation, Chambre criminelle, October 12, 2022, no. 21-81648; P. Conte, "Refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie. Notion de réquisition," *Droit pénal*, LexisNexis, January 1, 2023, no. 1, p. 31

[415] An encryption key could fit in the concept of Article 588 sexies c.5 of the Ley de Enjuiciamiento Criminal, which offers the possibility of transmitting a code of access. Differently from the French framework, this order cannot be directed at certain persons, for instance, the suspected person. In cases of lack of cooperation, an offense of disobedience is committed, Article 556 of the Código penal

[416] M. Quéméner, *Le droit face à la disruption numérique*, *op. cit.* note 360, p. 146

[417] Europol, "European Union serious and organised crime threat assessment - A corrupting influence," EU, 2021, p. 33. For example, it is used by "*Signal, Telegram, and WhatsApp*," S. Woolley, J. Gursky, *Countering disinformation and protecting democratic communication on encrypted messaging applications*, *op. cit.* note 405, p. 1

[418] Contrary to point-to-point encryption, E. Netter, *Numérique et grandes notions du droit privé*, *op. cit.* note 400, ¶ 85

which includes human trafficking.[419] Nevertheless, this framework is quite weak,[420] leaving a wide range of flexibility for the organ authorizing it, which might be a prosecutor. This has been highlighted in the Encrochat case. This company offered modified phones with increased anonymity and encryption, which were mainly used for criminal activity.[421] As the servers were in France, the *gendarmerie* began to investigate and managed to crack the encryption to obtain all communications worldwide.[422] The data were shared at the EU level, and the "*information has already been relevant in a large number of ongoing criminal investigations*,"[423] in up to 13 countries.[424] However, nullity procedures are multiplying. The technique was authorized by the judge of liberties and custody, but it collected data were collected in a generalized and indiscriminate manner. In France, the case law considered that the technique conforms to the constitutional framework[425] without considering the

[419] Article 230-1¶1 and 3 of the Code de procédure pénale

[420] F. Vadillo, "Techniques d'enquête numérique judiciaire," *op. cit.* note 217, p. 61

[421] Europol, "Internet organised crime threat assessment," EU, 2020, p. 21. Although one article mentioned data linked to human trafficking, J. Follorou, "Piratage d'EncroChat : les recours se multiplient contre la justice française," *Le Monde.fr*, March 10, 2021, online https://www.lemonde.fr/societe/article/2021/03/10/piratage-d-encrochat-les-recours-se-multiplient-contre-la-justice-francaise_6072569_3224.html (retrieved on April 29, 2021), the official press release and following procedures mainly mention drug trafficking and money laundering, Eurojust, Europol, "Communiqué de presse - Le démantèlement d'un réseau crypté crée une onde de choc au sein des groupes criminels organisés à travers l'Europe," EU, June 2, 2020; F. Rubio Moreno, "Caso EncroChat y la prueba resultante de las intervenciones masivas de comunicaciones encriptadas en procesos penales extranjeros," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2021, no. 153, p. 9

[422] Eurojust, "Annual report 2020 - Criminal justice across borders," EU, 2021, p. 29

[423] Europol, *IOCTA 2020*, *op. cit.* note 421, p. 21

[424] Eurojust, *Annual report 2020*, *op. cit.* note 422, p. 29

[425] However, the complaint was limited to the tools' protection by national defense secrecy, which was challenged by the right to a fair trial, R. Binsard et al., "Secret-défense : la raison d'État et le droit," *Dalloz Actualité*, October 6, 2021; Conseil constitutionnel, *M. Saïd Z.*, April 8, 2022, 2022-987 QPC. The use of tools protected by national defense secrecy has been criticized in the literature as well, A. Mornet, *Les fichiers pénaux de l'Union européenne : Contribution à l'étude de la protection des données à caractère personnel*, Thesis, Université Toulouse 1, December 4, 2020, ¶ 299. The Cour de cassation neither ruled on the proportionality of the measure, Cour de Cassation, Chambre criminelle, October 11, 2022, no. 21-85148. Thus, there is still space for further interpretation by the French Supreme Court, X. Laurent, "Captation de données numériques : une étape significative dans la consolidation du régime de l'article 706-102-1 du code de procédure pénale," *Dalloz IP/IT*, Dalloz, 2022, p. 578. It will be interesting to see what decisions other European countries made based on those data, C. Ascione Le Dréau, "QPC dans l'affaire EncroChat : des jours heureux pour Big Brother ? Décision rendue par Conseil constitutionnel," *Actualité juridique Pénal*, Dalloz, 2022, p. 376. Up until now, in the United Kingdom, the evidence has been admitted by courts, C. Griffiths, A. Jackson, "Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat: R v A, B, D & C [2021] EWCA Crim 128," *Journal of Criminal Law*, 2022, vol. 86, no. 4, pp. 271-276. Two supranational complaints are pending, CJEU, *Staatsanwaltschaft Berlin [Encrochat]*, pending, C-670/22; ECHR, *A.L. and E.J. v. France [Encrochat]*, pending, 44715/20 and 47930/21. For an analysis through the Spanish perspective, see F. Rubio Moreno, "Caso EncroChat y la prueba resultante de las intervenciones masivas de comunicaciones encriptadas en procesos penales extranjeros," *op. cit.* note 421, p. 9; A. Peralta Gutiérrez, F.J. Parra Iglesias, "Incorporación de prueba penal obtenida en proceso judicial extranjero: casos EncroChat y Sky ECC," *La ley penal: revista*

European case law on data protection. However, the EU does not regulate encryption, which is almost never questioned,[426] although it recognizes the need for "*collaboration between authorities, service providers and other industry partners*."[427]

339. Encryption and heterotopia. In the end, encryption creates what Foucault calls a "heterotopia": a physical—in that case, digital—location of utopia.[428] State sovereignty is challenged by the new sovereignty of digital actors, who define code, as their exclusive form of regulation and materialization of digital coercion. Their code also creates autonomous places, or heterotopias,[429] built but not controlled by digital actors. This could be the birth of a real (digital rather than physical) utopia of total controller absence until states and digital actors agree to debate encryption regulation.[430] To summarize, "*The ability to control is hampered or facilitated by technology, that is, by the extent to which we do or do not have technological capacity, and by the inherent characteristics of that technology*."[431]

340. Conclusion of the section. Through external sovereignty, states negotiated international law to improve criminal investigations while reasserting their independence. Nevertheless, these new texts rely on the cooperation of digital actors to obtain digital evidence. This situation highlights an autonomous role recognized for digital actors as a new step towards mutual recognition, although it questions mutual trust with private actors to protect human rights. Through their internal sovereignty, states define their legitimate coercion by law. However, certain questions do not rest

---

de derecho penal, procesal y penitenciario, Wolters Kluwer, 2021, no. 149, p. 3; on the Dutch framework in particular see G. Sagittae, "On the lawfulness of the EncroChat and Sky ECC-operations," *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 14, 2023, p. 20322844231159576; on the German framework, see M. Nicolas-Gréciano, C.-F. Stuckenberg, "Chronique de droit pénal constitutionnel allemand," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 669

[426] Council of the EU, "Resolution on Encryption - Security through encryption and security despite encryption," EU, November 24, 2020, p. 5, 13084/1/20 REV 1. Nevertheless, the EU is funding a "*Europol's new decryption facility*," European Commission, *EU Strategy to tackle Organised Crime 2021-2025*, *op. cit.* note 400, p. 26; European Commission, "Communication To The European Parliament, The European Council And The Council - Eleventh progress report towards an effective and genuine Security Union," EU, October 18, 2017, p. 9, COM(2017) 608 final. See also J. Alonso Lecuit, "El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea," *Análisis del Real Instituto Elcano*, Real Instituto Elcano de Estudios Internacionales y Estratégicos, 2021, no. 4, p. 1.

[427] European Commission, *Eleventh progress report towards an effective and genuine Security Union*, *op. cit.* note 426, p. 10

[428] M. Foucault, "Des espaces autres. Hétérotopies. Conférence au Cercle d'études architecturales," *Architecture, Mouvement, Continuité*, 1984, no. 5, pp. 46-49

[429] T. Christakis, *"European Digital Sovereignty," op. cit.* note 202, p. 62

[430] Conseil d'État (ed.), *Droit comparé et territorialité du droit*, *op. cit.* note 321, p. 161 (tenth conference by Antoine Garapon)

[431] J. Black, "Critical Reflection on Regulation," *Australian Journal of Legal Philosophy*, January 1, 2002, vol. 27, p. 14

any longer on their capacities but on how digital actors code cyberspace. States want to rule over coders, but their legal authority is constrained by fundamental rights. While data conservation and encryption are the most difficult aspects of obtaining digital evidence to investigate human trafficking, these matters are primarily in the hands of the digital actors. To maintain their sovereignty over technologies, states either bypass the problem through data preservation or eliminate the problem through encryption cracking. These strategies demonstrate that cooperation is still in the works by implicitly allowing digital actors who exercise sovereignty to clash with traditional owners of sovereignty.

341. Conclusion of the chapter. The legal frameworks highlight a long road of investigations into how to effectively collaborate with digital actors to improve investigations into cyber human trafficking and cybercrime in general. National approaches are limited by their territory, although new interpretations link digital actors to a state. However, these multiple new criteria favor potential conflicts of law and challenges the protection of human rights. Supranational frameworks for mutual legal assistance solve these issues, but they were drafted at a time when the request for data as digital evidence was not at the core of investigations, much less when prosecuting human trafficking. The offense of human trafficking was not even defined in 1959, when the first convention on mutual assistance on criminal matters was published. Furthermore, classical assistance rests on the cooperation of three actors: two states and a digital actor, which slows the process. As voluntary cooperation was developed to address these limitations, cooperation was neither ensured nor legally secured regarding the values of the rule of law. Accordingly, new reforms sought to consider the specific characteristics of cyberspace and the role of digital actors to rule over it, or at least to shape its functioning. The increased autonomy of digital actors from their country of origin is at the core of the Second Additional Protocol of the Budapest Convention and of the new European Production Order. Previously, digital actors were the final answerer of an international request; now, they are the direct addresses of new orders, and they contribute to framing its procedure. Digital Therefore, digital actors thus develop their own type of external sovereignty. Additionally, the lack of state regulation in certain areas linked to data requests highlights the implicit internal sovereignty of digital actors. These are increasingly defining the standards for data retention and encryption. The state faces a quasi-

impossibility to broadly regulate data retention due to the protection of human rights, while digital actors can establish their own contractual and technical norms. The state allows encryption go unregulated, favoring innovation but creating more obstacles to the implementation of digital coercion powers. Consequently, digital actors are at the core of its technical regulation. Today, all of these topics are central to the fight against cyber trafficking: The phenomenon provides a particular example of the extension of sovereign powers to digital actors, which must be recognized to ensure efficient cooperation for repression of this crime.

342. Conclusion of the title. The sovereign state is at the core of the repression of human trafficking, which is facilitated by new technologies. Yet, this study of the digital legitimate coercion of the state, offering numerous tools to investigate and prosecute the phenomenon, has to consider a wider scope. In particular, the state's legislation is framed by supranational frameworks, for instance, to protect human rights. It is also framed by pragmatic details linked to the specificities of cyberspace and the implementation of digital investigative techniques. By opening the closed system of state law, a different reality is pictured. Although the sovereign state offers extended powers of coercion, those powers face challenges and obstacles. Instead of questioning the reality of a state's sovereignty, it highlights the need to consider the state in its interactions with other entities. Thus, in particular to repress human cyber trafficking, the state's sovereign powers need to be complemented by the actions of other entities. In particular, digital actors rise as core partners to improve the efficiency of investigations against trafficking. As this division of powers is increasingly recognized by the state, its national legislation provides a framework for cooperation to obtain data from digital actors. Yet, states still face the limits of their own borders while the main digital actors are established globally. As new forms of cooperation are developed to improve the repression of offenses including trafficking, these new texts tend to put at their core a direct relationship between states and digital actors, especially since those frame the technical rules over cyberspace. They rise as addresses of supranational direct obligations, and they lead the regulation on data retention and encryption. Through their specific place in the international community, digital actors highlight a new type of external sovereignty; through setting original rules in the absence of state law, they offer a new type of internal sovereignty. Yet, states are not ready to fully accept new sovereigns. Different strategies are being developed to reassert control over them or to order this cohabitation between multiple sovereign entities.

343. Preliminary conclusion. When human trafficking evolves as a result of new technologies, its repression must search for new coercive means other than these classically exercised by the sovereign state. Today, some of these rest in the hands of digital actors. Increasingly recognized as core partners of the state in this fight, they hold sovereign powers of coercion. Qualifying digital actors as sovereign actors is highly disruptive for traditional legal theorists, who frame their studies on the basis of the state unit. However, part of the literature has been calling for the recognition of private entities' powers. In particular, digital actors were qualified as "*emergent Transnational Sovereigns […] actively participating in the ongoing construction of new transnational institutions and relationships*"[1] through their "*normative and practical authority*."[2] Outside the realm of law, the literature recognized the "*near-absolute sovereignty of corporate rulers*."[3] They are said to "*operate a kind of private sovereignty in cyberspace*."[4] Nevertheless, cyberspace is not disconnected from the physical world, which has been highlighted in studying cyber trafficking. Although the process is facilitated by online services and even when exploitation is developed online, the offense has material consequences for the victims, who server human rights violations, the traffickers, who gain profits, and the state, which face a reduced control over its material elements. Instead of supporting a "*post-sovereignty*"[5] perspective, sovereignty could be disconnected from the theory of the state to highlight entities with the powers to frame and apply coercion. The investigation and prosecution of cyber trafficking underline an emergency to recognize the material powers of digital actors to improve their cooperation with states. However, the existence of various holders of sovereignty is unusual for the traditional legal framework and for state strategies. As a result, it creates tensions when ordering powers among sovereigns.[6] This ordering remains central to ensuring an effective repression of cyber human trafficking.

---

[1] J.E. Cohen, "Law for the Platform Economy," *University of California, Davis Law Review*, 2017, vol. 51, p. 199

[2] J.E. Cohen, *Between truth and power: the legal constructions of informational capitalism*, Oxford University Press, 2019, p. 137. In the end, they "*behave as sovereign*," J. Pohle, T. Thiel, "Digital Sovereignty," *in* B. Herlo (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, p. 54

[3] F. Pasquale, "Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power," *Theoretical Inquiries in Law*, January 1, 2016, vol. 17, p. 512

[4] R. MacKinnon, *Consent of the Networked. The worldwide struggle for internet freedom*, Basic Books, 2017, p. 182

[5] B. Badie, "D'une souveraineté fictive à une post-souveraineté incertaine," *Studia Diplomatica*, Egmont Institute, 2000, vol. 53, no. 5, pp. 5-13

[6] *Ibid.* p. 12

PART 2. CYBER TRAFFICKING AND SOVEREIGNTY: ORDERING COERCION

344. The need to adapt repression of cyber human trafficking highlights the rise of various sovereign entities due to their many sources of coercion powers. Among traditional sovereign states, the ordering of their independence and their powers of coercion is established by public and private international law. Since digital actors are not fully acknowledged as sovereigns, the exercise of their coercive powers questions their ordering with the states' coercion. In particular, to repress cyber trafficking, there arises a "*relationship of force but also [...] a search for complementarity between interests and approaches*."[1] Many authors underline the first sort of relationship: force. Indeed, "*States find themselves both disputed and challenged in the exercise of their traditional prerogatives attached to sovereignty*."[2] As already developed, this challenge is explicit in the procurement of evidence against cyber trafficking offenses. Going further, various states mean to reassert their sovereignty against other sovereigns by enforcing their powers of coercion, particularly through the acme of their sovereignty: criminal law. However, in enforcing coercion against digital actors, some states also apply their own policies abroad through digital actors. Thus, this primary relationship of imposing coercion between sovereigns questions the very core of sovereignty (Title 1).[3] As such, to seek a more comprehensive repression of cyber trafficking, other types of relationships have been developed. Cooperation has been incentivized, particularly through the EU. New standards have been developed, both to improve the coordination between anti-trafficking actions and the protection of victims and to

---

[1] C. Husson-Rochcongar, "La gouvernance d'Internet et les droits de l'homme," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 50. Also underlining the need to study the relationships between these actors and the articulation between the norms they produce, C. Castets-Renard, V. Ndior, L. Rass-Masson, "Introduction," *in* C. Castets-Renard, V. Ndior, L. Rass-Masson (eds.), *Enjeux internationaux des activités économiques: entre logique territoriale des États et puissance des acteurs privés*, Larcier, Création, information, communication, 2020, pp. 13-14

[2] P. Türk, "Définition et enjeux de la souveraineté numérique," *Cahiers français*, La documentation française, June 2020, no. 415, pp. 18-19; R. Chemain, "La relation juridique des GAFA avec l'Union européenne," *Revue de l'Union européenne*, Dalloz, 2023, no. 665, p. 90

[3] It has to be highlighted that these initiatives for coercion of digital actors were limited to their facilitation of human trafficking for sexual exploitation, therefore underlining both a limit of the strategies of states regarding the repression of human trafficking and resulting in a limit to this part of the study.

embed rule-of-law principles in the interactions between sovereigns and people (Title 2). To order sovereigns, in these various types of relationships, the law is highlighted as a "*supplement*" to the real: It "*intervenes in a secondary manner, as if to 'second' the social*," yet this "*secondarity is active and creative, not only receptive*."[4]

[4] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016, pp. 122-136

TITLE 1. ENFORCING COERCION UPON SOVEREIGNS TO REPRESS CYBER TRAFFICKING

345. In repressing cyber human trafficking, the first type of relationship developed among sovereignty holders to order their powers of coercion was based on coercion itself. Despite the recognition of various sources of coercion and the requirement of independence among sovereignty holders, some sovereigns aimed for control of one another. In particular, the fight against cyber human trafficking offers examples of these attempts to exercise coercion upon sovereigns. First, traditional sovereigns–states–denied the role of digital actors in prosecuting traffickers and protecting victims. On the contrary, some states, especially the United States and France, have aimed at the prosecution and conviction of digital actors themselves as facilitators of cyber trafficking processes. Such a strategy, reinforced by legal amendments, seeks to trigger digital actors' criminal liability. These policies were further extended outside of the realm of law when they did not achieve the expected goals, and this led to reducing digital actors' independence by framing their sovereignty through states' control (Chapter 1). However, the process of increasingly linking digital actors' coercion to states' policies derived from the globally establishment of specific national policies. The fight against human trafficking, although harmonized at the international level, is still mainly a matter of national regulation and, thus, of the sovereignty of states. Even so, this regulatory independence is threatened if foreign policies are embedded in digital actors or new technologies. Thus, the independence of sovereign states is also questioned (Chapter 2).

Chapter 1. Imposing states' coercion through hard sovereignty

346. Corporations, sovereignty, and trafficking. States cannot deny the powers of coercion of digital actors, who are the new sovereigns. To maintain their own sovereignty, states aim to control digital actors through criminal law, the acme of coercion[1] that otherwise is known as "hard" sovereignty.[2] Making corporations liable for their involvement in a trafficking process is part of the anti-trafficking global strategy, and anti-trafficking treaties highlight the need to look for corporate liability.[3] Regarding cyber trafficking, states can implement two situations. On the one hand, a digital actor or company or a technological tool can be created for the purpose of trafficking, for instance, the creation of a website for a fake employment agency.[4] On the other hand, digital actors might be used by traffickers to facilitate their crimes. Depending on the reaction, or lack thereof, of digital actors, they might be seen as liable. Various companies have been prosecuted in the United States for websites hosting classified advertisements of victims, including minors, of sexual exploitation; these have been mainly Craigslist and Backpage. In France, a similar case was investigated on the advertisement website Vivastreet.[5] These prosecutions led to the closure or suspension of the targeted sections or the entire website.

347. While states' hard sovereignty is the pinnacle of their powers of coercion,

---

[1] See *supra* 106 to 108.

[2] Also named as a "*governing through crime*" strategy, J. Simon, *Governing through crime: how the war on crime transformed American democracy and created a culture of fear*, Oxford University Press, Studies in crime and public policy, 2007

[3] The Palermo Protocol does not consider corporate liability, S. Schumann, "Corporate Criminal Liability on Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 1659. However, see the Palermo Convention, Article 10, the Warsaw Convention, Article 22 and the Directive 2011/36/EU, Article 5. To protect states' sovereignty, those texts do not impose criminal liability but rather a criminal, administrative, or civil one.

[4] However, prosecutions in such a situation have not been highlighted in the doctrine or by law enforcement authorities.

[5] A similar case was filed in France against Wannonce, AFP, "Le site de petites annonces Wannonce visé par une plainte pour proxénétisme aggravé," *LExpress.fr*, January 27, 2022, online https://www.lexpress.fr/actualites/1/societe/le-site-de-petites-annonces-wannonce-vise-par-une-plainte-pour-proxenetisme-aggrave_2166957.html (retrieved on February 4, 2022). No similar case has been found in Spain. In Romania, an advertisement website (anuntul.ro) was involved in a case of procurement of prostitution (pimping). The ruling only ordered the deletion of the posts during the pretrial stage. There was no prosecution of the website, Curtea de Apel Bucureşti Secţia I Penală, November 5, 2013, no. 11308/302/201; for similar situations, see Curtea de Apel Craiova, Secția penală, April 6, 2015, no. 483/2015 (trafficking in minors and pimping; no prosecution of the website used); Tribunalul Constanţa, October 21, 2015, no. 366/2015 (*idem*).

media, NGOs, and law enforcement authorities have criticized the limits of the law to convict the companies operating these websites for human trafficking and to obtain reparations for victims[6] (Section 1). As a consequence, states have reformed these legal frameworks and have extended their actions to other means of control outside the law, leading to the development of digital actors' powers (Section 2).

Section 1. The limits of hard sovereignty to prove liability for cyber trafficking

348. Two sets of rules should be used to trigger the liability of digital actors facilitating human trafficking. First, the criteria of the criminal framework should be verified, particularly regarding corporate criminal liability and the commission of the offense (§1). Second, digital actors benefit from a specific liability regime for online intermediaries (§2).

§1. States' sovereignty facing corporate criminal liability for cyber-trafficking

349. Introducing corporate criminal liability. Originally, criminal law was not meant to apply to corporations: "*societas delinquere non potest*"[7] ("society cannot be wrong"). The introduction of the concept relied on a new interpretation of the main legal concepts.[8] However, the renewal of criminal liability mainly derived from the evolution

[6] S.C. Pierce, "Turning a Blind Eye: U.S. Corporate Involvement in Modern Day Slavery," *Journal of Gender, Race & Justice*, 2011 2010, vol. 14, no. 2, p. 578

[7] Corporate liability was seen as contradictory to the culpability principle, due to the lack of acts and intent, and to the personality principle, considering that corporations cannot be subjected to sanctions. In particular, by application of the principles of the personality of the offense and of the sanction and the principle "*nullum crimen, nulla peona sine culpa*." Corporations are a legal fiction; they are made of natural persons. As such, they cannot act by themselves to commit an offense, nor do they have the will to do so. See the title of the following article that summarizes this idea: J.C. Coffee Jr., "No Soul to Damn: No Body to Kick: An Unscandalized Inquiry into the Problem of Corporate Punishment," *Michigan Law Review*, 1981, vol. 79, no. 3, pp. 385-459. Nowadays, for some, "*societas delinquere potest*," J.C. Carbonell Mateu, "La persona jurídica como sujeto activo del delito," *in* J. del Vicente Remesal, E. Bacigalupo Zapater, D.-M. Luzón Peña (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, p. 536; J. Vidal, "Fascicule 82-20 : Droit pénal. – Responsabilités," *JurisClasseur Travail Traité*, LexisNexis, July 16, 2021, ¶ 130; while for others, "*societas punire potest*," M. Moreno Hernández, "Algunas reflexiones político-criminales y dogmáticas sobre la responsabilidad penal de las personas jurídicas. ¿Es necesaria una teoría general del delito empresarial?," *in* J.-M. Silva Sánchez, S. Mir Puig (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 156

[8] On personhood, see: W.R. Thomas, "How and Why Corporations Became (and Remain) Persons under the Criminal Law," *Florida State University Law Review*, 2018 2017, vol. 45, no. 2, pp. 479-538. On the material elements of the offense and the intent, see: J.C. Carbonell Mateu, "Responsabilidad penal de las personas jurídicas: reflexiones en torno a su 'dogmática' y al sistema de la reforma de 2010," *Cuadernos de política criminal*, Dykinson, 2010, no. 101, pp. 5-33. On guilt, see: M. Pieth, R.

of society.[9] Corporations increasingly affect people and society, especially when they take advantage of globalization and digitalization.[10] As corporations are considered to be part of legal relationships, they should be liable for potential excesses.[11] Moreover, their fiction and organization can favor the commission of offenses.[12] Considering these new realities, the exclusion of corporate liability cannot be justified any longer by the "*principle of minimum intervention*."[13] Such liability has been deemed a major improvement in repressing criminality, including human trafficking[14] and, in particular, cyber trafficking. Digital actors facilitate the *modus operandi* of traffickers,[15] causing

Ivory, "Emergence and Convergence: Corporate Criminal Liability Principles in Overview," *in* M. Pieth, R. Ivory (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, p. 11

[9] This evolution was supported by supranational organizations, such as the Council of Europe, Committee of Ministers, "Recommendation No. R (88) 18 Concerning Liability of Enterprises Having Legal Personality for Offences Committed in the Exercise of their Activities," Council of Europe, October 20, 1988, p. 18, and the EU, M.-E. Morin, *Le système pénal de l'Union européenne*, Thesis, Université d'Aix-Marseille, November 28, 2017, ¶ 580.

[10] R. Roso Cañadillas, "Prevención: responsabilidad social y penal de las personas jurídicas," *Revista General de Derecho Penal*, Iustel, 2020, no. 33, pp. 9-10; J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal: parte general*, 2021, p. 378

[11] J.G. Fernández Teruelo, "Regulación vigente. Exigencias legales que permiten la atribución de responsabilidad penal a la persona jurídica y estructura de imputación (CP art.31 bis 1,2 inciso 1º y 5)," *in* Á. Juanes Peces (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, ¶ 317

[12] L. Zúñiga Rodríguez, "Tratamiento jurídico penal de las sociedades instrumentales. Entre la criminalidad organizada y la criminalidad empresarial," *in* L. Zúñiga Rodríguez (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, p. 203. Since the mid-20th century, Sutherland has highlighted the role of companies within white-collar crimes and organized crime: It is considered that 80% of economic crimes are committed through corporations, J.C. Carbonell Mateu, "Responsabilidad penal de las personas jurídicas," *op. cit.* note 8, p. 7

[13] J.M. Zugaldía Espinar, *La responsabilidad criminal de las personas jurídicas, de los entes sin personalidad y de sus directivos: análisis de los arts. 31 bis y 129 del Código Penal*, Tirant lo Blanch, Collección delitos no. 95, 2013, p. 13; J.L. González Cussac, "El modelo español de responsabilidad penal de las personas jurídicas," *in* J.L. Gómez Colomer, S. Barona Vilar, P. Calderón Cuadrado (eds.), *El derecho procesal español del siglo XX a golpe de tango: Juan Montero Aroca : liber amicorum, en homenaje y para celebrar su LXX cumpleaños*, Tirant lo Blanch, 2012, p. 1019

[14] Corporations can be created or used to hide the offense. There are "*numerous examples of traffickers running bars, restaurants, or sham escort services as a cover for sex trafficking*," I. de Vries, M.A. Jose, A. Farrell, "It's Your Business: The Role of the Private Sector in Human Trafficking," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 748. Companies can deliberately or involuntarily commit human trafficking, especially in high-risk sectors such as the hospitality or agricultural sectors, which are favored by globalization and the relocation of production to countries with fewer labor rights and controls. For instance, in 2022, a former outsourced Facebook content moderator filed a complaint against it in Kenya, considering that his recruitment and conditions of work could be qualified as human trafficking, B. Perrigo, "Meta Accused Of Human Trafficking and Union-Busting in Kenya," *Time*, May 11, 2022, online https://time.com/6175026/facebook-sama-kenya-lawsuit/ (retrieved on May 19, 2022)

[15] Indeed, "*There is a high prevalence of third-party websites involved in human trafficking cases*," M.J. Delateur, "From Craigslist to Backpage.com: Conspiracy as a Strategy to Prosecute Third-Party Websites for Sex Trafficking," *Santa Clara Law Review*, 2016, vol. 56, no. 3, p. 546

more harm to victims.[16] For this reason, corporate liability is based on criminal policy interests.[17] Corporations are prompted to better control their inner organization,[18] supporting the preventive aspect of criminal law.[19] This notion multiplies the possibilities for repairing harm. When cyber trafficking is facilitated by well-known platforms, digital actors are easily identifiable[20] and, in general, are more reachable than individual traffickers.[21]

350. Corporate criminal liability models. Models of corporate criminal liability are usually divided between indirect and direct liability.[22] The former[23] is based on the wrongdoing of a natural person: The legal person is identified in the persons of "*managers, directors, and other employees with certain responsibilities*" (nominalist, identification or fiction theory) or includes "*any of its employees or agents*"[24] (reality theory,[25] vicarious liability model, or *respondeat superior*). Indirect liability is a transferred liability.[26] On the contrary, the direct liability theory[27] "*treats the corporation as the offender*,"[28] under the aggregation theory, "*by treating the collective as capable*

[16] L. Smith, "Shared Hope Statement Regarding FOSTA-SESTA and the Backpage Seizure," *Shared Hope International*, April 11, 2018, online https://sharedhope.org/2018/04/11/statement-regarding-fosta-sesta/ (retrieved on March 6, 2021)
[17] E. Mestre Delgado, "El principio de culpabilidad en la determinación de la responsabilidad penal de las personas jurídicas," *in* J. del Vicente Remesal, E. Bacigalupo Zapater, D.-M. Luzón Peña (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, p. 272
[18] M.J. Jimeno Bulnes, "La responsabilidad penal de las personas jurídicas y los modelos de compliance: un supuesto de anticipación probatoria," *Revista General de Derecho Penal*, Iustel, 2019, no. 32, p. 12; W.R. Thomas, "How and Why Corporations Became (and Remain) Persons," *op. cit.* note 8, p. 488
[19] Corporations are deemed "*the only [or suitable] ones with the necessary resources and knowledge to prevent possible illegal activities generated or committed under their activity*," B. Vernet Perna, "Estrategias de respuesta ante la criminalidad de empresas," *in* J. del Carpio Delgado (ed.), *Criminalidad en un mundo global: criminalidad de empresa, transnacional, organizada y recuperación de activos*, Tirant lo Blanch, Monografías, 2020, p. 34
[20] C. Castets-Renard, "Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet," *Recueil Dalloz*, 2012, p. 827
[21] J.G. Fernández Teruelo, "Regulación vigente," *op. cit.* note 11, ¶ 320. However, bankruptcy can be challenging to prosecute corporations, J. Planitzer, N. Katona, "Criminal Liability of Corporations for Trafficking in Human Beings for Labour Exploitation," *Global Policy*, November 2017, vol. 8, no. 4, p. 508
[22] For a detailed explanation of each category, see J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal*, *op. cit.* note 10, pp. 379-383
[23] Heteroresponsibility theory
[24] S. Rodríguez-López, "Criminal Liability of Legal Persons for Human Trafficking Offences in International and European Law," *Journal of Trafficking and Human Exploitation*, February 14, 2017, vol. 1, no. 1, p. 104
[25] K. Deckert, "Corporate Criminal Liability in France," *in* M. Pieth, R. Ivory (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, p. 152
[26] Based on a connective factor between the actions of a natural person and the legal person, M.J. Jimeno Bulnes, "La responsabilidad penal de las personas jurídicas," *op. cit.* note 18, p. 29
[27] Self-responsibility theory
[28] M. Pieth, R. Ivory, "Emergence and Convergence," *op. cit.* note 8, p. 49

of offending,"[29] or due to a lack of legal culture or business ethics, according to the organization or holistic model.[30]

351. National models. In the United States, the model has been based on the *respondeat superior* tort law doctrine since 1909.[31] It is deemed to be "*the broadest and most encompassing model*."[32] According to the *respondeat superior* doctrine, "*If an employee or agent of the corporation commits an offense […] while acting within the scope and nature of [their] employment, and acting, at least in part, to benefit the corporation, the corporation is criminally liable*."[33] In Europe, the French model is considered one of the most comprehensive in the world,[34] and corporate liability was introduced in 1994.[35] Today, the criminal code establishes an indirect liability model: "*Legal persons […] are criminally liable […] for offenses committed on their behalf by their organs or representatives*."[36] The American framework constitutes the main framework of this study, as it led the debates on corporate liability for cyber trafficking. The French framework constitutes the second model of this study due to one case similar to the American cases and to the questioning around the liability of digital actors for human trafficking. Differently, the Spanish framework relies on a direct liability

[29] *Ibid.* pp. 21-22
[30] S. Rodríguez-López, "Criminal Liability of Legal Persons for Human Trafficking," *op. cit.* note 24, p. 104. Three defects can be considered the fault of the corporation. It can be a fault for ineffective compliance regarding voluntary acts, for reckless behavior, or for a lack of transparency within the compliance system, A. Nieto Martín, "La autoregulación preventiva de la empresa como objeto de la política criminal," *in* J.-M. Silva Sánchez, S. Mir Puig (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 167
[31] US Supreme Court, *New York Central & Hudson River Railroad Co. v. US*, February 23, 1909, 212 U.S. 481
[32] S. Schumann, "Corporate Criminal Liability on Human Trafficking," *op. cit.* note 3, p. 1654; E. Lederman, "Corporate Criminal Liability: The Second Generation," *Stetson Law Review*, 2017 2016, vol. 46, no. 1, p. 72
[33] V.P. Nanda, "Corporate Criminal Liability in the United States: Is a New Approach Warranted?," *in* M. Pieth, R. Ivory (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, p. 65
[34] Yet it still receives high criticism in international evaluations on that topic, OECD, "Mise en oeuvre de la Convention de l'OCDE sur la lutte contre la corruption Rapport de Phase 4 France," OECD, 2021, ¶¶ 298-303
[35] Following the implementation of the Loi n°92-683 du 22 juillet 1992 portant réforme des dispositions générales du Code Pénal
[36] Article 121-2 of the Code Pénal

model[37] introduced in 2010.[38] It is included as a more recent element of comparison.

352. Today, corporate criminal liability is rarely questioned.[39] However, challenges to states' hard sovereignty arise in its application to cyber human trafficking cases.[40] Thus, hard sovereignty extended its reach, both on the criteria linked to the corporation (I), and to the natural persons linked to it (II).

I. Prosecuting corporations for human trafficking: who and why

353. First, determining corporate criminal liability requires determining which types of corporations are liable (A) and why (B).

A. Determining liable corporations

354. Legal personhood and nationality. In anti-trafficking supranational texts, only the EU directive defines corporations;[41] national criminal codes do not define

[37] V. Magro Servet, *Guía práctica sobre responsabilidad penal de empresas y planes de prevención (compliance)*, La Ley, 2017, p. 70; M. Marchena Gómez, "La contribución del magistrado José Manuel Maza a la consolidación de un modelo de autorresponsabilidad penal de las personas jurídicas," *in* Fiscalía General del Estado (ed.), *La responsabilidad penal de las personas jurídicas: homenaje al Excmo. Sr. D. José Manuel Maza Martín*, Ministerio de Justicia, 2018, p. 241. However, the doctrine is still debating the categorization of this framework. Some consider it a mixed model, J.G. Fernández Teruelo, "Regulación vigente," *op. cit.* note 11, ¶ 332. The Public Ministry considers it a vicarious liability, Fiscalía General del Estado, Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, *FIS-C-2016-00001*, January 22, 2016. Even the case law of the Tribunal Supremo is not interpreted in the same way by the doctrine, in particular, see Tribunal Supremo. Sala Segunda, de lo Penal, June 13, 2016, no. 516/2016; Tribunal Supremo. Sala Segunda, de lo Penal, February 29, 2016, no. 154/2016. The current framework rules that "*Legal persons shall be criminally liable: (a) for offenses committed in their name or on their behalf, and for their direct or indirect benefit, by their legal representatives or by those who, acting individually or as members of an organ of the legal person, are authorized to make decisions on behalf of the legal person or hold powers of organization and control within the same. b) offenses committed, in the exercise of corporate activities, on behalf of and for their direct or indirect benefit, by those who, being subject to the authority of the individuals mentioned in the preceding paragraph, have been able to carry out the acts because of a serious breach by the former of their duties of supervision, oversight, and control of their activity in view of the specific circumstances of the case*," Article 31 bis of the Código Penal. In both cases, the legal person is exempt from liability if the due compliance processes were implemented, highlighting the focus of the regime on a holistic approach.

[38] Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

[39] L. Gracia Martín, "¿Tiene hoy sentido -y si lo tiene, en qué dirección y con qué alcance- algún debate sobre la posibilidad de penar y sancionar a la persona jurídica?," *in* J.-M. Silva Sánchez, S. Mir Puig (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 125

[40] S. Schumann, "Corporate Criminal Liability on Human Trafficking," *op. cit.* note 3, p. 1664

[41] Defined as "*any entity having legal personality under the applicable law*," Article 5.4 of the Directive 2011/36/EU. Are excluded "*states or public bodies in the exercise of state authority and for public international organizations*." This exception will not be developed here, considering the basic cases of this study on human trafficking are linked to private digital actors.

them.[42] For this reason, one question is linked to the nationality of corporations.[43] This topic is not of interest in the United States,[44] because main digital actors are headquartered there. In France[45] and Spain,[46] foreign corporations can be prosecuted, but its implementation faces challenges. One regards the notification of procedural acts,[47] and the second challenge involves the implementation of sanctions. If a foreign

[42] In France, refer to Articles 1832 and following, in particular Article 1842 of the Code civil; regarding commercial companies, see Articles L210-1 and following of the Code de commerce, in particular Articles L210-6 and L251-4. In Spain, refer to Articles 35 and following of the Código Civil; regarding commercial companies, see Articles 116 and following of the Código de Comercio; see also the Ley de Sociedades de Capital. The Spanish doctrine and case law have come to refuse the acknowledgement of legal personality to shell companies that lack sufficient organizational structure only created to commit offenses, Fiscalía General del Estado, Circular 1/2016, *op. cit.* note 37, p. 14; Fiscalía General del Estado, Circular 1/2011 relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010, *FIS-C-2011-00001*, June 1, 2011, p. 7; Tribunal Supremo. Sala Segunda, de lo Penal, May 20, 1996, no. 274/1996. See B. Vernet Perna, "Estrategias de respuesta ante la criminalidad de empresas," *op. cit.* note 19, p. 39; V. Magro Servet, *Guía práctica*, *op. cit.* note 37, p. 76. In the United States, the author of a human trafficking offense is widely named as "*whoever*," 18 US Code (USC) § 1590 and § 1591. In general, legal persons are those who comply with legal requirements to be constituted. That includes "*corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals*," 1 USC § 1; US Court of Appeals, Ninth Circuit, *US v. Polizzi*, July 18, 1974, 500 F.2d 856

[43] As long as the state is competent regarding its jurisdiction. For instance, the parent company of Vivastreet is based in Jersey, L. Motet, "Vivastreet : les dessous de la prostitution par petites annonces," *Le Monde.fr*, February 2, 2017, online https://www.lemonde.fr/les-decodeurs/article/2017/02/02/vivastreet-les-dessous-de-la-prostitution-par-petites-annonces_5073149_4355770.html (retrieved on May 18, 2022). Extraterritoriality is seen as a main barrier to corporate liability, Z. Muskat-Gorska, "Human Trafficking and Forced Labour: Mapping Corporate Liability," *in* P. Kotiswaran (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, p. 449

[44] The United States considers the criminal liability of foreign corporations, although not in particular for human trafficking, but especially for corruption (Foreign Corrupt Practices Act). See, for instance, A. Garapon, P. Servan-Schreiber (eds.), *Deals de justice: le marché américain de l'obéissance mondialisée*, Presses universitaires de France, 2013

[45] J.-Y. Maréchal, "Art. 121-2 - Fasc. 20 : Responsabilité pénale des personnes morales," *JurisClasseur Pénal Code*, LexisNexis, May 27, 2022, ¶¶ 56-57. However, the jurisprudence did not consider how the legal personality of a foreign legal person should be set, M. Delmas-Marty, "Personnes morales étrangères et françaises (Questions de droit pénal international)," *Revue des sociétés*, Dalloz, 1993, p. 255.

[46] Fiscalía General del Estado, Circular 1/2011, *op. cit.* note 42, p. 7. The criterion of legal personality will be determined by the law of the nationality of the corporation (Article 9.11 of the Código civil), usually set by the nationality of its headquarters, M. Albaladejo Garcia (ed.), *Normas de Derecho internacional privado. Ambito de aplicación de los regímenes jurídicos civiles españoles*, Edersa, Comentarios al código civil y compilaciones forales, 2nd ed., 1992. For its determination, see J.M. Zugaldía Espinar, *La responsabilidad criminal de las personas jurídicas*, *op. cit.* note 13, pp. 149-150

[47] To protect the contradiction principle within an international situation, E. Velasco Núñez, "Medios de investigación y prueba en los delitos cometidos por persona jurídica," *in* Á. Juanes Peces (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, ¶ 2590. It is facilitated by Article 7 of the 1959 European Convention on Mutual Assistance in Criminal Matters and the 2000 Convention on Mutual Assistance in Criminal Matters between the member states of the EU. On civil matters linked to a criminal process, see Regulation 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the member states of judicial and extrajudicial documents in civil or commercial matters. But those frameworks are still limited to notifying the parent companies, usually headquartered in the United States.

corporation does not comply voluntarily, the EU offers special procedures to apply sanctions abroad.[48] To secure a European procedure against an American digital actor for cyber trafficking, one solution would be to consider both the European representation and the parent company as one entity.

355. Corporations' lives and environments. Digital actors might not have a legal personality, criminal acts might be scattered among entities, and criminal liability should consider groups of societies.[49] Despite the lack of legal personality and the principle of personality in sanctions, the group forms an economic or financial unity,[50] which is why the three national frameworks studied in this paper extended criminal liability to parent companies.[51] Finally, corporations' mergers[52] question criminal

[48] Based on the principle of mutual recognition, Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties (see the suppression of the verification of double criminality for human trafficking, Article 5.1)

[49] It is defined by the doctrine as a "*conglomerate of companies in which all of them depend on the same dominant or parent company that has sufficient economic participation in its capital to make decisions*," I. Blanco Cordero, "Responsabilidad penal de la sociedad matriz por los delitos cometidos en el grupo de empresas," *in* J.M. Suárez López et al. (eds.), *Estudios jurídicos penales y criminológicos: en homenaje al Prof. Dr. Dr. H. C. Mult. Lorenzo Morillas Cueva*, Dykinson SL, 2018, pp. 53-54

[50] Moreover, the parent company might be more solvable, and the offense might have been committed in the interest of the group, E. Daoud, A. André, "La responsabilité pénale des entreprises transnationales françaises : fiction ou réalité juridique ?," *Actualité juridique Pénal*, Dalloz, 2012, pp. 15-16

[51] In the United States, see I. Blanco Cordero, "Responsabilidad penal de la sociedad matriz," *op. cit.* note 49, pp. 64-65. For instance, that might be on the basis that the child company is a mere instrument for the parent, US Supreme Court, *National Labor Relations Board v. Deena Artware, Inc.*, February 23, 1960, 361 U.S. 398. For instance, when the parent company becomes involved in the day-to-day management of the subsidiary so that it no longer acts as a mere investor, US District Court, E.D. Wisconsin, *Handlos v. Litton Industries, Inc.*, May 7, 1971, 326 F. Supp. 965. Moreover, applying the agency theory of liability, the employee of the child company can be an agent of the parent company, US District Court, E.D. Pennsylvania, *US v. Johns-Manville Corporation*, April 16, 1964, 231 F. Supp. 690; or the child company can itself be an agent of the parent company, US Supreme Court, *US v. Bestfoods*, June 8, 1998, 524 U.S. 51. It is interesting to note that the Spanish code, since 1995, even before the introduction of corporate liability, has considered accessory penalties for legal entities. Article 129 nowadays broadens such application to entities lacking legal personality, including groups of corporations, especially when the parent company does not have any legal entity in the country. However, this article still relies on the conviction of the parent company, J.M. Zugaldía Espinar, *La responsabilidad criminal de las personas jurídicas*, *op. cit.* note 13, p. 145. In France and Spain, both the doctrine and the case law multiply interpretations to require the liability of the parent company: as possible *de facto* administrator, I. Blanco Cordero, "Responsabilidad penal de la sociedad matriz," *op. cit.* note 49, p. 57; representative or organ of the subsidiary, F. Stasiak, "Groupe de sociétés - Groupe de sociétés et responsabilité pénale : de l'esquive à l'esquisse," *Droit des sociétés*, LexisNexis, June 2017, no. 6, ¶ 21; or by considering the links of subordination, P. Conte, "Groupe de sociétés : responsabilité pénale de la société-mère," *Droit pénal*, LexisNexis, September 2021, no. 9, p. 25; N. Pérez Rivas, "La responsabilidad penal de los grupos de empresa: criterios sobre la atribución de responsabilidad penal a la empresa matriz por los delitos cometidos por sus filiales," *La Ley Penal*, June 2023, no. 162. In Cour de Cassation, Chambre criminelle, June 16, 2021, no. 20-83098, the central committee of the parent company was considered an organ, as well as employees of the child company which were considered representatives of the parent company.

[52] That regularly happens to digital actors, G. Parker, G. Petropoulos, M. Van Alstyne, "Platform mergers and antitrust," *Industrial and Corporate Change*, October 1, 2021, vol. 30, no. 5, pp. 1307-1336. For instance, Backpage was sold "*to an undisclosed foreign company in 2014*," Permanent subcommittee

liability. While the traditional rule is the absence of transfer of liability, that does not constitute "*economically realistic reasoning*."[53] Consequently, liability after a merger is increasingly recognized.[54]

356. Thus, to fit new economic realities, the concept of criminally liable corporations is an extensive one. Furthermore, the crime is intended to benefit them.

B. Benefiting or on the behalf of the corporation

357. The reason for the offense. The US and Spanish frameworks add the criterion of "benefit" to the corporation,[55] and both are to be interpreted in extensive ways.[56] In France and Spain, the offense must be committed "*on behalf of*" the

---

on investigations, *Backpage.com's knowing facilitation of online sex trafficking*, Committee on Homeland Security and Governmental Affairs, US, January 10, 2017, p. 6

[53] A. Gallois, "Fusion-absorption : revirement spectaculaire de la chambre criminelle de la Cour de cassation !," *Gazette du Palais*, Lextenso, March 30, 2021, no. 13, p. 50

[54] In the United States, see US Court of Appeals, Fifth Circuit, *US v. Alamo Bank of Texas*, September 14, 1989, 880 F.2d 828. Generally, on the basis of three considerations: when the successor company assumes its predecessor's responsibilities, when the merger is fraudulent, and when the successor is a mere continuation of the predecessor, B. del Rosal Blasco, "La transferencia de la responsabilidad penal (y civil, derivada del delito) en los supuestos de sucesión de empresa," *in* J.M. Suárez López et al. (eds.), *Estudios jurídicos penales y criminológicos: en homenaje al Prof. Dr. Dr. H. C. Mult. Lorenzo Morillas Cueva*, Dykinson SL, 2018, p. 188. However, it depends on state corporation law governing successor liability, E. McCready, "Corporate Criminal Liability," *American Criminal Law Review*, 2022, vol. 59, no. 3-Annual Survey of White Collar Crime, p. 583. In France, since 2020, Cour de Cassation, Chambre criminelle, November 25, 2020, no. 18-86955. It is limited to mergers within the framework of Directive 78/855/EEC concerning mergers of public limited liability companies, or to fraudulent mergers. For critics, see O. Bureth, "Responsabilité pénale des personnes morales et fusion-absorption : le grand chambardement ou comment créer une hydre !," *Petites affiches*, Lextenso, January 7, 2021, no. 5, p. 16; N. Catelan, "Opération économique et responsabilité pénale des personnes morales : revirement de jurisprudence," *Gazette du Palais*, Lextenso, March 16, 2021, no. 11, p. 51; A. Gallois, "Fusion-absorption : revirement spectaculaire de la chambre criminelle de la Cour de cassation !," *op. cit.* note 53, p. 50. Although this solution has to be developed, this shift allows for greater possibilities to look for corporate criminal liability. Criteria are thus developed by the literature, J.-C. Saint-Pau, "Responsabilité pénale d'une personne morale absorbante en cas de fraude à la loi," *La Semaine Juridique Edition Générale*, LexisNexis, July 18, 2022, no. 28, p. 1419. In Spain, Article 130.2 of the Código penal. See J.M. Zugaldía Espinar, *La responsabilidad criminal de las personas jurídicas*, *op. cit.* note 13, p. 115; E. Cortés Bechiarelli, "Límites a la extinción de la responsabilidad penal de la persona jurídica (CP art.130.2)," *in* Á. Juanes Peces (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 1100

[55] See also Article 22.1 of the Warsaw Convention and Article 5.1 of the Directive 2011/36/EU

[56] In the United States, the crime must benefit, at least in part, the legal person. This benefit does not have to be financial or real; it depends on the intent of the agent, "*whenever the employee's actions are favorable to the interests of the corporation, even without any direct evidence*," and "*It is […] necessary that the employee be primarily concerned with benefitting the corporation*," J.D. Greenberg, E.C. Brotman, "Strict Vicarious Criminal Liability for Corporations and Corporate Executives: Stretching the Boundaries of Criminalization Symposium: Reducing Corporate Criminality: Evaluating Department of Justice Policy on the Prosecution of Business Organizations and Options for Reform," *American Criminal Law Review*, 2014, vol. 51, no. 1, p. 82; E. McCready, "Corporate Criminal Liability," *op. cit.* note 54, p. 578. It "*is satisfied even if the conduct causes substantial harm to the corporation*," R. Luskin, "Caring about Corporate 'Due Care': Why Criminal Respondeat Superior Liability Outreaches Its Justification," *American Criminal Law Review*, 2020, vol. 57, no. 2, p. 312. In Spain, the benefit can be direct, indirect, or even potential, Fiscalía General del Estado, Circular 1/2016, *op. cit.* note 37, p. 30.

company,[57] but the case law on that topic is limited.[58] Some studies interprets it as a benefit, while others advocate for a different meaning: The offense is committed within the activities of the corporation.[59] The latter interpretation is adopted by the Spanish code: "*For or on behalf of*" is defined as when natural persons act "*as an extension*" of the corporation.[60]

358. An application to human trafficking. The commission of human trafficking can offer many advantages to a company, particularly cost savings realized by reducing wages, extending making them work longer hours, or providing harsh work conditions.[61] Digital actors supporting a human trafficking process may increase their data flow, offer a wider range of products or services, and attract more clients or viewers, gaining indirect benefits from these advertisements. For instance, Backpage increased "*[its] revenue from $11.7 million in 2009, to […] $135 million in 2014*."[62] Regarding the criterion of benefit,[63] recruitment and working relations are part of the activities of any company, while hosting content is among the activities of digital actors.

359. The criteria linked to the corporation are checked, and all of them are broad enough to prosecute corporations for human trafficking. Accordingly, other criteria are to be checked regarding natural persons materially committing the offense.

The case law considered that the criterion was to be considered *ex ante*, meaning that any negative impact was not taken into consideration, Tribunal Supremo. Sala Segunda, de lo Penal, February 29, 2016, *op. cit.* note 37; V. Magro Servet, *Guía práctica*, *op. cit.* note 37, p. 99

[57] Article 121-2 of the Code pénal. Accordingly, it does not transpose correctly the international texts. This criterion also appears in the Spanish code, Article 31 bis.1 of the Código penal.

[58] J.-Y. Maréchal, "Responsabilité pénale des personnes morales," *op. cit.* note 45, ¶ 110. The French one only considers that a natural person can act both on their own behalf and on behalf of the company, Cour de Cassation, Chambre criminelle, January 29, 2020, no. 17-83577 ; or when it is contradictory to its social interest, Cour de Cassation, Chambre criminelle, May 24, 2018, no. 16-86851

[59] J.-Y. Maréchal, "Responsabilité pénale des personnes morales," *op. cit.* note 45, ¶ 111. Then, liability can be applied even in the absence of benefit, Cour de Cassation, Chambre criminelle, June 28, 2017, no. 16-85291

[60] V. Magro Servet, *Guía práctica*, *op. cit.* note 37, p. 123

[61] This cost reduction can also happen when trafficked victims for organ removal sell their organs for a reduced price, allowing the brokers to increase their profits. Companies can also directly earn money from trafficked victims for the purpose of sexual exploitation.

[62] E.M. Donovan, "Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act: A Shield for Jane Doe," *Connecticut Law Review*, 2020, vol. 52, no. 1, p. 94. However, the author considers the general revenue, and does not specify if this increase is linked to illegal advertisements. Furthermore, another author highlights that the benefits come from advertisers, and not from individual postings, E.J. Born, "Too Far and Not Far Enough: Understanding the Impact of FOSTA," *New York University Law Review*, 2019, vol. 94, no. 6, p. 1644. However, the company would still benefit from human trafficking, although indirectly.

[63] Nevertheless, Vivastreet, "*depending on the month of the year, the 7,000 or so offers in the escorting sections bring in between 40% and 50% of the income generated by the ads […] According to our information, this would amount to between 11 million and 21 million euros per year*", L. Motet, "Vivastreet," *op. cit.* note 43

II. Behind the corporation: who, what, and how

360. Identification of the natural perpetrator. "*To talk about the liability of legal persons in criminal law is to continue talking about the criminal liability of natural persons*."[64] This requires identifying the person behind the corporation.[65] This criterion is important considering the "*use of subcontracting schemes to commit or benefit from human trafficking*," and its level of proof is seen as the most difficult.[66] In the United States, a wide range of natural persons can trigger corporate liability,[67] including all employees and agents[68] as long as they act within the scope of their employment.[69] In France, while the case law is unstable regarding the requirement to actually identify a natural person,[70] the interpretation of acting persons is also quite broad.[71] Similarly,

[64] R. Roso Cañadillas, "Prevención," *op. cit.* note 10, p. 33

[65] See also Article 22.1 of the Warsaw Convention and Article 5.1 of the Directive 2011/36/EU

[66] S.C. Pierce, "Turning a Blind Eye," *op. cit.* note 6, p. 590; Z. Muskat-Gorska, "Human Trafficking and Forced Labour," *op. cit.* note 43, p. 448

[67] Up to the point that the wide interpretation of this criterion is highly criticized by the literature, in particular considering the lack of a possible defense on the basis of a compliance system, E. Tuttle, "Reexamining the Vicarious Criminal Liability of Corporations for the Willful Crimes of Their Employees," *Cleveland State Law Review*, 2022 2021, vol. 70, no. 1, p. 138; J.D. Greenberg, E.C. Brotman, "Strict Vicarious Criminal Liability for Corporations," *op. cit.* note 56, pp. 84-86

[68] D. Harris, "Corporate Intent and the Concept of Agency," *Stanford Journal of Law, Business & Finance*, 2022, vol. 27, no. 1, p. 137. It can even be an independent contractor, US Court of Appeals, Seventh Circuit, *US v. Parfait Powder Puff*, November 4, 1947, 163 F.2d 1008

[69] That means "*actual or apparent authority from the corporation to engage in the act*." The former assumes knowledge and authorization of the corporation, while the second considers the reasonable belief of a third party, E. McCready, "Corporate Criminal Liability," *op. cit.* note 54, p. 575. In that latter case, the agent can even be acting against express orders, US Court of Appeals, Ninth Circuit, *US v. Hilton Hotels Corp.*, September 26, 1972, 467 F.2d 1000; or the corporate policy, R. Luskin, "Caring about Corporate 'Due Care,'" *op. cit.* note 56, p. 312

[70] The high court created an unstable case law by accepting or refusing to presume that the act was committed by an organ or a representative, Cour de Cassation, Chambre criminelle, June 20, 2006, 05-85.255; Cour de Cassation, Chambre criminelle, June 25, 2008, no. 07-80261. Criticized for stretching the principle of personality, the case law turned around, Cour de Cassation, Chambre criminelle, October 11, 2011, no. 10-87212; although with exceptions, Cour de Cassation, Chambre criminelle, May 15, 2012, no. 11-83301; Cour de Cassation, Chambre criminelle, June 12, 2012, no. 11-83657; Cour de Cassation, Chambre criminelle, June 18, 2013, no. 12-85917. A recent case law seems to accept the lack of identification of the natural person, making it difficult to end this debate, Cour de cassation, Chambre criminelle, June 21, 2022, no. 20-86857; J.-H. Robert, "Application de l'article 121-2 du Code pénal au cas où l'organe de la société prévenue est lui-même une société," *La semaine du droit pénal et procédure pénale*, LexisNexis, September 12, 2022, no. 36, pp. 1623-1626

[71] First, organs can trigger corporate liability, as an individual or a collective, as set by law or by statutes, J. Lasserre Capdeville, "La notion d'organe ou de représentant de la personne morale," *Actualité juridique Pénal*, Dalloz, 2018, p. 550. The case law broadened the concept to *de facto* managers, Cour de Cassation, Chambre criminelle, December 17, 2003, no. 00-87872, based on a "*'bundles of evidence' of powers that may indicate the existence of a management activity or participation in the general conduct of the business*," J. Lasserre Capdeville, "La notion d'organe ou de représentant," p. 550. However, in these cases, they are usually categorized as representatives. Second, representatives are an even broader concept. The Cour de Cassation refused to send a case to the Conseil Constitutionnel, considering the lack of a definition for this concept not relevant, Cour de cassation, Chambre criminelle, June 9, 2022, no. 22-90006. The case law opened it to any person, including employees, having a delegation of authority, Cour de Cassation, Chambre criminelle, December 1, 1998, no. 97-80560. The

Spanish law broadened the range of acting persons,[72] and corporate liability can be triggered "*even if the specific individual responsible has not been identified or it has not been possible to direct the proceedings against them*."[73]

361. Applying human trafficking to corporate liability. As a reminder, two categories of corporate liability exist regarding offenses applicable to corporate criminality: the "all crimes" approach and the "list-based" approach.[74]. In the United States, it depends on the definition of the offense:[75] Human trafficking is broadly open to legal persons. In France, since 2004,[76] corporate liability can be applied to any offense. On the contrary, in Spain, such liability is open only to offenses explicitly

Court is lenient on the form of the delegation, which can take any form, A. Benoit, "Responsabilité pénale des personnes morales : l'auteur de l'infraction doit avoir la qualité d'organe ou de représentant de la société," *Gazette du Palais*, Lextenso, April 3, 2018, no. 13, p. 50. It also includes those with a subdelegation, Cour de Cassation, Chambre criminelle, June 26, 2001, 00-83.466, formally given, even when not an employee of the company but an independent proxy, Cour de Cassation, Chambre criminelle, February 23, 2010, no. 09-81819, or resulting from the circumstances, Cour de Cassation, Chambre criminelle, February 7, 2006, 05-80.083. It can be an agent without any contractual link with the company, Cour de Cassation, Chambre criminelle, October 13, 2009, no. 09-80857. Going further, the high court validated the categorization as representative of an employee without any delegation of authority, Cour de Cassation, Chambre criminelle, April 6, 2004, 02-88.007; even an employee of a subsidiary, Cour de Cassation, Chambre criminelle, June 16, 2021, *op. cit.* note 51; E. Dreyer, "Responsabilité pénale des personnes morales : à la recherche de l'organe et du représentant perdus," *Gazette du Palais*, Lextenso, September 14, 2021, no. 31, p. 37

[72] J.G. Fernández Teruelo, "La responsabilidad penal de los dirigentes, representantes de la persona jurídica o de quienes ostentan facultades de organización y control de la misma," *in* Á. Juanes Peces (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, ¶ 1658. This has been criticized, M. Abel Souto, "Algunas discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el código penal español," *Revista General de Derecho Penal*, Iustel, 2021, no. 35, p. 39. First, the code considers three categories of persons having specific powers of management or direction. It includes legal representatives, those authorized to take decisions for the corporation, and those with powers of organization and control. The first category "*includes any person who formally has the power to legally bind the entity with its decisions, regardless of the title by virtue of which they hold such power, whether by delegation or by law*," M. Gómez Tomillo, *Introducción a la responsabilidad penal de las personas jurídicas*, Thomson Reuters Aranzadi, Colección Monografías Aranzadi Aranzadi derecho penal no. 768, Segunda edición, 2015, pp. 100-101. The second includes "*any person who has the real capacity to make socially relevant global or partial decisions on issues related to the company's line of business, in short, any person who effectively exercises social control, even in specific areas*," *Ibid.* pp. 102-103. The third "*includes a potentially large number of positions and middle management that have been attributed such powers, including surveillance and control measures to prevent crimes*," V. Magro Servet, *Guía práctica*, *op. cit.* note 37, p. 98. Second, the code also includes anyone, within corporate activities, subject to the authority of the first group of persons: it does not require a contractual link with the corporation, including "*self-employed or solely subcontracted workers*," *Ibid.* p. 104

[73] Article 31 ter of the Código penal.

[74] M. Pieth, R. Ivory, "Emergence and Convergence," *op. cit.* note 8, p. 20

[75] G.A. Jimenez, "Corporate Criminal Liability: Toward a Compliance-Oriented Approach Notes," *Indiana Journal of Global Legal Studies*, 2019, vol. 26, no. 1, p. 355

[76] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. Before, each offense had to consider the liability of corporations. Since the introduction of the offense of human trafficking, corporations have been deemed liable, Article 225-4-6 of the Code pénal, in the version from the Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure

including it, such as human trafficking.[77] However, the *numerus clausus* is criticized as inconsistent; for example, not all forms of exploitation after trafficking are included.[78]

362. While the literature on human trafficking is usually critical regarding corporate criminal liability, the links connecting the act of a person to the corporation are multiple. Accordingly, the acts (A) and the intent (B) of human trafficking should be attributed to such a person.

A. The absence of the material acts of human trafficking

363. Actions and means. Human trafficking requires three elements, including two material acts. It should be considered whether this definition is broad enough to convict digital actors for facilitating human trafficking.[79] First, a natural person should commit one of the actions of the offense,[80] and all three codes include the recruitment of victims.[81] Such action would be appropriate for corporations recruiting workers or for employment agencies advertising jobs or their services online. However, digital actors prosecuted for sex trafficking were not recruiting victims. Consequently, the actions of both transporting[82] and harboring[83] victims must be physically committed, although

[77] Article 177 bis.7 of the Código penal. Before, human trafficking was considered in Article 318 bis of the code, mixed with the smuggling of migrants, and the offense was considering accessory sanctions for legal persons (Article 129), although not liable, since 2003, see Ley Orgánica 11/2003, de 29 de septiembre, de medidas concretas en materia de seguridad ciudadana, violencia doméstica e integración social de los extranjeros, Article 13 (Article 318 bis.5 of the Código penal)

[78] Included are sexual exploitation and pimping, Article 189 bis of the Código penal; and organ trafficking, Article 156 bis.3. Is not included the offense against workers' rights, which has been critiziced by the doctrine, E. Pomares Cintas, *El Derecho Penal ante la explotación laboral y otras formas de violencia en el trabajo*, Tirant lo Blanch, Monografías, 2013, vol. 822, p. 52; M.S. Gil Nobajas, "Respuesta penal a la criminalidad empresarial en supuestos de explotación laboral," *in* J. Gómez Lanz, D. Benito Sánchez, A. Martínez de Bringas (eds.), *Sistema penal y exclusión social*, Aranzadi, Monographs in comparative and transnational law no. 10, 2020, pp. 186-191. The Tribunal Supremo refused to extend the *numerus clausus* for this offense, Tribunal Supremo. Sala Segunda, de lo Penal, February 23, 2017, no. 121/2017. Nor are included the offenses of organized group, that might also be used to prosecute human trafficking, Articles 515 and followings and 570 bis and followings, N.J. de la Mata Barranco, "Tipos penales para los que se prevé responsabilidad penal. Lagunas y deficiencias a la luz de la normativa europea," *in* Á. Juanes Peces (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, ¶ 1305

[79] Criminal law is of strict interpretation by application of the principle of legality of offenses.

[80] 18 USC § 1591.a, as in the 2010 version; Article 225-4-1.I of the Code pénal; Article 177 bis of the Código penal

[81] It must be noted that the Spanish Código penal uses a wider verb: "captar" (to win over), meaning, the process in which the author "*earns the will of the future victim*," P. Lloria García, "El delito de trata de seres humanos y la necesidad de creación de una ley integral," *Estudios Penales y Criminológicos*, June 22, 2019, vol. 39, p. 378. The United States code adds, similarly, "to entice," as an alternative to formal recruitment.

[82] Taking someone from one place to another, *Ibid.* p. 379. The French and Spanish codes add "to transfer," which is deemed to be the same action.

[83] Harboring victims can be restrictively interpreted as giving shelter. Twisting the principle of legality, such action could be extended, in particular in the French framework, to digital actors, since the verb "to

they can be organized online. Furthermore, the Spanish code includes the exchange or transfer of control to include cases of "*sale, exchange, or rental*."[84] The US code also adds similar action verbs: "to obtain" and "to provide." These actions hardly fit the situation of the investigated digital actors. They are committed by the trafficker, not by a natural person within a company that serves as a digital actor.[85] Second, when trafficking adults, certain means must be committed.[86] The codes usually consider the use of threat, force, fraud, or coercion; additionally, in France and Spain, the abuse of authority and of vulnerability[87] are considered as well as the exchange of remuneration or any advantage. The perpetrator should have a direct link, although possibly digital,[88] with the victim to implement these means. Nonetheless, regarding the online advertisement of victims, natural persons employed by digital actors usually do not have any contact with the victim. Consequently, they do not commit any means to void their consent.

364. From author to accomplice. Corporations, including digital actors, can play "*a major role*"[89] within the trafficking process, including digital actors, but not all of them can be qualified as perpetrators. Rodríguez-López develops three categories. First, "*When companies directly and willingly recruit victims, transport them, provide them with the required documentation […], and obtain benefits from that exploitation*," acting persons of the company are committing trafficking actions and means, and the company can be liable. Second, corporations can "*hire trafficked workers supplied by*

host" could be applied to online hosting in the sense of giving an online space for the advertisement of the victim. In any case, the creation of the advertisement is usually done by the trafficker or the victim, and not by a natural person from the corporation. The concept of harboring is extended through other verbs: "to receive" or "to welcome" ("accueillir") in the French code, "to take in" or "to receive" ("acoger" and "recibir") in the Spanish code; "to maintain" in the US definition. In general, it means "*to take care of the victim*," *Ibid.*

[84] *Ibid.* p. 380

[85] Moreover, the United States considers a second category within the offense: to benefit "*from participation in a venture which has engaged in an act*," 18 USC § 1591.a.2. It was interpreted as the following: "*The actor must have been one of two or more people engaged in sex trafficking together, and the actor must have participated in a way that furthered the trafficking*," K. Albert et al., "FOSTA in legal context," *Columbia Human Rights Law Review*, Columbia University. School of Law, 2021, vol. 52, no. 3, pp. 1120-1124; US Court of Appeals, Sixth Circuit, *United States v. Afyare*, March 2, 2016, no. 13-5924, *632 F. App'x 272* Therefore, the acting person should have participated in the actions already mentioned.

[86] Those means do not have to be proven regarding minor victims that could improve the triggering of corporate liability, being only required to fit within the offense's actions. However, then, the digital actor "*will alternatively need knowledge that the victims were minors*," with how such knowledge should be proven remaining to be seen, E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 62, p. 1641

[87] And abuse of necessity in Spain

[88] For instance, a person abusively recruiting for a company through their website could trigger the liability of the corporation.

[89] S. Schumann, "Corporate Criminal Liability on Human Trafficking," *op. cit.* note 3, p. 1658

third parties," which could still trigger their liability by extending the interpretation of the range of control of the legal person. Finally, corporations might be involved "*in human trafficking when their products, services, or facilities are used in the trafficking process*."[90] In that case, digital actors will hardly be able to be considered perpetrators. However, it would be interesting to explore the qualification of the accomplice.[91] Materially, the natural person must provide give assistance to the trafficker,[92] but complicity is sanctioned only when this assistance is provided knowingly, voluntarily, or intentionally.[93] The acting person needs "*an awareness of associating oneself with*"[94] a human trafficking offense, and this awareness might not exist or might be difficult to prove regarding digital actors.[95] However, it should be noted that Spain excludes criminal liability for accomplices for offenses "*committed using mechanical means or media of dissemination*."[96] Nonetheless, the article is not clear whether this applies to any offense committed this way, such as cyber human trafficking, or to

[90] S. Rodríguez-López, "Criminal Liability of Legal Persons for Human Trafficking," *op. cit.* note 24, pp. 98-99. Differently, Chen differentiates between "*direct responsibilities resulting from actions of the focal organization and indirect responsibilities resulting from actions of related parties over whom the focal organization has power*," S. Chen, "Corporate Responsibilities in Internet-Enabled Social Networks," *Journal of Business Ethics*, Springer, 2009, vol. 90, p. 527. Although a digital actor has a certain amount of power to control its components, the corporate liability framework does not encompass as an acting person a third party that is using its services. The natural person trafficker is not included in the scope of control of the corporation.

[91] In particular, the French code explicitly includes complicity in the form of liability of legal persons, Article 121-2 remitting to Article 121-7 of the Code pénal, see J.-Y. Maréchal, "Responsabilité pénale des personnes morales," *op. cit.* note 45, ¶ 77. Although not explicitly stated in the code, legal persons liable as accomplices are also accepted in Spain, M. Gómez Tomillo, *Introducción a la responsabilidad penal de las personas jurídicas*, *op. cit.* note 72, pp. 226-228. And accomplices bear the same sanctions as the author, although the penalty will have to be individualized, Article 121-6 of the Code pénal; Article 27 of the Código penal; US Supreme Court, *Waddington v. Sarausad*, January 21, 2009, 479 F. 3d 671

[92] In Spain, to "*contribute, collaborate, or help*," J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal*, *op. cit.* note 10, p. 233. It includes both active acts and passive behaviors, J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal*, *op. cit.* note 10. Similarly, in the United States, it includes, in some cases, the act of failing to prevent the commission of an offense, which therefore includes passive behaviors. In France, to facilitate "*by aid or assistance*" the preparation or consumption of the offense, Article 121-7 §1 of the Code pénal. It rejects complicity in the absence of any active acts, B. Bouloc, *Droit pénal général*, Dalloz, Précis, 27th ed., 2021, ¶ 356. It remains to be seen if the provision of a service that facilitates human trafficking is considered an active act of assistance.

[93] That is widely interpreted in the United States as "being aware" of the crime, Washington State Court of Appeals Division Two, *State Of Washington v. Darcus D. Allen*, July 27, 2021, 54007-0-II

[94] B. Bouloc, *Droit pénal général*, *op. cit.* note 92, ¶¶ 368-369

[95] On the concept of knowledge, see *infra* 366 to 368 and 382 to 383.

[96] Article 30 of the Código penal. The latter concept should be extended to "*any means of social communication, [such as] the traditional ones referred to press, radio, and television but, at the same time, without exclusion of modern ones […], including Internet […], with the obvious exception of those strictly related to personal communications that do not acquire the required social character of the medium*," L. Morillas Cueva, "La compleja delimitación de la autoría y participación en los delitos cometidos con empleo de medios o soportes de difusión mecánicos," *in* J.M. Lorenzo Salgado, M. Abel Souto (eds.), *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado*, Tirant lo Blanch, Homenajes & congresos, 1st ed., 2021, pp. 979-980

offenses whose core elements are committed precisely because of this dissemination,[97] such as child pornography. Due to the complexity of this regime, authors even advocate for its deletion.[98]

365. Despite the broad interpretations of the concepts of a natural person or of acting, the definition of human trafficking might apply to digital actors that facilitate cyber trafficking. A last element should be proved to trigger corporate liability: intent.

B. Proving criminal intent

366. The acting person's intent. The natural person should demonstrate the specific intent of human trafficking: the intent to exploit the victims. In the United States, vicarious liability makes the corporation liable by imputation of the acting person's fault,[99] and in France, the intent of the corporation is identified through the acting person.[100] Regarding digital actors, the exploitation does not occur or is not visible in their realm. Thus, it requires proof that a natural person knew that a publication advertised a victim and failed to remove the content, or that the website was built to support human trafficking. This question has been raised regarding Backpage, as it was "*editing 70 to 80% of the [advertisements] in the adult section [… to look] for the use of forbidden words and erased them*."[101] By erasing signs linked to being underage,[102] the moderators could have known this would be qualified as exploitation, but the advertisements remained online.

367. The corporation's intent. In Spain, a special fault of the corporation should

[97] *Ibid.* p. 981; M. Díaz y García Conlledo, "El complicado régimen privilegiado del art. 30 del Código Penal Español en materia de codelincuencia y encubrimiento en los delitos cometidos utilizando medios o soportes de difusión mecánicos," *Nuevo Foro Penal*, Universidad EAFIT, 2013, vol. 9, no. 81, p. 79
[98] M. Díaz y García Conlledo, "El complicado régimen privilegiado del art. 30 del Código Penal Español," *op. cit.* note 97, p. 88
[99] M.E. Diamantis, "The Extended Corporate Mind: When Corporations Use AI to Break the Law," *North Carolina Law Review*, 2020 2019, vol. 98, no. 4, p. 898. The case law even recognized a possible "collective knowledge" to prove the fault, US Court of Appeals, First Circuit, *US v. Bank of New England, N.A.*, June 10, 1987, 821 F.2d 844; E.S. Podgor, "Corporate Criminal Liability: Introduction," *Stetson Law Review*, 2012 2011, vol. 41, no. 1, p. 3
[100] J.-Y. Maréchal, "Responsabilité pénale des personnes morales," *op. cit.* note 45, ¶¶ 105-109
[101] J. Raphael, "Denial of Harm: Sex Trafficking, Backpage, and Free Speech Absolutism," *Dignity: A Journal on Sexual Exploitation and Violence*, 2017, vol. 2, no. 1, p. 4. For instance, words "*like "barely legal" or "high school" [were replaced] with words and phrases such as "brly legal" or "high schl"*," E.M. Donovan, "FOSTA and SESTA," *op. cit.* note 62, p. 88. It might be particularly useful when not all recruiters are aware of the actual working conditions, or when actions and means are not realized by the same person.
[102] Yet it is only a knowledge of potential exploitation, considering the possibilities to lie online.

be proved:[103] the lack of organization and control of the acting person.[104] The code develops the required compliance to avoid liability.[105] Depending on the sector, a corporation would need to consider the risks of human trafficking to build an adequate and effective compliance program. That could question the adequacy of Backpage's strategy to erase specific words instead of suspending the advertisements. This criterion considers internal efforts to prevent the commission of offenses and to better scale liability and sanctions. On the contrary, it is not considered in France,[106] and it is only taken into account by the organizational guidelines of the US Department of Justice to determine the level of the sanction.[107]

368. Trafficking facilitated through algorithms. Digital actors might host content linked to human trafficking that is accidentally promoted by their algorithms.[108] If the corporation is qualified as an accomplice and if the victim is a minor, the main obstacles are the identification of the acting person and the intent. In that case, the former criterion appears outdated when corporate "*operations require less and less human intervention*,"[109] particularly regarding online activities.[110] Some studies in the literature consider that offenses committed through algorithms might no longer require an acting person,[111] since the functioning of the software transforms the "*legal person's neuronal*

[103] To protect the principle of personality, Tribunal Supremo. Sala Segunda, de lo Penal, February 29, 2016, *op. cit.* note 37; V. Magro Servet, *Guía práctica*, *op. cit.* note 37, p. 95

[104] J.C. Carbonell Mateu, "Responsabilidad penal de las personas jurídicas," *op. cit.* note 8, acts 17-19; V. Magro Servet, *Guía práctica*, *op. cit.* note 37, act 70; Tribunal Supremo. Sala Segunda, de lo Penal, March 16, 2016, no. 221/2016. On the contrary, part of the doctrine only takes into account the fault of the acting person, J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal*, *op. cit.* note 10, p. 389; S. Pérez González, "Sobre la culpabilidad empresarial: notas para una coexistencia eficaz de los artículos 31 bis y 129 del Código Penal," *Estudios Penales y Criminológicos*, April 21, 2020, vol. 40, p. 196; Fiscalía General del Estado, Circular 1/2016, *op. cit.* note 37, p. 11

[105] Article 31 bis.5 of the Código penal, see *infra* Part 2. Title 2. Chapter 1. .

[106] That is criticized by the literature, C. Gomez-Jara Diez, "Corporate Culpability as a Limit to the Overcriminalization of Corporate Criminal Liability: The Interplay between Self-Regulation, Corporate Compliance, and Corporate Citizenship," *New Criminal Law Review*, 2011, vol. 14, no. 1, p. 82. It can question the conformity of the French code to international frameworks: The European anti-trafficking texts only rule corporate liability due to a "*lack of supervision or control*," Article 22.2 of the Warsaw Convention and Article 5.2 of Directive 2011/36/EU

[107] E. McCready, "Corporate Criminal Liability," *op. cit.* note 54, pp. 600-604. However, no corporation prosecuted in the fiscal year 2020 benefited from this mitigating factor.

[108] For instance, the selling and buying of victims of domestic servitude has happened on Instagram through "*posts […] promoted via algorithm-boosted hashtags*," O. Pinnell, J. Kelly, "Slave markets found on Instagram and other apps," *BBC News*, October 31, 2019, online https://www.bbc.com/news/technology-50228549 (retrieved on September 24, 2021)

[109] M.E. Diamantis, "The Extended Corporate Mind," *op. cit.* note 99, p. 899

[110] I. Salvadori, "Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal," *Cuadernos de política criminal*, Dykinson, 2021, no. 133, p. 141

[111] Entities based on algorithms do not have legal personality in Europe. Therefore, it is of specific interest to look for other persons that can answer for torts and offenses committed through them. Further, it could be considered that if corporations "*bear the financial risk when their algorithms misbehave,*

circuit"[112] into reality. However, regarding trafficking, proof would be required that the function of the algorithm was designed to support content linked to the offense, which is hardly imaginable; such support might well be unintended.

369. Contrary to the criticism of anti-trafficking scholars and practitioners, corporate criminal liability is constantly being extended, and these frameworks could be used to sanction human trafficking committed within traditional corporations. As digital actors gain sovereignty by developing their own forms of coercion, they facilitate cyber trafficking. However, extending criminal liability to digital actors in this situation seems impossible, because the requirements for material acts and the intent are hardly met. Therefore, the problem might lie not in corporate criminal liability but in the definition of human trafficking. Nonetheless, before the amendments to it are studied, another set of rules limit states' hard sovereignty and protect digital actors from liability.

§2. States' sovereignty facing digital actors' liability for cyber trafficking

370. Protecting digital actors from liability. Digital actors are particularly protected from criminal law, creating additional obstacles to prosecuting them for cyber trafficking.[113] Seen as major actors in economic development,[114] they obtained specific immunity in the 1990s, and these laws were passed in response to unstable case law. While a 1991 US case was decided in favor of a digital actor, despite the fact that it hosted illegal content,[115] a digital actor was convicted in a 1995 case involving a similar

technology firms will take more efficient precautions in designing and testing their products," *Ibid.* p. 154. For now, an offense committed through an algorithm would require finding the acting person at the origin of the act, for instance, those "*who have programmed, developed, produced or tested it*," or even those who have used it, *Ibid.* p. 157

[112] S. Pérez González, "Sobre la culpabilidad empresarial," *op. cit.* note 104, pp. 188-189; M.E. Diamantis, "The Extended Corporate Mind," *op. cit.* note 99, p. 916

[113] Permanent subcommittee on investigations, *Backpage*, *op. cit.* note 52, p. 4

[114] C. Castets-Renard, "Fascicule 1245 : Régulation des plateformes en ligne," *JurisClasseur Europe Traité*, December 1, 2021, ¶ 14; M. Tessier, J. Herzog, L. Madzou, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, pp. 179-180. On the Communication Decency Act, see Telecommunications Act, Public Law 104-104, February 8, 1996. See ¶1, 2, and 5 of the preamble of the Directive 2000/31/EC. However, these regimes could have been justified by the protection of fundamental rights online. Indeed, if broadly liable, digital actors would have protected themselves by taking down problematic contents, which would have affected many human rights, S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?," *Oslo Law Review*, Universitetsforlaget, 2021, vol. 8, no. 01, p. 13

[115] US District Court, Southern District of New York, *Cubby, Inc. v. CompuServe Inc.*, October 29, 1991, *776 F. Supp. 135*. According to the ruling, digital actors could be liable only for the content they knew, such knowledge existing when reviewing the posts on their website. Therefore, the case did not considered pre-screening moderation, E. Goldman, "An Overview of the United States' Section 230 Internet Immunity," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford

situation.[116] During the same period, European national case law around this topic began to develop,[117] but, disparities "*prevent[ed] the smooth functioning of the internal market*."[118] Consequently, the United States passed the Communications Decency Act in 1996,[119] which states that "*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. [And] no provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable*."[120] Therefore, this act creates a "*double-pronged protection for moderation: It gives moderators immunity both for the content they moderate and the content they miss*."[121] Since they do not become the "publisher" from the act of moderating, digital actors "*can claim 'the right but not the responsibility' to remove users and delete content*."[122] Differently, the EU constructed three frameworks for digital actors' liability, first established in the E-Commerce Directive[123] and, replaced

University Press, May 4, 2020, p. 156. In the absence of review, the digital actor would be "*a distributor of content, and not a publisher*," K. Klonick, "The new governors: the people, rules, and processes governing online speech," *Harvard Law Review*, 2018, vol. 131, p. 1604

[116] New York Supreme Court, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, May 24, 1995. Applying a similar criterion, and considering that the site was trying to moderate its posts, it was deemed as a publisher, in particular due to the use of "*automatic software and guidelines for posting*," K. Klonick, "The new governors," *op. cit.* note 115, p. 1605. It was liable for all posts, even when moderating only some of them, H.C. Halverson, "The Communications Decency Act: Immunity For Internet-Facilitated Commercial Sexual Exploitation," *Dignity: A Journal on Sexual Exploitation and Violence*, February 2018, vol. 3, no. 1, p. 5. According to this criterion, all main digital actors nowadays would be liable for illegal content, from instance linked to human trafficking, to be found in their realm. This decision held a severe liability, as most sites would not have had the resources to adequately moderate all their content; or to not moderate at all, at the risk of having their content impact their reputation, E. Goldman, *Balancing Section 230 and Anti-Sex Trafficking Initiatives - Hearing on "Latest Developments in Combating Online Sex Trafficking" - Written Remarks*, Legal Studies Research Papers Series, no. 2017-17, Santa Clara University School of Law, November 30, 2017, p. 4

[117] M. Peguera Poch, *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Derecho de la sociedad de la información no. 15, 2007, pp. 175-189

[118] ¶40 of the preamble of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")

[119] 47 USC § 230 - Protection for private blocking and screening of offensive material

[120] 47 USC § 230.c.1 and 2

[121] J. Grimmelmann, "The Virtues of Moderation," *Yale Journal of Law and Technology*, 2015, vol. 17, no. 1, p. 103; T. Gillespie, "Platforms Are Not Intermediaries," *Georgetown Law Technology Review*, July 21, 2018, vol. 2, p. 204

[122] T. Gillespie, "Platforms Are Not Intermediaries," *op. cit.* note 121, p. 205

[123] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Articles 12 to 14. As the deriving case law is highly developed, national frameworks will not be studied in detail.

by the Digital Services Act.[124] In general, digital actors are not liable as long as they do not have an active role regarding the content of the information. First, providers of mere conduct services[125] are exempt from liability. Second, providers of transmission services with storage functions are exempt when complying with similar conditions of passivity in general.[126] However, they have an active obligation to act expeditiously to remove the content when they obtain knowledge of its illegality or when it is ordered by a state authority.[127] Finally, providers of hosting services are not liable until they have knowledge of illegal content and, when they do, if they expeditiously remove access to it.[128]

371. Nonetheless, these regimes are not absolute; the law did not exclude digital actors from states' hard sovereignty (I). The problem derives from the case law: When interpreted broadly, digital actors began to be excluded in practice from the grasp of the states, particularly when facilitating cyber trafficking (II).

I. Balancing protection and liability of digital actors: the legal scope

372. Although digital actors were meant to be protected from liability based on economic sovereignty, this exemption was not drafted to completely exclude them completely from criminal prosecutions. Their liability should be studied in relation to criminal law (A) and its subjective scope (B).

A. Objective scope: extension to criminal liability

373. Section 230 and federal crimes. The US immunity is directed mainly to civil liability,[129] but also provides for an exemption to the immunity: The provision is not applicable when prosecuting federal crimes,[130] which include human trafficking.[131] Still, to be a federal offense, sex trafficking requires a supplementary criterion compared to

[124] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, Articles 4 to 7 and 89
[125] "*Consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*," Article 3.g.i of the Digital Services Act. By contrast, the exemption is not applicable when initiating the transmission, selecting the receiver, or selecting the information, Article 4.1
[126] These are: to not modify the information, to comply with conditions on access, to update rules, and to not interfere with the lawful use of technology, Article 5.1.a to d of the Digital Services Act
[127] Article 13.1.e of Directive 2000/31/EC
[128] Article 14 of Directive 2000/31/EC
[129] 47 USC § 230.c.2
[130] 47 USC § 230.e.1
[131] 18 USC § 1590 and 1591

human trafficking for labor exploitation: The offense must affect interstate or foreign commerce.[132] Differently put, it must be transnational or involve various US states. The problem lies in that "*state criminal prosecutions are pre-empted to the extent they are predicated on third-party content*."[133] However, prosecuting a digital actor could be seen as affecting interstate commerce by default, considering its possible use in multiple jurisdictions.

374. Applying the EU regime to criminal law. The EU regime on digital actors' liability does not specify what the type of liability to which it applies to. While the criminal competences of the EU were slowly emerging in 2000,[134] the E-Commerce Directive was based on an economy-related provision of the Treaty establishing the European Community.[135] Today, there is no further detail in the Digital Services Act,[136] so the scope of the regime remains within the margin of appreciation of member states.[137] However, this broad and explicit extension of the objective scope fits with the conditional liability[138] offered by the text: The digital actor can be liable even for content provided by a third party when being active or having knowledge of such content and not moderating it. Nonetheless, the literature[139] highlights the limited possibilities for applying this criminal regime to digital actors, as already mentioned, because of the definition of criminal offenses. Digital actors will not be seen as perpetrators but mainly as accomplices.[140] Therefore, it is not a "*liability for the acts of others, but rather liability for personal acts due to the failure to react to the actions of others*."[141]

375. Therefore, the laws also set forth the types of legal persons to whom these

[132] 18 USC § 1591.a.1; on the contrary, this criterion is not applicable when a person is prosecuted on the basis of benefiting from participation in a venture engaged in sex trafficking, 18 USC § 1591.a.2. If the criterion is not met, US states prosecute sex trafficking on the basis of state criminal law.
[133] E. Goldman, "An Overview of the US' Section 230," *op. cit.* note 115, pp. 161-162
[134] See *supra* 253.
[135] In particular, Articles 47.2, 55 and 95 of the Treaty establishing the European Community
[136] Articles 4 to 7 of the Digital Services Act
[137] National regimes apply to criminal law both in Spain, Article 13.1 of the Ley de servicios de la sociedad de la información y de comercio electrónico, and France, Article 6.I.3 of the Loi pour la confiance dans l'économie numérique. In the latter framework, see also Article 6.VI.1 § 2 explicitly mentioning corporate criminal liability for certain offenses when having knowledge of them, including human trafficking, by application of Article 6.I.7 § 4.
[138] T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018, p. 33
[139] Moreover, the literature regarding the criminal liability restriction of digital actors is limited, with most of it, and of the case law, being dedicated to civil liability.
[140] M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 55
[141] F.-J. Pansier, E. Jez, *La criminalité sur l'internet*, Presses universitaires de France, 2001, p. 9

exemptions are to be applied.

B. Subjective scope: delimitation of digital actors

376. United States: interactive computer services. Both the American and European regimes apply broadly to any natural or legal person providing a specific type of service.[142] The US version applies to Internet content providers[143] who are seen as publishers, as well as and interactive computer services. The latter category benefits from the immunity and broadly includes "*any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server*."[144] At its origin, the statute was meant to extend to online services and access providers. Furthermore, a third category "*awkwardly*" attempted to define digital actors as providers of services to host third-party content.[145] Thus, immune providers include those that "*filter, screen, allow, or disallow content; pick, choose, analyze, or digest content; or transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content*."[146] Nonetheless, these categories are likely to evolve through case law.

377. EU: information society services and hosting services. The EU delimits its regime through the broad[147] category of information society services, meaning "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services […] through the transmission of data on individual request*."[148] This general category fits "*many technical and legal differences between hosting (read: platforms) on the one hand and 'mere conduit' and 'caching' on the other*."[149] While the definitions of these three categories were implicitly

[142] Explicitly, see Article 2.b of the Directive 2000/31/EC
[143] Meaning, "*any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service*," 47 USC § 230.f.3
[144] 47 USC § 230.f.2
[145] T. Gillespie, *Custodians of the internet*, *op. cit.* note 138, p. 34
[146] 47 USC § 230.f.4
[147] Explicitly recognized as such in the Spanish preamble of the Ley de servicios de la sociedad de la información y de comercio electrónico
[148] Article 1.1.b of Directive (EU) 2015/1535 of the European Parliament and the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services. The Spanish transposition specifies that it includes "*services that are not remunerated by their recipients, insofar as they constitute an economic activity for the service provider*," Anexo a § 2 of the Ley de servicios de la sociedad de la información y de comercio electrónico
[149] The latter two categories group a wide range of diverse services that were not explored as much by the literature, S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries," *op. cit.* note 114, p. 9

developed in the E-Commerce Directive, the Digital Services Act finally offers explicit and, thus, harmonized definitions,[150] within the umbrella of "intermediary services." What interests this study here is the hosting services, which consist "*of the storage of information provided by, and at the request of, a recipient of the service*."[151]

378. Despite these broad objective and subjective scopes, the case law led to extending them even more, perhaps going further than the will of the legislators. The US case law focused on the extension of the scope of the liability regime since the absence of the notion of "knowledge" avoided "*tendentious philosophical inquiries into what and when an online service 'knows' about user content*."[152] Indeed, at the European level, debates involve the concepts of "hosting" and "knowledge."

II. Protecting digital actors from liability: case law extensions

379. While the immunity regime first established a balance for its application, the case law significantly extended the regime (A). The American law provides for broad immunity but excludes the prosecution of federal crimes such as human trafficking. The European regimes carves exceptions when the digital actors have an active role, requiring a certain "*threshold mental state*."[153] This balance may be appropriate for criminal law and the principle of culpability, but criminal law does not look for the liability of those with no intervention power or reason.[154] However, this study has already demonstrated the powers of coercion of digital actors over data, so knowledge or a link to the information can "*vary between high probability and physical impossibility*."[155]

---

[150] The change from a directive to a regulation is of particular importance since, for instance, the French framework sits in a totally different category. It includes providers that, for remuneration or for free, and at the individual request of a recipient of services, store information for online public communication services, Article 6.I.2 of the Loi pour la confiance dans l'économie numérique. This latter concept is defined as "*any transmission, upon individual request, of digital data not considered private correspondence by an electronic communication process allowing a reciprocal exchange of information*," Article 1.IV § 4. However, the interpretation of the national law must conform to the European texts and their interpretation by the CJEU.

[151] Article 3.g.iii of the Digital Services Act

[152] E. Goldman, "An Overview of the US' Section 230," *op. cit.* note 115, p. 159

[153] J. Riordan, "A Theoretical Taxonomy of Intermediary Liability," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 61

[154] M. Vivant, "La responsabilité des intermédiaires de l'internet," *La Semaine Juridique Edition Générale*, 1999, no. 45

[155] J. Bossan, "Le droit pénal confronté à la diversité des intermédiaires de l'internet," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2013, p. 296. For instance, Ziniti considers if scanning the content through an algorithm is enough to be considered as having knowledge of the content, C. Ziniti, "Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It," *Berkeley Technology Law Journal*, 2008, vol. 23, no. 1, p. 601

Therefore, the limited interpretation of digital actors' intent[156] is designed to significantly restrict the application of criminal law, to the point of making impossible the prosecution of their relationship to human trafficking content.[157] As such, the limitation of states' hard sovereignty is highly criticized (B).

A. A worldwide almost blank immunity

380. A broad interpretation of far-reaching immunity. The first interpretation of Section 230[158] in 1997 created "*nearly unlimited expansions of immunity*."[159] It resulted in a three-part test to apply the statute: "*(1) whether the defendant qualifies as a provider of an 'interactive computer service,' (2) whether the asserted claims treat the defendant as a publisher or speaker of the information, and (3) whether the content was wholly provided by another 'information content provider'.* "[160] First, the case law extended the objective scope of Section 230 from "*publication-related claims, such as defamation, […] to all claims not explicitly excluded in the statute*."[161] Second, regarding the subjective scope, the concept of "provider" was interpreted, "*expansively to include virtually any service available through the Internet*."[162] Consequently, digital actors "*have been protected from liability even though they republished content knowing it might violate the law, encouraged users to post illegal content, changed their design and policies to enable illegal activity, or sold dangerous products*."[163]

381. Limit: active digital actors. Nevertheless, later US case law carved an exception to this immunity, applying to cases in which digital actors "*played a significant role in the creation or development of the allegedly harmful content*."[164] One of the first approaches[165] was close to the criminal principle of culpability but was difficult to prove:

---

[156] J. Bossan, "Le droit pénal confronté à la diversité des intermédiaires de l'internet," *op. cit.* note 155, p. 297
[157] *Ibid.* p. 298
[158] US District Court, E.D. Virginia, Alexandria Division, *Zeran v. America Online, Inc.*, March 21, 1997, *958 F. Supp. 1124*
[159] M.R. Bartels, "Programmed Defamation: Applying Sec. 230 of the Communications Decency Act to Recommendation Systems," *Fordham Law Review*, 2020, vol. 89, no. 2, p. 660
[160] *Ibid.*; C. Ziniti, "Optimal Liability System for Online Service Providers," *op. cit.* note 155, p. 586
[161] C. Ziniti, "Optimal Liability System for Online Service Providers," *op. cit.* note 155, p. 587
[162] E. Goldman, "An Overview of the US' Section 230," *op. cit.* note 115, p. 158
[163] D. Citron, B. Wittes, "The Problem Isn't Just Backpage: Revising Section 230 Immunity," *Georgetown Law Technology Review*, July 1, 2018, vol. 2, no. 2, p. 463
[164] C. Omer, "Intermediary Liability for Harmful Speech: lessons from abroad," *Harvard Journal of Law & Technology*, 2014, vol. 28, no. 1, p. 302
[165] US Court of Appeals, Ninth Circuit, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, June 27, 2005, *125 S. Ct. 2764*

The digital actor must facilitate a service with "*the primary and intentional purpose to share [illegal content] without permission*."[166] This criterion would not fit advertisement websites, since they are usually not created for the primary purpose of advertising trafficked victims. Accordingly, the main approach[167] considered a narrow exception to immunity if the digital actor "*created, or co-developed, the specific illegal aspects of third-party content*."[168] On the contrary, this argument is not available when neutral functions are available to both bad actors and users.[169] This exception could have applied, for instance, if advertising websites had offered a criterion of research to look for minors, which was not the case.[170] Similarly, a later 2023 decision by the US Supreme Court stated that "*a platform [should have] consciously and selectively [chosen] to promote content provided by*" an offender to be qualified as aiding or abetting, meaning, as active, and, thus, it was not covered by the exemption.[171] Therefore, despite this case law limiting the immunity regime, the statute would still apply to digital actors for civil liability, since it does not apply to human trafficking federal prosecutions.

382. Interpreting the "knowledge" and "passivity" of hosting service providers. A similar broadening trend was developed by the CJEU.[172] In its first case

[166] A.R. Perer, "Policing the Virtual Red Light District: A Legislative Solution to the Problems of Internet Prostitution and Sex Trafficking," *Brooklyn Law Review*, 2012, vol. 77, no. 2, pp. 835-837

[167] US Court of Appeals, Ninth Circuit, *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, April 3, 2008, no. 04-56916, 04-57173, *521 F.3d 1157*: The way the website was designed and its categories of research allowed housing discrimination. See also US Court of Appeals, Tenth Circuit, *Federal Trade Commi. v. Accusearch Inc.*, June 29, 2009, no. 08-800, *570 F.3d 1187*, in which the website was created to illegally obtain data. The Ninth Circuit has been extending this interpretation to the indirect design of a social media, considered as developer and thus not immune, by their algorithm, leading to discrimination in targeted advertisement, US Court of Appeals, Ninth Circuit, *Vargas v. Facebook, Inc.*, June 23, 2023, no. 21-16499, *3:19-cv-05081-WHO*; E. Goldman, "Uh-Oh, the Ninth Circuit Is Messing Again With Its Roommates Ruling-Vargas v. Facebook," *Technology & Marketing Law Blog*, June 26, 2023, online https://blog.ericgoldman.org/archives/2023/06/uh-oh-the-ninth-circuit-is-messing-again-with-its-roommates-ruling-vargas-v-facebook.htm (retrieved on June 26, 2023)

[168] M.R. Bartels, "Programmed Defamation," *op. cit.* note 159, p. 661. This approach is named the "material contribution" test, H. Tripp, "All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims," *Penn State Law Review*, 2019, vol. 124, no. 1, p. 243

[169] US Court of Appeals, Second Circuit, *Herrick v. Grindr LLC*, March 27, 2019, no. 18-396

[170] The courts also developed an exception based on contractual liability when a website manifested its intention to remove certain publications, but then the liability came from the lack of execution of the contract and not from a criminal liability, US Court of Appeals, Ninth Circuit, *Barnes v. Yahoo!, Inc.*, June 22, 2009, no. 05-36189, *570 F.3d 1096 (2009)*; A.R. Perer, "Policing the Virtual Red Light District," *op. cit.* note 166, pp. 833-834

[171] US Supreme Court, *Twitter, Inc. v. Taamneh et al.*, May 18, 2023, no. 21–1496, p. 26; US Supreme Court, *Gonzalez, et al. petitioners v. Google LLC*, May 18, 2023, no. 21–1333

[172] It must be noted that, in parallel, the ECHR is also developing a case law on online intermediaries' liability, P. Korpisaari, "From Delfi to Sanchez – when can an online communication platform be

law in 2010,[173] the CJEU mixed the criterion of "knowledge" with technical passivity: As soon as a hosting digital actor does not have an active role regarding the data[174], but only a mere technical role, it does not have knowledge of the data's illegality. It is the "'storage but no knowledge" test, through a neutrality requirement.[175] This blank immunity was put into perspective through a thoughtful solution[176] the following year.[177] The court excluded the need for actual knowledge of the content:[178] As soon as the digital actor has an active role, apparent knowledge is enough to exclude its immunity.[179] The digital actor can establish the terms and conditions of its service without triggering its liability,[180] but if these conditions lead to optimizing the offers, promoting the illicit offer, or permitting its customers to do so,[181] then the digital actor "*played an active role*."[182] This interpretation would facilitate defeating the immunity of advertising services, but only in the case of managing the advertisements and selecting or promoting ones linked to trafficked victims. However, it questions the principle of culpability and the level of intent: This promotion could result from the unintended functioning of an algorithm or from moderators that might not have identified the illegality of the content. Through this case law and a broad concept of "intermediary," the CJEU extended the immunity regime of hosting services to a wide range of digital

responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act," *Journal of Media Law*, Routledge, November 24, 2022, vol. 0, no. 0, p. 17

[173] CJEU, *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA (C‑236/08), Google France SARL v. Viaticum SA and Luteciel SARL (C‑237/08), Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin and Tiger SARL (C‑238/08)*, March 23, 2010, C‑236/08 to C‑238/08

[174] E. Stella, "Synthèse - Activités internet," *JurisClasseur Communication*, LexisNexis, September 24, 2020, p. 2; C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 41, in particular, this active role is not triggered by being a paid service, also underlined in CJEU, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, September 15, 2016, C-484/14

[175] P. Valcke, A. Kuczerawy, P.-J. Ombelet, "Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 107

[176] L. Costes, *Le Lamy, droit du numérique: guide : solutions et applications, pratique contractuelle*, Wolters Kluwer France, 2020, ¶ 2395; C. Castets-Renard, "Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet," *op. cit.* note 20, p. 827

[177] CJEU, *L'Oréal SA and others v. eBay International AG*, July 12, 2011, C-324/09

[178] Which obviously triggers the liability of the digital actor. It was explicitly acknowledged for a newspaper publishing company's online version of its articles: in that case, it had actual knowledge of its content, which was not third-party content, CJEU, *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis*, September 11, 2014, C-291/13

[179] P. Valcke, A. Kuczerawy, P.-J. Ombelet, "Did the Romans Get It Right?," *op. cit.* note 175, p. 108

[180] L. Costes, *Le Lamy, droit du numérique*, *op. cit.* note 176, ¶ 2397

[181] Extended in CJEU, *Coöperatieve Vereniging SNB-REACT U.A. v. Deepak Mehta*, August 7, 2018, C-521/17, underscoring that it must be checked by national courts, C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 45

[182] C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 44

actors[183] that had been considered intermediaries, such as "*an Internet access provider, a social network, and an auction platform, an operator of an open wireless, a landlord of stalls*."[184] Also included were those that had been considered hosting services, such as Internet referencing service providers,[185] online marketplaces,[186] providers of an IP address rental and registration service allowing the anonymous use of Internet domain names,[187] and websites such as Airbnb.[188]

383. Restricting the "knowledge" criterion. However, in 2021,[189] it appears that the CJEU returned to its previous case law. It is broadly known that YouTube optimizes its platform, and according to the prior case law, it could have had apparent knowledge of all of its content. Although the court adheres to its criteria of "apparent knowledge" and "neutrality,"[190] it considers that the implementation of technological measures aimed at detecting copyright infringements does not trigger the active role of the digital actor.[191] The knowledge that a digital actor could be or is used for illegal purposes is not enough to trigger the knowledge criterion; the digital actor must have knowledge of a specific infringing content.[192] The automatic indexation and recommendation systems used by digital actors are not sufficient to trigger their active role.[193] On the contrary, national judges should consider internal investigations and substantial notifications.[194] This solution was applied to video content in joint interpretation with

[183] E. Arroyo Amayuelas, "La responsabilidad de los intermediarios en internet ¿puertos seguros a prueba de futuro?," *Cuadernos Derecho Transnacional*, 2020, vol. 12, no. 1, ¶¶ 5, 8
[184] M. Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?*, Cambridge University Press, Cambridge Intellectual Property and Information Law, 2017, pp. 89-90
[185] CJEU, *Google v. Vuitton*, *op. cit.* note 173
[186] CJEU, *L'Oréal v. eBay*, *op. cit.* note 177
[187] CJEU, *SNB-REACT*, *op. cit.* note 181
[188] CJEU, *Airbnb Ireland UC*, December 19, 2019, C- 390/18; N. Mallet-Poujol, "Chronique - Droit de l'Internet," *La semaine juridique Entreprise et affaires*, January 14, 2021, no. 2, p. 26; E. Cruysmans, "Airbnb, un service de la société de l'information," *Les Pages : obligations, contrats et responsabilités*, 2020, vol. 2020, no. 71, p. 3
[189] CJEU, *Frank Peterson v. Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH (C-682/18), and Elsevier Inc. v. Cyando AG (C-683/18)*, June 22, 2021, C-682/18 and C-683/18
[190] *Ibid.* ¶¶ 104, 106
[191] *Ibid.* ¶ 109
[192] *Ibid.* ¶¶ 111-113
[193] *Ibid.* ¶ 114
[194] *Ibid.* ¶¶ 115-116. Limiting the case of knowledge to almost only accurate notifications is not consistent with the Spanish interpretation of the law. Indeed, the law considers that the digital actor has knowledge of the illegal content when a competent organ has resolved on the illegality of the data, meaning, a judicial or administrative decision. However, the Tribunal Supremo considers that it cannot be the only case of knowledge for digital actors, Tribunal Supremo. Sala Primera, de lo Civil, de Diciembre de 2009, no. 773/2009; Tribunal Supremo. Sala Primera, de lo Civil, May 18, 2010, no. 316/2010; M. Ortego Ruiz, *Prestadores de servicios de Internet y alojamiento de contenidos ilícitos*, Reus, Colección de propiedad intelectual, 1st ed., 2015, pp. 42-47; P. Chaparro Matamoros, "La responsabilidad de los prestadores de servicios de la sociedad de la información," *in* L. Martínez Vázquez de Castro, P. Escribano Tortajada (eds.), *Internet y los derechos de la personalidad: la*

the Copyright Directive,[195] and it remains to be seen what happens next. The application of this interpretation restricts the liability of digital actors, closing the gap with US law: Even when moderating or implementing a semi-active role, particularly through automatic means, the knowledge of digital actors is not triggered. This interpretation also closes the gap with the intent of the offense of human trafficking, but creates a double set of conditions to trigger digital actors' criminal liability.

384. Protecting private initiatives: the Digital Services Act. This latest solution of the CJEU was formally adopted in part by the Digital Services Act. The text created additional detail regarding digital actors' liability regime. These actors can still be immune, and the "knowledge" criterion will not be met "*solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content*."[196] This provision creates a Good Samaritan principle, close to the mindset of the United States' Section 230: It seeks to incentivize digital actors to moderate their content by excluding the application of the "knowledge" criterion in these cases.[197] Moderating content does not, by default, create knowledge for the digital actor. However, as its interpretation remains to be developed, scholars argue that the "*threshold test of knowledge/control seems liable to increase legal uncertainty regarding the liability exemption for hosting service providers*."[198] Indeed, "*there is doubt about how these standards would be implemented effectively and uniformly in practice. Hence, the framework on voluntary mechanisms should not be considered*

protección jurídica desde el punto de vista del derecho privado, Tirant lo Blanch, Homenajes y congresos, 2019, pp. 99-142. Differently in France, such notification of content, when substantial, meaning, listing the legally-required information, creates a presumption of knowledge, Article 6.I.5 of the Loi pour la confiance dans l'économie numérique. A similar presumption is included in Article 16.3 of the Digital Services Act.

[195] Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market

[196] Article 7 of the Digital Services Act

[197] C. Busch, "Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation Special Issue: Governing the Digital Space," *UCLA Journal of Law and Technology*, 2022, vol. 27, no. 2, p. 54; J. Barata, "Obligations, Liabilities and Safeguards in Content Moderation," *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, March 2, 2021, online https://intr2dok.vifa-recht.de/receive/mir_mods_00010155 (retrieved on November 27, 2021)

[198] M. Peguera, "The Platform Neutrality Conundrum and the Digital Services Act," *International Review of Intellectual Property and Competition Law*, May 1, 2022, vol. 53, no. 5, p. 683

complete."[199]

385. Although the case law attempted to limit at some points the immunity from liability of digital actors, it is quite narrow or unstable, with the judges vacillating between the priorities of hard sovereignty and economic sovereignty. The latter still seems predominant, but this extension of immunity and the mere concept of immunity for digital actors raise numerous concerns.

A. An immunity criticized worldwide

386. Paradox of digital actors' liability. The US liability regime for digital actors "*provides the strongest and most unconditional form of immunity*."[200] It appears that the interpretation of the European framework is heading toward a similar broad extension of the immunity, with the liability of hosting services being considered an "*empty shell*."[201] This evolution could handle the criminal requirement of intent when prosecuting human trafficking. However, digital actors do not have a consequent legal incentive to detect content related to this offense:[202] Modifying a website's architecture might be considered an active role or as obtaining knowledge of the crime. Due to the impossibility of perfect enforcement, these digital actors would become liable for any content linked to human trafficking that escaped their control. In the United States, immunity applies even when the digital actors knowingly host sex trafficking content, as long as their architecture is not designed specifically for this purpose.[203] Therefore, it reduces the "*responsibility and culpability for websites that […] facilitate […] sex*

[199] B. Genç-Gelgeç, "Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies?," *Croatian Yearbook of European Law and Policy*, November 16, 2022, vol. 18, p. 44

[200] G. Dinwoodie, "Who are Internet Intermediaries?," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 45. It must be noted that some authors consider that the Communications Decency Act was meant to limit access to explicit material (pornography in particular), by allowing digital actors to moderate without triggering their liability. They argue that this broad interpretation does not fit with this objective of the law, considering that the immunity should only apply to "*providers […] engaged in good faith efforts to restrict illegal activity*," D. Citron, B. Wittes, "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity," *Fordham Law Review*, November 1, 2017, vol. 86, no. 2, pp. 403, 416; M. Graw Leary, "The Indecency and Injustice of Section 230 of the Communications Decency Act," *Harvard Journal of Law & Public Policy*, 2018, vol. 41, no. 2, p. 581

[201] S. Stalla-Bourdillon, "Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 288

[202] For a similar argument applied to supply chains, see L. Ezell, "Human Trafficking in Multinational Supply Chains: A Corporate Director's Fiduciary Duty to Monitor and Eliminate Human Trafficking Violations," *Vanderbilt Law Review*, 2016, vol. 69, no. 2, p. 517

[203] M. Graw Leary, "The Indecency and Injustice of Section 230," *op. cit.* note 200, p. 556

trafficking."[204]

387. Internet's evolution. However, digital actors' liability regimes are suffering from global criticism. First, while some digital actors nowadays have a global presence and, at the very least, an economic power, "*simple risk allocation is unfeasible*" for many small or new digital actors.[205] Second, a period of innovation allowed the multiplication of technical solutions. Consequently, since the introduction of the legal frameworks more than 20 years ago,[206] "*the Internet has changed tremendously*"[207] and the frameworks are "*outdated*."[208] Perhaps Web 2.0[209] does not need the "*parental controls*"[210] of its early days, which can be "*extremely convenient for tech giants*."[211] Third, the statutes are based on the traditional digital environment and do not integrate new actors and recent architectures of the Internet.[212] Fourth, authors underline the lack of consistency in the interpretation of these statutes. To protect economic sovereignty, these statutes were meant to create legal security, but the current case law no longer fulfills that requirement.[213] In particular, both in the United States and in the EU, the statutes leave a broad margin of appreciation to the states: The exceptions to the American regime still rely strongly on the individual state laws,[214] and while the

[204] H.C. Halverson, "The Communications Decency Act," *op. cit.* note 116, p. 10
[205] S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries," *op. cit.* note 114, p. 12. For instance, the EU sets leveled obligations depending on the kind and size of digital actors in the Digital Services Act, see *infra* 0.
[206] D. Citron, B. Wittes, "The Internet Will Not Break," *op. cit.* note 200, p. 411
[207] C. Ziniti, "Optimal Liability System for Online Service Providers," *op. cit.* note 155, p. 589; C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 48
[208] G.N. Yannopoulos, "The Immunity of Internet Intermediaries Reconsidered?," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 47
[209] M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique*, Michalon Editions, 2010, p. 307
[210] E. Carney, "Protecting Internet Freedom at the Expense of Facilitating Online Child Sex Trafficking: An Explanation as to Why CDA's Section 230 Has No Place in a New NAFTA," *Catholic University Law Review*, 2019, vol. 68, no. 2, p. 375
[211] F. Stjernfelt, A.M. Lauritzen, *Your post has been removed: tech giants and freedom of speech*, SpringerOpen, 2020, p. 167
[212] S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries," *op. cit.* note 114, p. 7; A. Lampe, "De la difficile qualification des sites collaboratifs aux limites du statut d'hébergeur prévu par la LCEN," *Revue Lamy Droit de l'Immatériel*, June 1, 2008, no. 39. For instance, the E-Commerce Directive was not considering search engines (but they are included in the Digital Services Act), R. Boos, *La lutte contre la cybercriminalité au regard de l'action des États*, Thesis, Université de Lorraine, 2016, ¶ 333. Similarly, for more remote "*network intermediaries (e.g. related to provision of domain names and domain name-related services, IP addresses, client software, etc.)*," S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries," *op. cit.* note 114, p. 27.
[213] For instance, on the notion of "development" of information in the United States, M.R. Bartels, "Programmed Defamation," *op. cit.* note 159, p. 667
[214] C. Ziniti, "Optimal Liability System for Online Service Providers," *op. cit.* note 155, p. 605.

Digital Services Act replaces the E-Commerce Directive, the content of the regime has barely changed and, thus, is open to interpretation.[215] Specifically, the inconsistencies in interpreting the "knowledge"[216] and "intermediary"[217] criteria are the targets of frequent criticism.

388. Economic development *versus* moral duty. These frameworks, particularly the American one, have been summarized as follows: "*You have the right, but not the responsibility*."[218] Then, "*it has produced unjust results*."[219] In the EU, the only responsibility is to expeditiously take down the known content, which is not specific enough to offer a proper way for the state to impose its sovereign control. Today, common sense, users,[220] and the literature are usually in favor of imposing further liability on digital actors in response to a sort of moral duty toward the online world.[221] The current immunity regimes are seen as a "*gift*," while they should be a reward associated with public obligations,[222] which could include the incorporation of digital actors in the repression of cyber human trafficking.

389. Conclusion of the section. Corporate criminal liability is increasingly broadened to control corporations through states' hard sovereignty. However, the offense of human trafficking hardly fits its criteria in terms of actors facilitating the phenomenon without being directly or knowingly involved in it. Nevertheless, as soon as these actors are knowingly helping to commit a crime, criminal law could be triggered through complicity. Regarding digital actors, a second level of criteria must be verified. In privileging economic sovereignty, states offer broad immunity to digital

---

[215] And the broad immunity can be seen as inconsistent with other more recent law that "*imposed contradicting obligations to the providers, who are called to observe the rules, while bearing the often demanding compliance costs*," G.N. Yannopoulos, "The Immunity of Internet Intermediaries Reconsidered?," *op. cit.* note 208, p. 47. In particular regarding copyright infringements, J. McNamee, M. Fernández Pérez, "Fundamental Rights and Digital Platforms in the European Union: a Suggested Way Forward," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 102

[216] M. Husovec, *Injunctions against Intermediaries in the European Union*, *op. cit.* note 184, p. 53; C. Angelopoulos, S. Smet, "Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability," *Journal of Media Law*, Routledge, December 6, 2016, vol. 8, no. 2, p. 275; S. Stalla-Bourdillon, "Internet Intermediaries as Responsible Actors?," *op. cit.* note 201, pp. 278-288

[217] For instance, Uber was excluded from the scope of this directive, CJEU, *Asociación Profesional Elite Taxi v. Uber Systems Spain SL*, December 20, 2017, C- 434/15; CJEU, *Uber France SAS*, April 10, 2018, C- 320/16, underlining the difficulties "*to qualify the main activities of those platforms*," C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 4

[218] F. Stjernfelt, A.M. Lauritzen, *Your post has been removed*, *op. cit.* note 211, p. 167

[219] D. Citron, B. Wittes, "The Problem Isn't Just Backpage," *op. cit.* note 163, p. 468

[220] T. Gillespie, "Platforms Are Not Intermediaries," *op. cit.* note 121, p. 207

[221] A.R. Perer, "Policing the Virtual Red Light District," *op. cit.* note 166, p. 832

[222] T. Gillespie, "Platforms Are Not Intermediaries," *op. cit.* note 121, pp. 213-215

actors for online content linked to human trafficking, even when they effectively know about it in the United States. This raises a question about the need to reform the statutes: In the United States, they do not apply when prosecuting federal crimes, including human trafficking. However, states have reformed and are willing to refine these regimes to better repress human trafficking and restate their hard sovereignty over digital actors.

Section 2. From hard sovereignty to extended criminal policy

390. According to law enforcement authorities, scholars, and activists, corporate criminal liability and digital actors' liability make it difficult to prosecute websites that facilitate cyber human trafficking. However, hard sovereignty could still be applied when examining the conditions established by law, that are designed to protect criminal law principles and the legitimacy of the state's coercion. While traditional legitimacy is grounded in positive validity depending on the superior norm, current liberal states also attribute the legitimacy of law to its effectiveness.[223] Legitimacy can include a pragmatic perspective through the applicability and application of norms. Despite the implementation of the law rarely being perfect, its "*empirical validity*" must be considered.[224] To resolve these problems of the applicability of criminal liability to digital actors for human trafficking, the United States amended both this offense and digital actors' immunity. However, the amendments do not appear to improve the fight against the phenomenon (§1). Nevertheless, the United States and France have obtained the closure of specific sections or websites used to advertise trafficked victims. These "sanctions" were not based mainly on hard sovereignty but on a broader interpretation of states' criminal policies, using a new type of social control that questions its legitimacy. Criminal policy is "*a strategy to respond to the criminal phenomenon that includes deviant and delinquent behavior. Criminal policy shifts disciplinary boundaries; in fact, it is multidisciplinary and transdisciplinary*."[225] By going beyond the framework of the state, this criminal policy can be considered extended

[223] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016, p. 60
[224] M. Delmas-Marty, *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit no. 1, 2004, p. 194
[225] C. Lazerges, "Des modèles de politique criminelle aux mouvements et systèmes de politique criminelle," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, vol. 3, no. 3, p. 533

(§2).

§1. Questioning the necessity of broadening hard sovereignty

391. The American difficulties of prosecuting digital actors for human trafficking led to amendments of both criminal law and digital actors' liability, whose attractiveness outgrew the borders of the country. They were meant to strengthen hard sovereignty by facilitating the conviction of digital actors for trafficking. However, their applicability is still highly questioned (I). Furthermore, the prosecution policies and realities challenge the necessity of the amendments (II).

I. Criticized amendments: extension of human trafficking and exception to immunity

392. Extending human trafficking. Authors have criticized the lack of "*a specific corporate liability statute*"[226] regarding human trafficking. Nevertheless, as already studied, the problem lies mainly in its definition, which hardly fits with the actions (not) committed by websites hosting content linked to trafficking. Thus, the United States extended the definition of sex trafficking[227] by passing, in 2015, the Justice for Victims of Trafficking Act. This act first lessened the intent requirement by triggering liability when a person acts in reckless disregard;[228] second, it added the verb "to advertise,"[229] which is designed to trigger the liability of advertisement websites. However, these provisions adapt the definition to only one possibility of using digital actors to facilitate trafficking. Additionally, the extended intent is not applicable to this action. Digital actors, through their agents, must know that they are advertising content linked to trafficking,[230] which might not be the case. A few years later, the United States passed

[226] S.C. Pierce, "Turning a Blind Eye," *op. cit.* note 6, p. 594. In the 2022 Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, the corporate criminal liability framework is not modified.
[227] 18 USC § 1591.a
[228] Section 108 of the Justice for Victims of Trafficking Act of 2015. Morever, it adds the verbs "to patronize" and "to solicit" within the offense actions. However, these modifications are meant to clarify the possibilities to convict persons using the services of trafficked victims, Section 109
[229] Section 118 of the Justice for Victims of Trafficking Act of 2015, adopting a 2014 proposed amendment, the Stop Advertising Victims of Exploitation (SAVE) Act. A similar extension has already been implemented by the states of Washington, Tennessee and Connecticut, limited to the advertisement of minor victims, but all of them were repealed, R. Dalton, "Abolishing child sex trafficking on the internet: Imposing criminal culpability on digital facilitators," *University of Memphis Law Review*, 2013, vol. 43, no. 4, pp. 1114-1121
[230] A.W. Balfour, "Where One Marketplace Closes, (Hopefully) Another Won't Open: In Defense of FOSTA," *Boston College Law Review*, 2019, vol. 60, no. 8, p. 2489

the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA).[231] First, this act clarifies the second definition of sex trafficking, meaning benefiting from participation in a venture committing the acts of trafficking.[232] Section 5 defines "participation in a venture" as "*knowingly*[233] *assisting, supporting, or facilitating*" the commission of trafficking. Since the intent is not reduced, its applicability to advertisement websites seems jeopardized. Second, it creates a new offense:[234] the promotion or facilitation of prostitution and the reckless disregard of sex trafficking.[235] According to the new statute, "*Whoever […] owns, manages, or operates an interactive computer service […], or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person and […] acts in reckless disregard of the fact that such conduct contributed to sex trafficking […] shall be fined under this title, imprisoned for not more than 25 years,*[236] *or both*." This provision was created to trigger "*criminal and civil liability for website owners and managers*"[237] and to lower the intent required in the offense of sex trafficking.[238]

393. Comparisons and propositions abroad. These extensions of the sex trafficking definition are growing closer to the broad interpretation of the offense of pimping in France.[239] Prior to the introduction of the human trafficking offense, case law convicted newspapers and electronic services for pimping when they knowingly advertised sexual services.[240] In Spain, the definition of pimping is more restrictive, but

[231] It came into effect in April 2018.
[232] 18 USC § 1591.a.2
[233] The intent could be seen as being in accordance with the case law interpretation that refused to consider the "*mere negative acquiescence*" of a person, US Court of Appeals, Sixth Circuit, *United States v. Afyare*, *op. cit.* note 85. However, when interpreting this concept, the court required that "*The actor must have been one of two or more people engaged in sex trafficking together, and the actor must have participated in a way that furthered the trafficking*," questioning then what kind of actions the author should have committed to fit within the new definition, K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1120-1124
[234] That is however not included in Chapter 77 on trafficking in persons but in Chapter 117 on transportation or illegal sexual activity.
[235] 18 USC § 2421A, introduced in Section 3 of FOSTA
[236] By comparison, the commission of sex trafficking is punished by "*imprisonment for any term of years not less than 15 or for life*" when victims are adults or minors of 14 years old, and by "*imprisonment for not less than 10 years or for life*" when victims are minors of 18 years old, 18 USC § 1591.b
[237] C. Burnitis, "Facing the Future with FOSTA: Examining the Allow States and Victims to Fight Online Sex Trafficking Act of 2017," *University of Miami Race and Social Justice Law Review*, 2020, vol. 10, no. 2, p. 150
[238] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, p. 1147; A.W. Balfour, "In Defense of FOSTA," *op. cit.* note 230, pp. 2489-2490
[239] Articles 225-5 and 225-6 of the Code pénal
[240] For instance, was convicted the director of a free newspaper including publication of sexual services under the heading "Relaxation," Cour de Cassation, Chambre criminelle, October 9, 1996, no. 95-81232 ; the company owning an advertisement website including ads for sexual services, Cour de Cassation, Chambre criminelle, October 25, 2000, no. 00-80829 ; and the "*manager of a minitel server*

some studies in the literature also advocate for this expansion. A proposed amendment[241] wishes to criminalize the act of providing a place for the commission of sexual services for profit and in a habitual manner. It was argued that this should be further extended to advertisement websites that benefit from sexual services advertisements.[242] In the United Kingdom, various similar amendments were proposed, but not accepted, in the process of passing the 2022 Police, Crime, Sentencing, and Courts Act;[243] further amendments are under negotiations on this topic in the draft of the Online Safety Bill.[244]

394. Drawbacks of the amendments. However, American amendments, particularly FOSTA, are not exempt from criticism. First, the language used to define the participation in a venture and the new offense is considered "*too broad*"[245] and "*unclear*,"[246] especially due to its various definitions at the state level.[247] The new offense groups "prostitution" with "sex trafficking," creating confusion about what is

center, who largely favored, with full knowledge of the facts, an abundant prostitution network from which he made considerable profits," Y. Mayaud, C. Gayet, *Code pénal: annoté*, Dalloz, Codes Dalloz, 120th ed., 2022, arts. 225-5

[241] Anteproyecto de Ley Orgánica para la garantía integral de la libertad sexual of 2021. For a short analysis, see P. Lloria García, "La protección integral de la libertad sexual," *Agenda Pública*, June 7, 2022, online https://agendapublica.elpais.com/noticia/18033/proteccion-integral-libertad-sexual (retrieved on June 10, 2022)

[242] T. García Sedano, "La tercería locativa: obligaciones, retos y riesgos," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2022, no. 156, p. 4

[243] One was dedicated to creating an offense of arranging or facilitating the request and acceptance of "*sexual relations as a condition of accommodation*," intended to "*capture, for example, publishers or hosts of advertisements for such arrangements*," House of Commons, Police, Crime, Sentencing and Courts Bill (Amendment Paper), United Kingdom, June 16, 2021 amendment NC64. The amendment was weirdly limited to a very specific kind of payment for sexual relations. A second one was meant to create an offense for advertising content linked to commercial sexual exploitation, *Ibid.* amendment NC78. However, "*Laws against "incitement for the purposes of prostitution" (section 52 of the 2003 UK Sexual Offences Act) prevent workers from advertising, but also from offering advice to each other, threatening the very communities of safety that sex workers self-organize*," K. Hardy, C. Barbagallo, "Hustling the Platform: Capitalist Experiments and Resistance in the Digital Sex Industry," *South Atlantic Quarterly*, Duke University Press, July 2021, vol. 120, no. 3, p. 545

[244] R. Keighley, T. Sanders, "Prevention of modern slavery within sex work: Study protocol of a mixed methods project looking at the role of adult services websites," *PLOS ONE*, May 18, 2023, vol. 18, no. 5, pp. 2-3

[245] A.W. Balfour, "In Defense of FOSTA," *op. cit.* note 230, p. 2500; H. Tripp, "All Sex Workers Deserve Protection," *op. cit.* note 168, p. 235; L. Chamberlain, "FOSTA: A Hostile Law with a Human Cost," *Fordham Law Review*, 2019, vol. 87, no. 5, p. 2196. The latter author recalls arguments of defenders of FOSTA, considering that the act is limited to "speech that directly seeks to advertise sexual services for pay," but the interpretation of the statute remains to be seen, *Ibid.* p. 2194

[246] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, p. 1133

[247] On the diversity of the definitions in the United States, see C. Branscum, C.M. Cain, S.W. Fallik, "Exploring the Nature of Anti-trafficking Laws: A Content Analysis of State Statutes," *Journal of Human Trafficking*, Routledge, July 3, 2023, vol. 9, no. 3, pp. 348-362. This problem of multiple definitions is also applicable for the notion of "prostitution," only vaguely defined by the case law, K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1105, 1148

targeted and potentially focusing on legal sex work.[248] The lack of clarity of the new statute increases with its first interpretation: "*It is possible to interpret § 2421A as proscribing not only acting with the intent to promote a specific unlawful act of prostitution, but also acting with the intent to 'facilitate prostitution by providing sex workers and others with tools to ensure the receipt of payment for sexual services'.*"[249] Additionally, "facilitating" and "promoting" should be interpreted as synonyms to "aiding" and "abetting" for the former and "pandering" and "pimping" for the latter.[250] Moreover, the new requirements regarding the intent complicate the interpretation and proof of the offense.[251] The main actions must be committed intentionally, with knowledge of the means and the purpose.[252] Furthermore, the new definition of "participation in a venture" adds a third component of knowledge regarding the assistance, support, or facilitation of the crime.[253] This "*would likely be the most difficult element for future plaintiffs to prove*,"[254] as "*a prosecutor must prove that the shareholder knew of the violation itself*."[255] It remains to be seen what "*degree of*

[248] On this distinction, see *infra* 424 to 426. Promoting prostitution and sex trafficking might encompass, if broadly interpreted, political campaigns regarding the legal regulation of sex work, E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *Northwestern University Law Review*, 2020, vol. 115, no. 2, p. 537

[249] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1141-1146 citing US Court of Appeals, District of Columbia, *Woodhull Freedom Found. v. United States*, January 24, 2020, no. 18-5298, *948 F.3d 363*. On the contrary, the first court interpretation required "*to prove that website owners actually intended to promote or facilitate prostitution; merely proving that websites owners' recklessness or even knowledge of such activities is not enough to hold them liable*," US District Court for the District of Columbia, *Woodhull Freedom Found. v. US*, September 24, 2018, 18-cv-01552 (RJL), *334 F. Supp. 3d 185*; C. Burnitis, "Facing the Future with FOSTA," *op. cit.* note 237, p. 157. The lowered intent by the statute was again increased under this case law, in accordance with prior case law regarding the intent element linked to prostitution, which is interpreted narrowly, K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1137-1138; Court of Appeal of California, Fourth District, Division Two, *Wooten v. Superior Court*, October 30, 2001, *113 Cal. Rptr. 2d 195*

[250] US District Court, District of Columbia, *Woodhull Freedom Found. v. United States*, March 29, 2022, 18-1552 (RJL)

[251] E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 62, p. 1638

[252] However, the commission of the sex act does not have to be proven, K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1117-1118. Furthermore, the notion of "reckless disregard" is not considered the most adapted, as it leads to many questions in its implementation. The notion of "willfully blindness" has been advocated for, as it has already been widely developed by the case law, A. Miller Welborn Young, "Willful Blindness: Applying a Drug Trafficking Theory of Liability to International Human Trafficking Prosecution," *Berkeley Journal of International Law*, 2022, vol. 40, no. 1, pp. 143-170

[253] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1125-1126. The Ninth Circuit considers that it requires "*a more active degree of "participation in the venture" than a "continuous business relationship" between a platform and its users*," US Court of Appeals, Ninth Circuit, *Does 1-6 v. Reddit, Inc.*, October 24, 2022, no. 21-56293, *2022 WL 13743458*; US Court of Appeals, Ninth Circuit, *Doe v. Twitter, Inc.*, May 3, 2023, no. 22-15103, *3:21-cv-00485-JCS*

[254] E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 62, p. 1644; US Government Accountability Office, *Sex trafficking - Online Platforms and Federal Prosecutions*, US, June 2021, p. 29

[255] M. McKnelly, "Untangling SESTA/FOSTA: How the Internet's 'Knowledge' Threatens Anti-Sex Trafficking Law," *Berkeley Technology Law Journal*, 2019, vol. 34, no. 4, p. 1257. It modified the statute from "*creating an effect standard (knowingly engaging in conduct, the effect of which was to assist in a*

certainty" will be required, especially regarding the content moderation of data potentially linked to trafficking.[256] While Section 230 avoided the concept of knowledge, the new criminal statutes enhance this criterion.

395. A blank exception to immunity for sex trafficking. The second objective of FOSTA was to create a "*significant exception*"[257] to digital actors' immunity[258]. The immunity that was not applicable to the federal offense of sex trafficking. FOSTA broadens the exception to digital actors' immunity for civil claims and state prosecutions linked to a sex trafficking offense and for state prosecutions linked to the offense of reckless promotion of sex trafficking.[259] Thus, as long as they are posting content linked to sex trafficking, digital actors can be deemed liable. This situation indirectly obliges digital actors to "*proactively look for [a] possible sex trafficking violation*," since a notice-and-takedown mechanism is not enough to protect them[260] from possible prosecution. The first criticism is quite obvious: Why is this exemption limited to sex trafficking? Digital actors can facilitate human trafficking for various exploitation purposes. Section 230 remain a challenge for civil claims and state prosecutions for trafficking for other purposes, such as labor exploitation, forced begging or criminality, and organ removal. Furthermore, cybercrime, in its broad definition, encompasses all types of offenses facilitated by new technologies, from terrorism to domestic violence. These victims will be unable to claim civil damages from digital actors, and attorneys general will struggle when their action is based on state law. Such a limited amendment can be seen as a consequence of penal populism,[261] meaning "*the temptation to exorcise the great problems of society by the*

violation) to an intent standard (knowingly engaging in conduct while knowing that the conduct will assist in a violation)," K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1123-1124

[256] M. McKnelly, "Untangling SESTA/FOSTA," *op. cit.* note 255, pp. 1254-1263. The author offers to consider the case law on trademark infringement, holding that "*knowledge of violating activity as a 'general matter' was not enough to trigger a mental state of knowledge*"; on copyright infringement, actual knowledge is required, that includes receiving a takedown notice without removing it afterwards.

[257] C. Burnitis, "Facing the Future with FOSTA," *op. cit.* note 237, p. 151. However, "*the changes to section 230 are far less broad than initially reported*," K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, p. 1084

[258] Section 4 of FOSTA. Since 2012, one author has offered a proposition to modify Section 230: "*Classified-ads websites would be liable for unlawful sex postings by third parties if the websites were notified about the postings but took no steps to remove the postings, because they would then become distributors that knowingly distribute illegal content*," A.R. Perer, "Policing the Virtual Red Light District," *op. cit.* note 166, pp. 825, 847

[259] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1100-1101

[260] T. Gillespie, "Platforms Are Not Intermediaries," *op. cit.* note 121, p. 208

[261] As defined by Salas, "*Penal populism characterizes any speech that calls to punish in the name of the scorned victims and against the disqualified institutions*," which fits perfectly with the development of the Craigslist and Backpage cases, D. Salas, *La volonté de punir : essai sur le populisme pénal*,

only legal prohibition,"[262] or by eliminating an immunity.

396. Applicability of the new Section 230. The immunity is plainly excluded, without conditions. Due to this broad exception, its applicability in practice is questioned. First, well-known digital actors could take action to control their content, "*to accommodate new regulatory obligations in ways that new entrants cannot*," consequently favoring "*marketplace dominance*."[263] This risk is increased as Section 230 refers to the states' definition of offenses linked to sex trafficking, multiplying the possible violations committed by digital actors for the content they host without even having knowledge of it.[264] Second, to ensure that no content is linked to sex trafficking in any possible way, digital actors might be prompted to moderate their content even further than explicit advertisements of sexual services that potentially cast trafficked victims.[265] Indeed, a manual review of all content from an anti-trafficking perspective is not possible, nor is it achievable to leave this task to artificial intelligence. Therefore, "*the least resource intensive [approach] and the most likely to effectively preclude liability*" would be to "*steer clear of all such topics entirely*."[266]

397. Foreign proposition: France. Despite these drawbacks, steps toward modifying the liability of digital actors for sex trafficking were attractive to various countries. Since 2011, concerns have been raised in France about the (not only) legal difficulties of establishing the liability of hosting actors.[267] For now, the trend in the EU is not to modify the liability of digital actors but to establish new obligations, including monitoring and removing content.[268] In France, digital actors "*must contribute to the*

Hachette littératures, 2008. Salas highlights that the use of penal populism is particularly true for sexual crimes, in which sex trafficking could be included, *Ibid.* p. 81

[262] D. Salas, *La volonté de punir*, *op. cit.* note 261

[263] E. Goldman, "An Overview of the US' Section 230," *op. cit.* note 115, p. 163

[264] E. Goldman, *Balancing Section 230 and Anti-Sex Trafficking Initiatives - Hearing on "Latest Developments in Combating Online Sex Trafficking" - Written Remarks*, *op. cit.* note 116, p. 5

[265] L. Chamberlain, "FOSTA: A Hostile Law with a Human Cost," *op. cit.* note 245, p. 2189. On that specific topic and the actual consequences of FOSTA, see *infra* Part 2. Title 1. Chapter 1. Section 2.

[266] *Ibid.* pp. 2197-2198

[267] G. Geoffroy, *Rapport d'information sur la prostitution en France*, no. 3334, Assemblée Nationale, France, April 13, 2011, p. 271. Regarding extra-legal challenges, the report considers the localization abroad of servers, and their possible quick disappearance.

[268] In particular, specific content such as child pornography, Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, Article 25; copyright infringements, Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, Article 17; and terrorism, Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, Article 21, and Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online

fight against the dissemination" of a list of offenses, including human trafficking, and pimping, but not to any other offenses connected to other purposes of human trafficking.[269] This obligation does not come with requirements for results or any type of liability for trafficking.[270] Therefore, the 2021 action plan against child prostitution considers the need to further examine the framework applicable to websites that hosting sexual services,[271] with a few voices reminding the critics of the equivalent FOSTA.[272]

398. To convict digital actors for trafficking, the United States broadened the scope of sex trafficking, created neighbor offenses, lowered the requirements on intent, and deleted the immunity of digital actors. However, many voices criticized the applicability of the new statutes, especially the necessity and efficiency of FOSTA were questioned due to the realities of the prosecutions.

II. The ineffectiveness of legal reforms: realities of prosecutions

399. "Corporations" prosecutions for "sex trafficking." Section 230 and corporate criminal liability have never prohibited the conviction of digital actors.[273] However, in general, few corporations are prosecuted,[274] including advertisement websites that are believed to facilitate sex trafficking.[275] Most of these few prosecutions

[269] Article 6.I.7 § 3 of the Loi pour la confiance dans l'économie numérique, introduced by the Loi n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, underlining a similar focus on sex trafficking. The list is mostly directed at sex offenses and terrorism. That could be another example of penal populism.

[270] Article 6.VI.1 of the Loi pour la confiance dans l'économie numérique nevertheless creates an offense applicable only to natural persons when they do not create a take-down mechanism or do not preserve the data.

[271] Gouvernement, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, France, November 15, 2021 action 35

[272] N. Duranton, *Rapport d'information sur les actes du colloque « Droits de l'Homme et démocratie à l'ère numérique », organisé le 14 novembre 2019, dans le cadre de la présidence française du Comité des ministres du Conseil de l'Europe*, Sénat Session ordinaire 2019-2020, 2019, pp. 88-89

[273] E. Goldman, *Balancing Section 230 and Anti-Sex Trafficking Initiatives - Hearing on "Latest Developments in Combating Online Sex Trafficking" - Written Remarks*, *op. cit.* note 116, p. 5. The Department of Justice successfully prosecuted and settled complaints with the main digital actors on the basis of other federal crimes than human trafficking, like Google, Yahoo, and Microsoft for illegal gambling ads, Google for illegal pharmacy ads, E. Goldman, "An Overview of the US' Section 230," *op. cit.* note 115, pp. 161-162. However, these examples contribute to the literature underlining the US criminal policy to favor negotiated justice instead of criminal conviction, O. Boulon, "Une justice négociée," *in* A. Garapon, P. Servan-Schreiber (eds.), *Deals de justice: le marché américain de l'obéissance mondialisée*, Presses universitaires de France, 2013, p. 41

[274] For the 2020 fiscal year, only 39 organizations were prosecuted in the United States, E. McCready, "Corporate Criminal Liability," *op. cit.* note 54, pp. 603-604

[275] In 2016, the corporation owning Rentboy was convicted, US District Court Eastern District of New York, *United States v. Easy Rent Systems, Inc.*, January 28, 2016, 16-CR-45. The criminal prosecution against Backpage is still pending after the last decision to allow for retrial, US Court of Appeals, Ninth

and convictions[276] involved natural persons. Nevertheless, since the passage of FOSTA, at least six pending prosecutions linked to advertisement websites have not charged legal persons.[277] In general, however, few corporations are prosecuted for human trafficking: In 2022, in the US federal court system, only one corporation was among 238 new defendants was charged with human trafficking, only one was a corporation.[278] In France, between 2016 and 2018, no legal person was convicted of human trafficking.[279] Furthermore, most of the prosecutions did not charge sex trafficking. The US Senate led an investigation titled "*Backpage.com's Knowing Facilitation of Online Sex Trafficking*,"[280] and when the website was taken down, the Federal Bureau of Investigation announced that "*sex trafficking will not be tolerated*."[281] However, no action was based on the sex trafficking offense.[282] Since the passage of FOSTA, of the six cases studied by the US Government Accountability Office,[283] only two have involved charges of with sex trafficking,[284] while the majority have facilitated victims' civil claims.

400. Facilitating civil claims. Convicting offenders who facilitate sex trafficking is

---

Circuit, *Plaintiff-Appellee, v. Lacey, Larkin, Spear, Brunst, Padilla, Vaught*, September 21, 2022, no. 22-10000. Craigslist was never prosecuted for federal crimes.

[276] US District Court Northern District of California, *USA v. Omuro and others*, June 24, 2014, 3:14-cr-00336

[277] US Government Accountability Office, *Sex trafficking*, *op. cit.* note 254, pp. 47-48

[278] L. Lane et al., *2022 Federal Human Trafficking Report*, Human Trafficking Institute, 2023, p. 26

[279] GRETA, "Evaluation Report - France - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, February 18, 2022, ¶¶ 105-107. Data are higher for exploitation offenses, such as pimping or unworthy working and housing conditions (convictions of nine and eleven legal persons, respectively, between 2016 and 2018).

[280] Permanent subcommittee on investigations, *Backpage*, *op. cit.* note 52

[281] Department of Justice, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment - Press Release Number: 18 - 427," *The United States Department of Justice*, April 9, 2018, online https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads (retrieved on May 23, 2022)

[282] Craigslist was considered a public nuisance, US District Court, N.D. Illinois, *Dart v. Craigslist, Inc.*, October 20, 2009, 09 C 1385, *665 F. Supp. 2d 961*. The company owning Rentboy was convicted of money laundering, the companies linked to Backpage are charged with money laundering, US Government Accountability Office, *Sex trafficking*, *op. cit.* note 254, pp. 46-47. Rentboy and Backpage were closed on the basis of the Travel Act for racketeering for promoting prostitution, 18 USC § 1952, S. Majic, "Same Same but Different? Gender, sex work, and respectability politics in the MyRedBook and Rentboy closures," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 88; L. Chamberlain, "FOSTA: A Hostile Law with a Human Cost," *op. cit.* note 245, p. 2201

[283] US Government Accountability Office, *Sex trafficking*, *op. cit.* note 254, pp. 47-48

[284] And one for the new offense created by FOSTA, 18 USC § 2421A. The latter resulted in the closure of CityxGuide and the prosecution of its owner, which "*resulted in a plea deal where the defendant pled guilty to promotion of prostitution and conspiracy to facilitate prostitution*," with no charges of sex trafficking, K. Albert, "Enough About FOSTA's 'Unintended Consequences'; They Were Always Intended," *Techdirt.*, July 29, 2021, online https://www.techdirt.com/articles/20210728/13245147264/enough-about-fostas-unintended-consequences-they-were-always-intended.shtml (retrieved on August 7, 2021)

one part of the anti-trafficking framework with the other being the protection of victims. In the United States, victims can file civil claims through independent proceedings.[285] Before FOSTA, all victims' claims failed, considering that Backpage was neither providing the advertisements nor playing an active role.[286] In particular, in 2016, a court ruled in favor of Backpage's immunity,[287] but the literature criticized that the ruling did not "*address the factual question of whether Backpage.com actually encouraged sex trafficking through its website or whether it was responsible for the development of the alleged sex traffickers' advertisements*."[288] Since FOSTA, there has been a "*rise in state-level civil actions related to trafficking*."[289] In 2021, 15 new federal civil actions were brought against websites and technology companies,[290] but FOSTA did not resolve the questions around Section 230. On the contrary, the new act "*created confusion*."[291] For some judges, immunity was still applicable in state civil actions related to sex trafficking,[292] and in this regard, a case involving sex trafficking facilitated through Facebook[293] went up before the US Supreme Court. While denying the petition

[285] 18 USC § 1595, FOSTA (Section 6) added the possibility for the attorney general of a state to also bring a civil action.

[286] US District Court Eastern District of Missouri Eastern Division, *M.A. ex rel P.K. v. Village Voice Media Holdings, LLC*, August 15, 2011, 4:10cv1740 TCM, *809 F. Supp. 2d 1041*; US District Court Western District of Washington at Tacoma, *J.S. v. Vill. Voice Media Holdings, LLC*, March 5, 2013, 3:12-cv-06031-BHS. However, in 2015, one court allowed "*a state claim to reach discovery*," underscoring that Backpage could have lost its immunity "*if the company helped develop the content through its posting rules, screening process, and content requirements*," M. Graw Leary, "The Indecency and Injustice of Section 230," *op. cit.* note 200, p. 589; Supreme Court of the State of Washington, *J.S. v. Vill. Voice Media Holdings, LLC*, September 3, 2015, no. 90510-0, *184 Wash.2d 95*; J. Raphael, "Denial of Harm," *op. cit.* note 101, p. 4. Similarly, two other decisions highlighted the possibility of excluding immunity if websites play an active role, E. Goldman, "The complicated story of FOSTA and section 320," *First Amendment Law Review*, 2019, vol. 17, pp. 287-288; US District Court Middle District of Florida Orlando Division, *Florida Abolitionist v. Backpage.com LLC*, March 31, 2018, 6:17-cv-218-Orl-28TBS; US District Court District of Massachusetts, *Doe No. 1 v. Backpage.com, LLC*, March 29, 2018, 17-11069-LTS

[287] US Court of Appeals, First Circuit, *Doe No. 1 v. Backpage.com, LLC*, March 14, 2016, no. 15-1724, *817 F.3d 12, 17*. The same year, another court considered that, despite the role of the website when moderating the post, it "*did not provide material contribution to the offensive content because its editing of an advertisement did not alter the intent of the third party*," Superior Court of the State of California, County of Sacramento, *People of the State of California v. Carl Ferrer*, November 16, 2016, no. 16FE019224, WL 7884408; M.-H. Maras, "Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?," *Journal of Internet Law*, November 1, 2017, vol. 21, no. 5, p. 20

[288] M.R. Bartels, "Programmed Defamation," *op. cit.* note 159, p. 664

[289] K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, pp. 1109-1111

[290] L. Lane, A. Gray, A. Rodolph, *2021 Federal Human Trafficking Report*, Human Trafficking Institute, 2022, p. 21

[291] B. Horton, "The Hydraulics of Intermediary Liability Regulation," *Cleveland State Law Review*, 2022 2021, vol. 70, no. 2, pp. 251-252

[292] L. Wiesner, "Good Intentions and Unintended Consequences: SESTA/FOSTA's First Two Years," *Temple Law Review*, 2021 2020, vol. 93, p. 174; US District Court, District of Oregon, *A.M v. Omegle.com*, July 13, 2022, 3:21-cv-01674-MO

[293] L. Wiesner, "Good Intentions and Unintended Consequences," *op. cit.* note 292, p. 174. The Texas court considered that Facebook was still partly immunized, but not for state civil claims, broadening the

for writ of certiorari, the court called for Congress to clarify the scope of Section 230.[294] Interestingly, the prior exception based on the active role of the digital actor is now displaced in the definition of sex trafficking. First, in 2020, a court also considered that "*general knowledge of potential trafficking was insufficient to prove [a digital actor] had knowledge or reckless disregard for the alleged sex trafficking occurring on their platform*."[295] Following case law is not consistent in the interpretation of the knowledge criterion,[296] although the Ninth Circuit Court of Appeals case law seems to confirm the requirement for a stronger proof of knowledge to apply FOSTA exception to Section 230.[297] American case law is now further struggling around the notions of "knowledge" and "active role," as the European courts are.[298]

401. Both prior and current criminal laws do not seem adapted to applying the anti-trafficking framework to digital actors. Digital actors can facilitate trafficking, but states' hard sovereignty does not seem suitable. However, despite the lack of convictions,

---

new exception, Supreme Court of Texas, *In re Facebook, Inc.*, June 25, 2021, no. 20-0434, *625 S.W.3d 80*

[294] US Supreme Court, *Doe v. Facebook, Inc.*, March 7, 2022, no. 21-459

[295] C. Martell, "Customer Transparency Can Dampen the Growing Human Trafficking Problem," *Journal of Business, Entrepreneurship and the Law*, 2021, vol. 14, no. 1, p. 61; US District Court, Southern District of California, *Doe v. KIK Interactive, Inc.*, August 31, 2020, 20-60702-CIV-SINGHAL, *482 F. Supp. 3d 1242*

[296] Twitter was not immune since it makes it difficult for users to report illegal content, it fails to properly monitor content linked to human trafficking, even not removing hashtags associated with child pornography, and its search suggestion feature makes it easier for users to find the illicit content, US District Court, Northern District of California, *Doe v. Twitter, Inc.*, August 19, 2021, 21-cv-00485-JCS, *555 F. Supp. 3d 889*; nor was MindGeek (owner of PornHub) due to its possibility to moderate, US District Court, Central District of California, *Doe v. Mindgeek US Inc.*, November 2, 2021, 8:21-cv-00338-CJC-ADS. See also US District Court, Northern District of Alabama, *Doe v. MG Freesites, Ltd.*, February 9, 2022, 7:21-cv-00220-LSC. On the contrary, when only republishing information, websites were deemed immune to civil claims, such as with Craigslist: failing to remove posts and providing neutral tools do not trigger its active role, especially considering it did not verify the age or identity of the persons, US District Court, Western District of Washington, *M.L. v. Craigslist, Inc.*, April 25, 2022, C19-6153 BHS-TLF.

[297] See US Court of Appeals, Ninth Circuit, *Does 1-6 v. Reddit, Inc.*, *op. cit.* note 253; US Court of Appeals, Ninth Circuit, *J.B. v. Craigslist, Inc.*, May 3, 2023, no. 22-15290, *4:19-cv-07848-HSG*; E. Goldman, "Defendants Get Important FOSTA Win in 9th Circuit-Doe v. Reddit," *Technology & Marketing Law Blog*, October 26, 2022, online https://blog.ericgoldman.org/archives/2022/10/defendants-get-important-fosta-win-in-9th-circuit-doe-v-reddit.htm (retrieved on October 26, 2022); E. Goldman, "The Ninth Circuit's FOSTA Jurisprudence Is Getting Clearer (and More Defense-Favorable)," *Technology & Marketing Law Blog*, May 5, 2023, online https://blog.ericgoldman.org/archives/2023/05/the-ninth-circuits-fosta-jurisprudence-is-getting-clearer-and-more-defense-favorable.htm (retrieved on May 5, 2023)

[298] Other questions could arise regarding the proportionality of those claims. Craigslist currently faces claims for advertisements published before 2008. Plaintiffs also try to reach, if not Backpage, the provider of its online infrastructure, US District Court for the Southern District of Texas Houston Division, *A.B. v. Salesforce*, March 22, 2021, 4:30-CV-01254; California Court of Appeals, First District, Second Division, *Does v. Salesforce.com*, December 30, 2021, no. A159566; US District Court, Northern District of Illinois, *G.G. v. Salesforce.com*, May 16, 2022, 20-cv-02335

some websites closed, either entirely[299] or partly.[300] Indeed, hard sovereignty was not the only state's strategy to succeed in its objectives. The use of every tool available under the law is indeed necessary to combat a phenomenon as complex as cyber trafficking. Nevertheless, questions arise when these tools are extralegal.

§2. Questioning the legitimacy of extending the scope of hard sovereignty

402. To fully understand the Craigslist and Backpage cases, the situation needs some perspective: The direct application of criminal law is not the only coercive tool available. In modern societies, the law tends to be seen as the core of the rule of law, leading "*to the complete juridicization of the social order*."[301] However, the law might not be adapted to ensure states' control over digital actors or to make them realize their own role in repressing trafficking. Indeed, the outcomes of the American cases significantly questioned the adequacy of hard sovereignty (I). Furthermore, these "convictions" were obtained based not only on legal legitimacy but also on other factors. As the state relies on other means of control, grounds for legitimacy are to be discussed (II).

I. The ineffectiveness of hard sovereignty to repress cyber trafficking

403. States' positive obligations: from coercion to collaboration. When repressing human trafficking, states have three main positive obligations derived from the ECHR's case law: "*(1) the duty to put in place a legislative and administrative framework to prohibit and punish trafficking; (2) the duty, in certain circumstances, to take operational measures to protect victims, or potential victims, of trafficking; and (3) a procedural obligation to investigate situations of potential trafficking*."[302] No obligation for results exists regarding conviction. The European anti-trafficking framework does not include liability for actors facilitating the offense that could not fulfill the criteria of criminal law.[303] Instead, on the basis of the third obligation, states must rely on all

[299] Like Backpage, L. Chamberlain, "FOSTA: A Hostile Law with a Human Cost," *op. cit.* note 245, p. 2201
[300] Regarding Craigslist, see R. Dalton, "Abolishing child sex trafficking on the internet," *op. cit.* note 229, p. 1109; regarding Vivastreet, see Le Monde, "Prostitution : Vivastreet suspend sa rubrique Rencontres," *Le Monde.fr*, June 19, 2018, online https://www.lemonde.fr/societe/article/2018/06/19/prostitution-vivastreet-suspend-sa-rubrique-rencontres_5317513_3224.html (retrieved on May 18, 2022)
[301] J. Chevallier, *L'État de droit*, LGDJ, Clefs, 6th ed., 2017, p. 59
[302] ECHR, *Zoletic and Others v. Azerbaijan*, October 7, 2021, no. 20116/12, ¶ 182
[303] See, for instance, Articles 21 and 22 of the Warsaw Convention

possible tools to investigate human trafficking: As such, digital actors could be seen as partners instead of offenders.[304] "*To the extent that they are forums for trafficking, they are also forums for its antidote*."[305] Partnerships exist in Europe, although they are still in their early stages. For instance, the French Central Office for the Repression of Human Trafficking collaborates with various digital actors, including Vivastreet[306] and Airbnb.[307] Similarly, in Romania, an awareness-raising campaign was led by the National Agency Against Trafficking in Human Beings on one of the largest platforms for announcements.[308] Similarly, in studying cyber trafficking, the GRETA focuses on the cooperation between states and digital actors rather than on their prosecution and conviction.[309]

404. To prosecute or not to prosecute. There are two visions of the repression of cyber human trafficking. One is that digital actors represent a hub of content linked to human trafficking and should be convicted,[310] while the other is that digital actors

[304] See, *supra* Part 1. Title 1. Chapter 2. . This idea could be derived from a broad interpretation of the case law of the ECHR, in which it included the investigation of Facebook accounts to repress human trafficking, ECHR, *S.M. v. Croatia*, June 25, 2020, no. 60561/14, ¶ 337. On the contrary, relying on digital actors to repair the harms made to the victims underlines a violation in the positive obligations of the state: it can be seen as a proof of the lack of protection of the victims that do not dare to go after their trafficker or cannot rely on the states' remedies; and a lack of investigation on primary traffickers that might not be prosecuted, known, or their properties might not be secured for later remedies. For instance, a fund for victim compensation, such as that prescribed by Article 15.4 of the Warsaw Convention and Article 17 of Directive 2011/36/EU in relation to Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims; see also Article 6.6 of the Palermo Protocol. Similarly, in France, investigations tend to focus on cases with various victims and traffickers, leading to different treatment depending on the size of the case, G. Mainsant, *Sur le trottoir, l'État: la police face à la prostitution*, Éditions du Seuil, La Couleur des idées, 2021, p. 208

[305] A.F. Levy, "The virtues of unvirtuous spaces," *Wake Forest Law Review*, 2017, vol. 52, pp. 406-407. While for now, when required to participate in judicial processes, they usually do not appear in court, G. Favarel-Garrigues, L. Mathieu, "Proxénètes en procès," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 65-93

[306] Regarding suspicious content, quicker information requests could be sent to obtain further data on the poster, G. Geoffroy, *Rapport d'information sur la prostitution en France*, *op. cit.* note 267, p. 271. But also with OVH, La Centrale, Overblog, etc., Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes - Rapport sur la cybercriminalité*, République française, February 2014, p. 37

[307] Airbnb, "Airbnb soutient le travail du Gouvernement contre la prostitution," *Airbnb Newsroom*, November 15, 2021, online https://news.airbnb.com/fr/airbnb-soutient-le-travail-du-gouvernement-contre-la-prostitution/ (retrieved on November 20, 2021)

[308] GRETA, "Evaluation Report - Romania - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings," Council of Europe, June 3, 2021, ¶ 162; Agenţia Naţională Împotriva Traficului de Persoane, "ANITP şi OLX, impreună pentru siguranţa ta," *ANITP*, October 31, 2018, online https://anitp.mai.gov.ro/4999-2/ (retrieved on July 5, 2022)

[309] GRETA, "Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties. Fourth evaluation round. Thematic focus: Addressing vulnerabilities to trafficking in human beings," Council of Europe, June 30, 2023, ¶ 17, GRETA(2023)11

[310] Position led on the basis of state criminal law in the United States mostly, and by the non-governmental organization that led the complaint against Vivastreet in France.

can contribute to human trafficking investigations[311], as law enforcement authorities avoid prosecutions with an uncertain outcome. When closing websites or increasing moderation,[312] anti-trafficking actors have raised concerns that victims would be advertised in less controlled online spaces.[313] As such, the US Department of Justice deemed that FOSTA would not facilitate the prosecution of primary sex traffickers and even "*increase exploitation in the sex industry*" by going further underground.[314] Similarly, the French Central Office for the Repression of Human Trafficking "*has itself spoken against the closure of*" Vivastreet.[315]

405. Consequences of hard sovereignty. After the passage of FOSTA, one of its sponsors claimed that it resulted in the shutdown of "*nearly 90% of the online sex trafficking business and advertisements*."[316] However, the traffickers quickly rebounded to other websites, and this drop was mainly due to the closure of Backpage, not the enactment of FOSTA.[317] The closure of one website simply moved the problem to other places, "*smaller sites without legal consequences*"[318] for primary traffickers. This simplification of the consequences of FOSTA is a useful example of the "*governance by numbers*"[319] that guides many current policies, and the legitimacy of the norms is established on the basis of statistics and data. Nonetheless, these numbers erase nuances and lack context. Furthermore, FOSTA has resulted in consequences for human trafficking investigations as prior strategies based on the availability of data on Backpage, and Craigslist became more difficult to implement.[320] Although advertisements are still online, they are now fragmented among various

[311] This strategy could be put in parallel with the one to not prosecute sex workers or victims of pimping for loitering when those act as informers for the police (before the suppression of this offense in France in 2016), G. Mainsant, *Sur le trottoir, l'État*, *op. cit.* note 304, pp. 99-108
[312] Could disappear red flags of human trafficking content, or an alert raised by trafficked victims, K. Albert et al., "FOSTA in legal context," *op. cit.* note 85, p. 1102
[313] A. Levy, "Online sex trafficking bill will make things worse for victims, expert says," *Perma*, March 29, 2018, online https://perma.cc/8ND4-5DGQ (retrieved on March 18, 2021)
[314] C.A. Jackson, J. Heineman, "Repeal FOSTA and Decriminalize Sex Work," *Contexts*, August 2018, vol. 17, no. 3, p. 74
[315] N. Duranton, *Rapport d'information sur les actes du colloque « Droits de l'Homme et démocratie à l'ère numérique »*, *op. cit.* note 272, pp. 88-89
[316] G. Kessler, "Has the sex-trafficking law eliminated 90 percent of sex-trafficking ads? - The Washington Post," *Washington Post*, August 20, 2018, online https://www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/ (retrieved on March 18, 2021); C. Burnitis, "Facing the Future with FOSTA," *op. cit.* note 237, p. 153
[317] E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 62, p. 1652
[318] A.W. Balfour, "In Defense of FOSTA," *op. cit.* note 230, p. 2508
[319] A. Supiot, *La gouvernance par les nombres: cours au Collège de France (2012-2014)*, Fayard, 2020
[320] L. Wiesner, "Good Intentions and Unintended Consequences," *op. cit.* note 292, p. 170

unknown websites[321] and take many forms.[322] Additionally, they are often located overseas,[323] making partnerships more complicated because of the need to rely on mutual legal assistance.[324] As FOSTA made online investigation more difficult, "*Arrests for sex trafficking have gone down, while arrests for prostitution have increased*."[325] The former focuses on primary traffickers, while the latter focuses on sex workers or trafficked victims,[326] which is counter to the international obligation to avoid prosecuting victims.[327] Asserting the state's hard sovereignty has led to weakened sovereignty through the violation of the duty to protect.

406. To improve the fight against cyber human trafficking, hard sovereignty hardly seems to support the protection of victims and the conviction of primary traffickers. Therefore, this strategy questions the legitimacy of states' coercion over digital actors. Furthermore, American extralegal actions also challenge their legitimacy.

---

[321] C. Bronstein, "Deplatforming sexual speech in the age of FOSTA/SESTA," *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, p. 376

[322] US Government Accountability Office, *Sex trafficking*, *op. cit.* note 254, p. 23

[323] J. Khodarkovsky, A.N. Russo, L.E. Britsch, "Prosecuting sex trafficking cases in the wake of the Backpage takedown and the world of cryptocurrency," *Department of Justice journal of federal law and practice USA*, 2021, vol. 69, no. 3, p. 6; "*We find that within six months of the shutdown of Backpage and Craigslist, there was a significant increase in the number of advertisements […] Moreover, roughly 75% of this increase was to offshore sites not subject to US legal jurisdiction*," H.S. Zeng, B. Danaher, M.D. Smith, "Internet Governance Through Site Shutdowns: The Impact of Shutting Down Two Major Commercial Sex Advertising Sites," *Management Science*, August 16, 2022, p. 2

[324] Digital actors try to protect themselves by "*host[ing] servers abroad, resid[ing] abroad, us[ing] offshore bank accounts and financial institutions, or introduc[ing] third parties*," US Government Accountability Office, *Sex trafficking*, *op. cit.* note 254, pp. 20-21. For an example of server relocation, see A. White, S. Guikema, B. Carr, "Why are You Here? Modeling Illicit Massage Business Location Characteristics with Machine Learning," *Journal of Human Trafficking*, Routledge, October 4, 2021, vol. 0, no. 0, p. 2

[325] E. Goldman, "The complicated story of FOSTA and section 320," *op. cit.* note 286, p. 292

[326] Moreover, survivors of trafficking criticized the decrease in protection of victims, C. Martell, "Customer Transparency Can Dampen the Growing Human Trafficking Problem," *op. cit.* note 295, p. 57

[327] Implicitly, Article 9.1.b of the Palermo Protoco, Article 26 of the Warsaw Convention and Article 8 of Directive 2011/36/EU. Although only the Palermo Protocol is applicable to the United States, the principle of non-prosecution extended the European frameworks through soft law, see, for instance, Office of the High Commissioner for Human Rights, "Recommended Principles and Guidelines on Human Rights and Human Trafficking," UN, 2010 principle 7; Conference of the Parties to the UN Convention against Transnational Organized Crime, "Resolution 5/2 Implementation of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime," UN, 2010, ¶ 8.e. On the non-punishment principle, see R.W. Piotrowicz, L. Sorrentino, "Human Trafficking and the Emergence of the Non-Punishment Principle," *Human Rights Law Review*, December 2016, vol. 16, no. 4, pp. 669-699; A. Schloenhardt, R. Markey-Towler, "Non-Criminalisation of Victims of Trafficking in Persons — Principles, Promises, and Perspectives," *Groningen Journal of International Law*, July 15, 2016, vol. 4, no. 1, p. 10; R. Piotrowicz, L. Sorrentino, "The non-punishment provision with regard to victims of trafficking A human rights approach," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 171

II. Extralegal actions: from hard sovereignty to social control

407. Extralegal pressures. The closure or suspension of websites did not result from the anti-trafficking framework or from legal actions. In the United States, they derived mostly from extralegal pressure,[328] thereby questioning the legitimacy of these closures. The first pressure arose from state entities. Threats of prosecution[329] were enough to produce significant changes to Craigslist that required posters to identify themselves through credit card information; furthermore, the adult section was renamed and, finally, closed.[330] Soon after the adoption of FOSTA, "*Craigslist eliminated its 'Personals' section*,"[331] independently of any criminal proceeding. The Backpage case led to a Senate investigation in 2017, which found the website liable for facilitating sex trafficking, aside from judicial proceedings.[332] Similarly, in France, Vivastreet temporarily suspended its meetings section, including erotica, after the criminal investigation was launched.[333] Before any legal conviction, websites introduced changes to comply with the petitions of law enforcement authorities, and social convictions had impacts before legal ones. A second set of pressures contributed to enforce social sanctions, which can be called a "*liability dictated by public opinion*."[334] Various media[335] and NGO[336] pressure[337] resulted in Backpage's

[328] Those extralegal actions also facilitated legal prosecutions, in particular that of Backpage, who pleaded guilty after being "*devastated*" by charges and multiple pressures, N. Cowen, R. Colosi, "Sex work and online platforms: what should regulation do?," *Journal of Entrepreneurship and Public Policy*, Emerald Publishing Limited, January 1, 2020, vol. 10, no. 2, p. 288

[329] In early 2009, "*The South Carolina Attorney General threatened Craigslist with criminal prosecution for aiding and abetting prostitution*," J.E.D. Larkin, "Criminal and Civil Liability for User Generated Content: Craigslist, a Case Study," *Journal of Technology Law & Policy*, June 2010, vol. 15, no. 1, p. 88. The following year, "*Attorneys general from seventeen states signed a letter [asking Craigslist] to remove the adult services section*," E.M. Donovan, "FOSTA and SESTA," *op. cit.* note 62, pp. 92-93

[330] J.E.D. Larkin, "Criminal and Civil Liability for User Generated Content," *op. cit.* note 329, p. 90; R. Dalton, "Abolishing child sex trafficking on the internet," *op. cit.* note 229, p. 1109

[331] L. Wiesner, "Good Intentions and Unintended Consequences," *op. cit.* note 292, p. 173

[332] Permanent subcommittee on investigations, *Backpage*, *op. cit.* note 52

[333] Le Monde, "Prostitution," *op. cit.* note 300

[334] N. Seddiki, "Repenser la responsabilité en affaires dans un monde globalisé," *Paix et Securité Internationales*, 2020, no. 8, p. 199

[335] "*The interferences between media representations, social perceptions, and the law are perfectly visible in relation to human trafficking [… Journalism] triggered the emergence of the first anti-trafficking campaign*," S. Rodríguez-López, "(De)Constructing Stereotypes: Media Representations, Social Perceptions, and Legal Responses to Human Trafficking," *Journal of Human Trafficking*, Routledge, January 2, 2018, vol. 4, no. 1, p. 62.

[336] The role of application stores is also mentioned in pressuring digital actors to change their activity; in particular, see the case of Tumblr, C. Bronstein, "Pornography, Trans Visibility, and the Demise of Tumblr," *TSQ: Transgender Studies Quarterly*, May 1, 2020, vol. 7, no. 2, pp. 242-247

[337] A campaign on Change.org was created. Similarly, for PornHub, T. Comerford, "Pornography Isn't the Problem: A Feminist Theoretical Perspective on the War against Pornhub Notes," *Boston College Law Review*, 2022, vol. 63, no. 3, p. 1178. Regarding Backpage, various advertisers withdrew from its parent company, E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 62, p. 1630 Indeed,

voluntary shutdown of its adult section and the modification of its policies.[338] Similar pressures arose in 2012–2013 regarding Google's allegedly profits from sex trafficking advertisements.[339]. Third, actions were taken by financial institutions based on state entities' requests[340] to credit card institutions.[341] A sheriff contacted Visa and MasterCard to ask them to stop their transactions on Backpage in 2015,[342] and they complied, "*cutting off services to the entire site's worldwide operations*."[343]

408. Autonomy of third-party actions. Since the Backpage case, payment processors realized that, in accordance with public policy objectives, they were allowed to determine "*what constitutes acceptable and prohibited transactions*," relying on the justification that they might be liable for sex trafficking.[344] In 2020, as a result of media

"*Commercial partners do not, for the most part, want to be associated with content deemed obscene or otherwise controversial*," S. Paasonen, K. Jarrett, B. Light, *NSFW: sex, humor, and risk in social media*, The MIT Press, 2019, p. 80

[338] M.A. O'Brien, "Free Speech or Slavery Profiteering: Solutions for Policing Online Sex-Trafficking Advertisement," *Vanderbilt Journal of Entertainment & Technology Law*, 2017, vol. 20, no. 1, p. 292

[339] Through a letter from the National Association of Human Trafficking and Victim Advocates and anti-trafficking organizations to state attorneys general, and a non-governmental investigation from Consumer Watchdog et al., *How Google's backing of Backpage protects child sex trafficking*, May 17, 2017, p. 13

[340] Since "*the early 2000s, the US government designated payment providers as responsible for tracking and blocking online payments related to child pornography, unlawful sales of tobacco, and Internet gambling*," N. Tusikov, "Revenue Chokepoints: Global Regulation by Payment Intermediaries," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, pp. 215-216; I. Brown, C.T. Marsden, *Regulating code: good governance and better regulation in the information age*, The MIT Press, Information revolution and global politics, 2013, pp. 106-110. They were also "*pressured to act as intellectual property enforcers, extending the reach of intellectual property law to websites operating from servers and physical facilities located abroad*," G.F. Frosio, "Why keep a dog and bark yourself? From intermediary liability to responsibility," *International Journal of Law and Information Technology*, March 1, 2018, vol. 26, no. 1, pp. 32-33. More controversial, payment processors were pressured to stop their transactions on WikiLeaks in 2010, A. Bridy, "Internet Payment Blockades," *Florida Law Review*, October 10, 2016, vol. 67, no. 5, pp. 1524-1527

[341] Similar calls to partner with financial institutions to repress human trafficking were made in France, see, for instance, R. Plant, "Mettre fin à l'exploitation, réflexions sur l'expérience nigériane et internationale," *in* B. Lavaud-Legendre (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 230

[342] A.F. Levy, "The virtues of unvirtuous spaces," *op. cit.* note 305, p. 415 The same tried to go against Craigslist first, US District Court, N.D. Illinois, *Dart v. Craigslist, Inc.*, *op. cit.* note 282

[343] G. Frosio, M. Husovec, "Accountability and Responsibility of Online Intermediaries," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 618-619. However, Backpage challenged this action and won the case, US Court of Appeals, Seventh Circuit, *Backpage.com, LLC v. Dart*, November 30, 2015, no. 15–3047, *807 F.3d 229*. The judge considered that this reaction was not only applicable to illegal advertisements, but also to protected speech, since not all advertisements were linked to trafficked victims or illegal prostitution.

[344] N. Tusikov, "Censoring Sex: Payment Platforms' Regulation of Sexual Expression," *in* M. Deflem, D. M. D. Silva (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, p. 66. Indeed, it is not clear when they are protected by Section 230, E. Goldman, "Section 230 Doesn't Protect App Stores That Sell Virtual Chips for Casino Apps-In re Apple App Store," *Technology & Marketing Law Blog*, September 6, 2022, online https://blog.ericgoldman.org/archives/2022/09/section-230-doesnt-protect-app-stores-that-sell-virtual-chips-for-casino-apps-in-re-apple-app-store.htm (retrieved on September 7, 2022). This seems

pressures against PornHub,[345] Visa and MasterCard stopped their collaboration with the website.[346] This led, independently from any prosecution,[347] to the discretionary removal of 10 million videos,[348] which did not result in restoring the collaboration with the credit card companies.[349]. More generally, in 2021, Visa and MasterCard announced the modification of their terms of service with adult content merchants to require age and identity verification,[350] content review before publication, and response to reports of illegal or nonconsensual content within seven business days.[351] This resulted in the decision of OnlyFans to ban pornography from the platform for only six days.[352] Therefore, third parties are establishing their own normative framework to

---

to clash with a "*growing precedent that app stores benefit from Section 230*," E. Goldman, "Section 230 Protect Apple's App Store from Claims Over Cryptocurrency Theft-Diep v. Apple," *Technology & Marketing Law Blog*, September 8, 2022, online https://blog.ericgoldman.org/archives/2022/09/section-230-protect-apples-app-store-from-claims-over-cryptocurrency-theft-diep-v-apple.htm (retrieved on September 8, 2022). Further amendments are in discussion to strengthen the liability of financial institutions in repressing human trafficking, in particular the End Banking for Human Traffickers Act, V. Mia, "The Failures of SESTA/FOSTA A Sex Worker Manifesto," *Tsq-Transgender Studies Quarterly*, Duke University Press, May 1, 2020, vol. 7, no. 2, p. 239

[345] A NGO anti-trafficking campaign and a New York Times investigation flagging child pornography on PornHub, for an analysis, see A. McKee, C. Lumby, "Pornhub, child sexual abuse materials and anti-pornography campaigning," *Porn Studies*, Routledge, October 2, 2022, vol. 9, no. 4, pp. 464-476

[346] M. Benisty, "Après avoir fait son beurre sur le sexe, OnlyFans bannit les contenus explicites," *Madmoizelle*, August 20, 2021, online https://www.madmoizelle.com/apres-avoir-fait-son-beurre-sur-le-sexe-onlyfans-bannit-les-contenus-explicites-1189063 (retrieved on August 20, 2021). This also led to the introduction of an amendment, the Survivors of Human Trafficking Fight Back Act, "*specifically targeting Tubist pornography sites like Pornhub. The proposed legislation targets user-posted photos and videos that depict child pornography, sexual assault victims, sex trafficking victims, and nonconsensual pornography. The bill requires websites to report such content and creates criminal and civil causes of action for sites housing or posting it, threatening websites pornography performers use to make a living-much like FOSTA-SESTA destroyed online resources for transactional sex workers*," T. Comerford, "Pornography Isn't the Problem," *op. cit.* note 337, pp. 1206-1209

[347] However, civil claims actions were indeed introduced, M. Le Corre, "Pourquoi 34 femmes ont attaqué Pornhub, « système mafieux », en justice," *Madmoizelle*, June 21, 2021, online https://www.madmoizelle.com/pourquoi-34-femmes-ont-attaque-pornhub-systeme-mafieux-en-justice-1139769 (retrieved on August 2, 2021); La Presse canadienne, "Mindgeek, société mère de Pornhub, visée par une poursuite aux États-Unis," *Radio-Canada.ca*, Radio-Canada.ca, June 18, 2021, online https://ici.radio-canada.ca/nouvelle/1802513/sites-porno-consentement-exploitation-sexuelle-feras-antoon-mindgeek (retrieved on June 24, 2021)

[348] J. Musto et al., "Anti-Trafficking in the Time of FOSTA/SESTA: Networked Moral Gentrification and Sexual Humanitarian Creep," *Social Sciences*, February 8, 2021, vol. 10, no. 2, p. 71

[349] S. Morrison, "The mystery behind OnlyFans' flip-flop on porn," *Vox*, August 26, 2021, online https://www.vox.com/recode/22642250/onlyfans-reverse-ban-porn-sexually-explicit-content-policy-bbc-mystery (retrieved on September 9, 2021)

[350] For both users and content producers, D. Leloup, F. Reynaud, "OnlyFans, Pornhub… Le monde bancaire régulateur de facto de l'industrie pornographique," *Le Monde.fr*, August 24, 2021, online https://www.lemonde.fr/pixels/article/2021/08/24/onlyfans-pornhub-le-monde-bancaire-regule-de-facto-de-l-industrie-pornographique_6092199_4408996.html (retrieved on September 7, 2021)

[351] S. Morrison, *The mystery behind OnlyFans' flip-flop on porn*, *op. cit.* note 349

[352] M. Benisty, *Après avoir fait son beurre sur le sexe, OnlyFans bannit les contenus explicites*, *op. cit.* note 346. Shortly after this announcement, a BBC News investigation revealed the lack of moderation regarding minor posters or sex work services on the platform, followed by a letter from members of Congress to the Department of Justice to investigate the website, N. Titheradge, "OnlyFans:

decide on the social liability of digital actors based on economic sanctions.[353]

409. Legitimacy of extralegal actions. Criminal law features the most difficult part of states' sovereignty. As such, it must rest on strict legitimacy by following democratic rules for setting offenses and states' criminal proceedings. Prosecuting corporations that facilitate sex trafficking for other offenses is still legitimate, and states use all legal options at their disposal to combat this complex phenomenon. However, this situation highlights a lack of interest on the part of the states to apply their criminal framework according to their own political priorities[354] and focuses on prosecutions instead of enhancements for victim protection.[355] Nevertheless, reliance on an extended criminal policy through third parties and social sanctions questions its legitimacy, and the lack of reliance on a legal basis skirts the norms to ensure that laws have a democratic basis. These types of sanctions, which are external to the judicial system, do not offer means of control or of due process. It could be argued that the voluntary actions taken by digital actors were grounded in the dissuasive role of criminal law. However, when the sheriff threatened to prosecute payment processors for not complying with the request to stop their transactions on Backpage, the offense hardly fit with the actions of these corporations. Instead of avoiding a criminal conviction, digital actors were taking action to avoid social and economic coercion. Thus, a team led by financial institutions and the media currently dictates social sanctions, while the state is too late to protect victims and investigate traffickers. Third parties realize they can play a role in social ordering outside the realm of states' legitimate coercion. The main issue,

---

How it handles illegal sex videos - BBC investigation," *BBC News*, August 19, 2021, online https://www.bbc.com/news/uk-58255865 (retrieved on September 17, 2021).

[353] Current investigations against Meta give another example of the relevance of private parties and media in the prosecution of digital actors, including private investigators and shareholders, J. Stempel, "Zuckerberg, Meta are sued for failing to address sex trafficking, child exploitation," *Reuters*, March 21, 2023, online https://www.reuters.com/legal/zuckerberg-meta-are-sued-failing-address-sex-trafficking-child-exploitation-2023-03-21/ (retrieved on March 23, 2023); A. Chapman, "How Meta's Failure to Act Upon Human Trafficking Claims Led to Another Lawsuit," *Impakter*, March 28, 2023, online https://impakter.com/metas-failure-act-upon-human-trafficking-claims-lawsuit/ (retrieved on March 30, 2023)

[354] Repressing cyber trafficking is part of both American and European priorities, The White House, "The National Action Plan To Combat Human Trafficking," US, December 2021, pp. 13-14; European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," EU, April 14, 2021, pp. 11-12, COM(2021) 171 final. Additionally, using the anti-trafficking framework to publicize those cases when prosecuting other offenses can be seen as a transparency problem.

[355] Since prosecutions are not based on a human trafficking offense, the identification and protection of victims get less importance; moreover, the state failed to protect trafficked victims, by challenging their civil actions against online intermediaries while not facilitating their actions against primary traffickers nor offering state-based ways for remedies.

however, is that these sanctions do not have a legal basis.

410. Legitimacy of digital actors as gatekeepers. In enhancing private orders, the state failed to protect the primacy of its sovereignty. Due to legal changes, digital actors must define what content is related to human trafficking: Digital actors came to decide what is illegal.[356] "*FOSTA has advanced a model of governance that makes the enforcement of anti-trafficking laws [the job] of a diffuse network of platforms and websites*."[357] Consequently, they hold "*quasi-judicial duties*,"[358] blurring "*the distinction between private interests and public responsibilities.*"[359] The control of online spaces to fight against trafficking can be deemed delegated[360] from states to digital actors, which become "*police, judge, and executioner,*"[361] as they lack a legitimate role provided by a legal framework in these "*enforcement tasks.*"[362] As such, digital actors can be deemed gatekeepers[363] of the online spaces for content linked to human trafficking. In general, they are "*agents who have a central role in the management of resources and infrastructure that are crucial for societies*."[364] Therefore, a digital actor has "*more control than [a mere] intermediary*."[365] Nevertheless, online gatekeepers can be multiples, as various roles are interconnected and can pressure one another.[366]

---

[356] C. Castets-Renard, "Régulation des plateformes en ligne," *op. cit.* note 114, ¶ 49

[357] J. Musto, M. Thakor, B. Gerasimov, "Editorial: Between Hope and Hype: Critical evaluations of technology's role in anti-trafficking," *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 8-9

[358] G.N. Yannopoulos, "The Immunity of Internet Intermediaries Reconsidered?," *op. cit.* note 208, p. 56

[359] N. Elkin-Koren, M. Perel, "Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 670

[360] *Ibid.*

[361] F. Stjernfelt, A.M. Lauritzen, *Your post has been removed*, *op. cit.* note 211, p. 262; T. Mirrlees, "GAFAM and Hate Content Moderation: Deplatforming and Deleting the Alt-right," *in* M. Deflem, D. M. D. Silva (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, p. 93. Also known as "*the Internet police*," G.F. Frosio, "The Death of 'No Monitoring Obligations': A Story of Untameable Monsters," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, November 30, 2017, vol. 8, no. 3, p. 16

[362] N. Elkin-Koren, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence," *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, p. 4

[363] Concept coined in 1947 by Lewin, K. Barzilai-Nahon, "Toward a theory of network gatekeeping: A framework for exploring information control," *Journal of the American Society for Information Science and Technology*, 2008, vol. 59, no. 9, p. 1493. It nowadays extends to who controls online content, see M. Taddeo, L. Floridi, "New Civic Responsibilities for Online Service Providers," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 1; J. McNamee, M. Fernández Pérez, "Fundamental Rights and Digital Platforms in the EU," *op. cit.* note 215, p. 111

[364] M. Taddeo, "The Civic Role of OSPs in Mature Information Societies," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 133-135

[365] E.B. Laidlaw, "Private Power, Public Interest: An Examination of Search Engine Accountability," *International Journal of Law and Information Technology*, March 1, 2009, vol. 17, no. 1, p. 115

[366] K. Barzilai-Nahon, "Toward a theory of network gatekeeping," *op. cit.* note 363, p. 1493

Gatekeepers multiply as the law extends to repress those that are linked to criminal content. To avoid their new liability and the risks linked to a limited legal certainty, digital actors are gatekeeping the Internet to restrict its use by traffickers. Nonetheless, this can hardly be considered prevention, since the law is dedicated to content linked to the exploitation of the victims through their advertisements, while the offense of human trafficking does not require exploitation but merely intent. The phenomenon is not disrupted; traffickers will only look for other opportunities as some digital actors learn how to detect their patterns online.

411. Conclusion of the section. Legitimacy understood as effectiveness is questioned. This extension of hard sovereignty to an extended criminal policy can, at first, seem effective: Results were obtained from enforcing coercion upon digital actors. They suffered sanctions and were forced to adapt their policies to become the gatekeepers of online spaces against cyber human trafficking. American amendments even appear as if they have a "*resonance force*" abroad, which is one expression of effectiveness.[367] However, when the details of the application of the law are examined, the effectiveness becomes loose. First, the reformed law faces much criticism in its drafting and its interpretation by judges; its chances for correct implementation according to its goals are challenging. Second, actions happen before the passage of the amendments, which questions the "*degree of adequacy […] in relation to the goal(s) set by a meta-positive reference*" such as the principle of utility or necessity.[368] Third, the "*degree of realization […] in the social reality*"[369] is unsatisfying: After the entry into force of FOSTA, few legal actions were developed to effectively realize its goals. Nevertheless, this realization might not be supported by the strict application of the law through convictions, but by internal conformity to its goals by private actors. However, the application of these goals through private actors, outside of the realm of the rule of law, and its consequences challenge the "*degree of adequacy of a norm*

[367] L. Heuschling, "'Effectivité', 'efficacité', 'efficience', et 'qualité' d'une norme/d'un droit. Analyse des mots et des concepts," *in* M. Fatin-Rouge Stéfanini et al. (eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?*, Bruylant, À la croisée des droits 6, 2012, p. 59

[368] *Ibid.*. Further, the validity of FOSTA has already been contested since 2018 in front of courts, due to its potential lack of conformity with the US Constitution's First Amendment, see US Court of Appeals, District of Columbia, *Woodhull Freedom Found. v. United States*, *op. cit.* note 249, overruling US District Court for the District of Columbia, *Woodhull Freedom Found. v. US*, *op. cit.* note 249, and US Court of Appeals, District of Columbia, *Woodhull Freedom Found. v. US (Opening Brief)*, June 9, 2022, no. 22-5105

[369] L. Heuschling, "'Effectivité', 'efficacité', 'efficience', et 'qualité,'" *op. cit.* note 367, p. 59

[…] to [its] purpose(s),"[370] here the improvement of the repression of cyber trafficking. In their attempt to solve the phenomenon through hard sovereignty, sovereigns stepped outside the realm of law, leading to further sharing the powers of coercion with digital actors.

412. Conclusion of the chapter. As states realized that digital actors had gained powers of coercion for human trafficking investigations, one of their first reactions was to seek to impose their own powers of coercion on digital actors. This follows the trend of holding corporations liable when they are somehow linked to an offense. However, the definition of human trafficking hardly fits with the role of digital actors in facilitating the process. Moreover, these corporations are still highly protected by their immunity as online intermediaries. Due to the inadequacy of hard sovereignty, states relied on other tools than those legitimized by the rule of law. To protect the legitimacy of states' actions, hard sovereignty relies on a new ethical "*evaluation of fault*"[371] through the "*moralization of the penal risk*."[372] To some, "*only the coercive mechanisms of criminal law are capable of effectively enforcing the compliance of the business world with the values*" of the Palermo Protocol.[373] However, instead of coercing digital actors that facilitate trafficking, such moralization indirectly required them to internalize the repression of the offense outside of any legal framework. This internalization is based mainly on the deletion of online content instead of on the prosecution of primary traffickers and the protection of victims. As states attempted to make digital actors liable, they collaterally increased their powers of coercion. Furthermore, it should be highlighted that the pressures between holders of sovereignty are not equal, and the extended American criminal policy questions the protection of European sovereignties.

[370] *Ibid.*
[371] H. Dumont, "Criminalité collective et principaux responsables : échec ou mutation du droit pénal ? Conclusion," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2012, vol. 1, no. 1, p. 123
[372] *Ibid.* p. 124
[373] N. García Rivas, "Responsabilidad penal de las personas jurídicas en la trata sexual y protección de las víctimas," *in* P. Lloria García, J. Cruz Ángeles (eds.), *La violencia sobre la mujer en el S. XXI: género, derecho y TIC*, Aranzadi, Estudios, 2019, pp. 59-80

Chapter 2. Ordering states' sovereignties through digital actors

413. Independence as sovereignty. Internal sovereignty was defined by the monopoly of legitimate coercion over people, and from an international perspective, various independent sovereign entities coexist.[1] The previous chapter highlighted the limited, although increasing, independence of digital actors, as states can establish their criminal policies through these actors, especially regarding the repression of human trafficking. On the contrary, sovereign states should be independent from one another and then equal.[2] However, legal theory does not consider the reality of differences in powers between states.[3] In particular, legal powers can be used by strong actors to influence international relations and foreign jurisdictions.[4] If not all states are equal, that leads to the question of which one (or ones) are the leaders. Regarding the fight against human trafficking and the regulation of the Internet, the United States can be named identified as the world leader.[5]

414. Who runs the world (of the Internet)?[6] The premise of the Internet, the US Advanced Research Projects Agency Network (ARPANET), was developed in the United States.[7] Most major digital actors are headquartered there, and their legal mother tongue is American English.[8] The Snowden scandal emphasized how digital

---

[1] O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, pp. 15-16

[2] J. Adams, M. Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies*, September 29, 2016, vol. 4, no. 6, p. 260

[3] J. Charpentier, "Le phénomène étatique à travers les grandes mutations politiques contemporaines," *in* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 25

[4] M. Delmas-Marty, "Le droit pénal comme éthique de la mondialisation," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2004, p. 8

[5] Additionally, China and Russia have powerful influences on the structure of the Internet, although at a more national level in the case of China. See, for instance, H. de Vauplane, "Une nouvelle géopolitique de la norme," *in* A. Garapon, P. Servan-Schreiber (eds.), *Deals de justice: le marché américain de l'obéissance mondialisée*, Presses universitaires de France, 2013, p. 23

[6] Referring to the song of Beyoncé, "*Run the World (Girls)*," 2011

[7] A.L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Century Foundation, May 15, 2000, p. 21. On the phases of the US interlinks with the governance over the Internet, see J. Ortiz Freuler, "The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century," *Global Media and China*, SAGE Publications Ltd, November 12, 2022, pp. 1-18

[8] B. de L. Chapelle, P. Fehlinger, "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 733

actors are closely connected to the US government.[9] Additionally, some institutions supervising the Internet are or were highly connected to the United States. For instance, the Internet Corporation for Assigned Names and Numbers was contractually linked, until 2016, to the US Department of Commerce.[10] The main language used on the Internet is English.[11] In this environment, "*Would Europe risk being subjugated?*"[12]

415. Leading the fight against trafficking. Regarding the repression of trafficking, the US leadership is less clear. Nevertheless, various scholars point to the United States' annual trafficking in persons report and its worldwide consequences. The Warsaw Convention offers a peer-monitoring system. On the contrary, unilaterally, the US State Department produces its own country-by-country evaluation,[13] which is "*part of an established tradition of US congressional oversight of the actions of other countries in politically important areas*."[14] Despite the quality of the reports improving over the years, the evaluations of some countries reveal the reports to be a political tool instead of objective assessments of anti-trafficking policies.[15] A negative ranking means economic sanctions,[16] and the ranking establishes priorities in the administration of international anti-trafficking grants.[17]

416. At the crossroads of both sectors, the systematization of the use of digital actors by the United States to broaden its anti-trafficking policies is still in development. Digital actors might have sovereign powers, but they lack full autonomy; their

---

[9] B. de La Chapelle, "Souveraineté et juridiction dans le cyberespace," *Hérodote*, La découverte, 2014, vol. 2014/1, no. 152-153, p. 175. See also the WikiLeaks scandal, N. Choucri, D.D. Clark, "Who controls cyberspace?," *Bulletin of the Atomic Scientists*, SAGE Publications, September 1, 2013, vol. 69, no. 5, pp. 20-31

[10] M. Arnaud, "Le WHOIS, talon d'Achille de la protection des données personnelles," *Hermes, La Revue*, C.N.R.S. Editions, 2009, vol. 53, no. 1, p. 107; P. Bellanger, "De la souveraineté numérique," *Le débat*, Gallimard, 2012, vol. 2012/3, no. 170, p. 152

[11] S. Biegel, *Beyond our control? Confronting the limits of our legal system in the age of cyberspace*, MIT Press, 2001, p. 125

[12] A. Bourdin-Revuz, *Le numérique, locomotive de la 3e révolution industrielle?*, Ellipses, 2013, p. 153

[13] 22 US Code (USC) § 2151n.f

[14] A.T. Gallagher, "Improving the Effectiveness of the International Law of Human Trafficking: A Vision for the Future of the US Trafficking in Persons Reports," *Human Rights Review*, Springer, 2011, vol. 12, no. 3, p. 382

[15] *Ibid.* pp. 388-389; E. Snajdr, "Beneath the master narrative: human trafficking, myths of sexual slavery and ethnographic realities," *Dialectical Anthropology*, June 1, 2013, vol. 37, no. 2, pp. 229-256

[16] Including a US opposition to *"non-humanitarian, non-trade-related assistance from international financial institutions and multilateral development banks, such as the International Monetary Fund and the World Bank*," J. Chuang, "The United States as Global Sheriff: Using Unilateral Sanctions to Combat Human Trafficking," *Michigan Journal of International Law*, Michigan Journal of International Law, 2006, vol. 27, no. 2, p. 452

[17] N. Godsey, "The Next Step: Why Non-Governmental Organizations Must Take a Growing Role in the New Global Anti-Trafficking Framework," *Regent Journal of International Law*, 2012 2011, vol. 8, no. 1, pp. 49-51

involvement in national policies leads to worldwide implementation, which can clash with others' sovereignties. Delmas-Marty stated that states' autonomy is a utopia and developed the notion of "*ordered pluralism*."[18] On the contrary, this chapter underlines a "disordered American imperialism."[19] Ordering pluralism was meant to arrange coexisting powers by defining their limits;[20] on the contrary, the United States uses disorganized powers to extend its goals overseas. First, its criminal imperialism, based on criminal policies and actions to repress human trafficking, has worldwide consequences (Section 1). Second, its repression is increasingly supported by automatic tools: European sovereignties can be threatened by US code imperialism (Section 2).

Section 1. US criminal imperialism: extended criminal policy on sex trafficking

417. Criminal and media imperialism. In 2008,[21] the US Code introduced extraterritorial jurisdiction for human trafficking.[22] However, this is far from the only way to affect foreign sovereignties. Traditionally, each independent state can establish its own norms, particularly regarding the limits of criminal law. When delimiting the repression of trafficking, one question quickly emerges: the difference between sex trafficking and sex work.[23] The US policies rest on their conflation,[24] leading to a focus

[18] M. Delmas-Marty, *Le flou du droit: du code pénal aux droits de l'homme*, Presses universitaires de France, Les Voies du droit, 1st ed., 1986, p. 332; M. Delmas-Marty, *Le pluralisme ordonné*, Éditions du Seuil, Les forces imaginantes du droit no. 2, 2004

[19] Delmas-Marty uses the notion of imperialism as opposed to pluralism, M. Delmas-Marty, "Les processus de mondialisation du droit," *in* C.-A. Morand (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no. 46, 2001, p. 78

[20] M. Delmas-Marty, *Trois défis pour un droit mondial*, Seuil, Seuil essais, 1998, p. 173

[21] 18 USC § 1596

[22] The extension of US jurisdiction can be seen as a kind of criminal imperialism. It can be traced back to the 1789 Alien Tort Claims Act. It gives jurisdiction to federal courts for claims brought by foreigners for international law violations that occurred abroad. However, main case law limited its application to avoid intrusions into foreign sovereignties, US Supreme Court, *Sosa v. Alvarez-Machain et al.*, June 29, 2004, no. 03–339; US Supreme Court, *Kiobel v. Royal Dutch Petroleum Co. et al.*, April 17, 2013, no. 10–1491; H. Muir Watt, "L'Alien Tort Statute devant la Cour Suprême des États-Unis. Territorialité, diplomatie judiciaire, ou économie politique ?," *Revue critique de droit international privé*, Dalloz, 2013, vol. 2013/3, no. 3, pp. 594-605

[23] Depending on the moral perspective on this phenomenon, the terms "sex work," "prostitution," or "sexual exploitation" are used. The last two convey a higher stigma, while the former was coined by a sex worker, Carol Leigh (also known as Scarlot Harlot), in 1978. To give credit to the people directly concerned by this topic, the term "sex work" will be used. On the use of these expressions, see D.M. Haak, "Re(de)fining Prostitution and Sex Work: Conceptual Clarity for Legal Thinking," *Windsor Review of Legal and Social Issues*, February 13, 2019, vol. 40, pp. 67-112

[24] J.L. Musto, "What's in a name?: Conflations and contradictions in contemporary U.S. discourses of human trafficking," *Women's Studies International Forum*, July 1, 2009, vol. 32, no. 4, pp. 281-287

on digital actors as facilitators of sex trafficking. To protect themselves from liability, digital actors increasingly include in their own private policies the repression of the content linked to this phenomenon. This highlights US "*platform imperialism*":[25] US policies shape online content around human trafficking and sex work through digital actors.

418. While moral and legal perspectives on human trafficking and sex work are multiple (§1), US criminal imperialism on human trafficking influences foreign policies and clashes with the European protection of human rights,[26] questioning the reality of independent sovereigns (§2).

§1. Legal sovereignties: regulating sex work through human trafficking

419. Opposing moral perspectives on the difference or conflation between sex work and exploitation (I) have led to various regulations of sex work and policies on the repression of human trafficking (II).

I. Moral perspectives on sex work

420. Radical feminism *versus* liberal feminism. Moral positions on sex work have rested on two polarized feminist perspectives since the 1980s: "structuralist" or radical feminism and "individualist" or liberal feminism.[27] The former argues that sex

[25] D.Y. Jin, "Facebook's Platform Imperialism: The Economics and Geopolitics of Social Media," *in* O. Boyd-Barrett, T. Mirrlees (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, pp. 189-190

[26] J. van Dijck, "Guarding Public Values in a Connective World: Challenges for Europe," *in* O. Boyd-Barrett, T. Mirrlees (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, p. 176

[27] A. Ferguson, "Sex War: The Debate between Radical and Libertarian Feminists," *Signs: Journal of Women in Culture and Society*, University of Chicago Press, 1984, vol. 10, no. 1, pp. 106-112; J.E. Halley et al., "From the International to the Local Feminist Legal Responses to Rape, Prostitution/Sex Work and Sex Trafficking: Four Studies in Contemporary Governance Feminism," *Harvard Women's Law Journal*, 2006, vol. 29, no. 2, p. 347; C. Plumauzille, "Prostitution," *in* J. Rennes (ed.), *Encyclopédie critique du genre*, La Découverte, 2021, p. 590

work is exploitation and coercive per se,[28] as it harms the dignity[29] of women[30] and relies on patriarchal domination and objectification[31] as a manifestation of sexual subordination of women.[32] Sex work equates to rape,[33] and sex workers are victims.[34] On the contrary, liberal feminism draws a distinction between coercive sex work, which can be qualified as pimping or human trafficking, and consensual sex work, which is a potential occupation based on controlling one's own sexuality.[35]

421. Sex wars at the supranational level. This clear-cut division was present in the negotiation of the Palermo Protocol.[36] This ideological gap focused on the definition of trafficking and the notion of "consent," in an attempt to internationally define sex work through the anti-trafficking framework.[37] The final definition[38] resulted in a

[28] For a summary of their claims: "*1) Prostitution is an evil per se; 2) violence is omnipresent in all forms of prostitution and trafficking for sexual exploitation; 3) clients and traffickers represent the personification of evil; 4) sex workers can have no will acknowledged; 5) prostitution and trafficking for sexual exploitation are inextricably linked; 6) the magnitude of both phenomena is high and increasing in recent years; and finally, 7) legalization would make the situation worse than it is today*," C. Villacampa Estiarte, "Políticas De Criminalización De La Prostitución: Análisis Crítico De Su Fundamentación Y Resultados," *Revista de Derecho Penal y Criminología*, Universidad Nacional de Educación a Distancia (UNED), 2012, no. 7, p. 99

[29] On the concept of dignity, see M. García Arán, "Trata de personas y regulación de la prostitución," *in* E. Pérez Alonso (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 655-675; B. Lavaud-Legendre, *Où sont passées les bonnes mœurs?*, Presses universitaires de France, Collection "Partage du savoir," 2005

[30] Therefore, it hides the realities of male, and non-cisgender sex workers.

[31] On this topic, see S. Paasonen et al., *Objectification: on the difference between sex and sexism*, Routledge, Gender insights, 2020

[32] Hiding the realities of sex work based on the consensual domination of men by women sex workers.

[33] E. Lê, "La construction juridique de la prostitution. Trois récits différenciés," *Cahiers du Genre*, December 15, 2014, vol. 57, no. 2, p. 147

[34] J. Outshoorn, "Debating Prostitution in Parliament: A Feminist Analysis," *European Journal of Women's Studies*, SAGE Publications Ltd, November 1, 2001, vol. 8, no. 4, p. 478

[35] J.R. Walkowitz, "The Politics of Prostitution," *Signs*, University of Chicago Press, 1980, vol. 6, no. 1, pp. 125-126; A. Jolin, "On the Backs of Working Prostitutes: Feminist Theory and Prostitution Policy," *Crime & Delinquency*, SAGE Publications Inc, January 1, 1994, vol. 40, no. 1, p. 79

[36] The origin of the protocol is an example of how the United States has "*been the primary anti-trafficking voice in the world*," M.P. Lagon, "The Global Abolition of Human Trafficking: The Indispensible Role of the United States," *Georgetown Journal of International Affairs*, 2011, vol. 12, no. 1, pp. 90-92. Since the Trafficking Victims Protection Act was negotiated in the United States at the same time, the Protocol draft was first written by the United States, C. Villacampa Estiarte, "La trata de seres humanos para explotación sexual: relevancia penal y confluencia con la prostitución," *in* C. Villacampa Estiarte, J.R. Barberà i Gomis (eds.), *Prostitución: ¿hacia la legalización?*, Tirant lo Blanch [u.a.], Tirant monografías no. 783, 2012, pp. 221-223. Negotiations featured "*heavy feminist lobbying*," J. Doezema, "Now You See Her, Now You Don't: Sex Workers at the UN Trafficking Protocol Negotiation," *Social & Legal Studies*, SAGE Publications Ltd, March 1, 2005, vol. 14, no. 1, p. 62

[37] J. Doezema, "Now You See Her, Now You Don't," *op. cit.* note 36, pp. 61-89

[38] Article 3 of the Palermo Protocol. The weight of the two camps played differently in the United States, C. Villacampa Estiarte, "Políticas De Criminalización De La Prostitución," *op. cit.* note 28, p. 98; A.W. Peters, *Responding to human trafficking - sex, gender, and culture in the law*, University of Pennsylvania Press, Pennsylvania Studies in Human Rights, 2015, pp. 49-50. Consequently, the international definition was not abided by the United States, and it passed its own definition of labor and sex trafficking instead, J. Chuang, "The United States as Global Sheriff," *op. cit.* note 16, p. 466; J.E. Halley et al., "Four Studies in Contemporary Governance Feminism," *op. cit.* note 27, pp. 358-359

compromise.[39] Coercive means are an element of the offense but are broadened—in other words, they are not limited to the strict use of force—and the consent of the victim is irrelevant. Exploitation does not equate to sex work but includes the exploitation of prostitution. Therefore, the regulation of sex work still belongs to the state's legal sovereignty. A similar division can be found in the EU. The regulation of sex work is not the competence of the Union; still, various institutions have developed their own vision. The EU political agenda, established by the European Parliament, tends toward a radical perspective[40] and seeks to conflate human trafficking and sex work.[41] In contrast, the CJEU adopts a more pragmatic approach.[42] In 1982, it was established that, as long as sex work is not forbidden, freedom of circulation—including the right to seek employment for sex work—cannot be denied on the basis of public policy.[43]. In 2001, in applying the right to establishment, the court considered that sex work can be seen as an "*economic activity pursued by a self-employed person*" as long as it is conducted "*outside any relationship of subordination […]; under that person's own responsibility; and in return for remuneration paid to that person directly and in full*."[44]

422. Outside the binary approach. Going further than this dual division, other

[39] C. Villacampa Estiarte, "Políticas De Criminalización De La Prostitución," *op. cit.* note 28, p. 103

[40] Since 1989, the European Parliament has considered that sex work, as much as human trafficking, is "*incompatible with the dignity and worth of the human person*," European Parliament, "Resolution on the exploitation of prostitution and the traffic in human beings," EU, April 14, 1989, ¶ A, OJ No C 120/2, p.352. Nevertheless, it seems that the Parliament indirectly recognized that some persons engage in sex work of their own free will (¶ E). In that sense, see also European Parliament, "Resolution on trade in women," EU, September 16, 1993, ¶ C, OJ No C 268, p.141. In 1996, it reaffirmed that sex work means a "*disregard for humanity*," European Parliament, "Resolution on trafficking in human beings," EU, February 5, 1996, OJ No C 120/2, p.352. In 2014, it stated that "*Prostitution and forced prostitution are forms of slavery incompatible with human dignity and fundamental human rights*," European Parliament, "Resolution on sexual exploitation and prostitution and its impact on gender equality," EU, February 26, 2014, ¶ B, 2013/2103(INI). Since then, the Parliament tends to talk about sexual exploitation instead of prostitution, see, for instance, European Parliament, "Resolution on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims," EU, February 10, 2021, 2020/2029(INI); European Parliament, "Resolution with recommendations to the Commission on combating gender-based violence: cyberviolence," EU, December 14, 2021, 2020/2035(INL); European Parliament, "Resolution on equality between women and men in the European Union in 2018-2020," EU, December 15, 2021, 2021/2020(INI); European Parliament, "Resolution on the EU Gender Action Plan III," EU, March 10, 2022, 2021/2003(INI)

[41] J. Outshoorn, "European Union and prostitution policy," *in* S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, 1st ed., 2019, pp. 366, 370-372

[42] A. Guamán Hernández, "La prostitución como actividad económica, la incidencia de la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas sobre la cuestión," *in* R. Serra Cristóbal (ed.), *Prostitución y trata: marco jurídico y régimen de derechos*, Tirant lo Blanch, Tirant monografías no. 484, 2007, pp. 255-294

[43] ECJ, *Rezguia Adoui v Belgian State and City of Liège; Dominique Cornuaille v Belgian State*, May 18, 1982, no. 115 and 116/81

[44] ECJ, *Aldona Malgorzata Jany e.a. and Staatssecretaris van Justitie*, November 20, 2001, C-268/99

perspectives have sought to change the global discourse. For instance, the third wave of feminism meant to bypass this ideological gap by recognizing the diversity of life experiences of women.[45] It requires the settlement of a definition of "choice" as a core element. However, this tactic leads to the division of two categories of persons: Sex workers who choose to exercise this activity and victims who did not choose it.[46] The first perspective hides the fact that persons can lack opportunities and that exploitative conditions can arise from a chosen activity.[47] The second perspective hides the fact that victims still have agency, they can choose to migrate, et cetera.[48] Moreover, the harm-reduction perspective[49] attempts to change the focus from a moral perspective to the prevention and remedy of human rights violations, including those involving sex workers' human rights violations. This requires thinking about the prevention and repression of basic offenses such as rape, social assistance to stigmatized minorities,[50] and labor regulation in a globalized context.[51]

423. Moral perspectives on sex work and its conflation with human trafficking have led to various legal and sovereign models of regulation.

II. Legal perspectives on sex work

424. Historical categories. Today, feminist topics are "*absorbed by the state [and*

[45] R.C. Snyder-Hall, "Third-Wave Feminism and the Defense of 'Choice,'" *Perspectives on Politics*, March 2010, vol. 8, no. 1, pp. 258-259

[46] J. Doezema, "Now You See Her, Now You Don't," *op. cit.* note 36, p. 80

[47] M. Farley, "'Bad for the Body, Bad for the Heart': Prostitution Harms Women Even if Legalized or Decriminalized," *Violence Against Women*, SAGE Publications Inc, October 1, 2004, vol. 10, no. 10, p. 1094; K.N. Deering et al., "A Systematic Review of the Correlates of Violence Against Sex Workers," *American Journal of Public Health*, American Public Health Association, May 2014, vol. 104, no. 5, pp. 42-54; S. Machat et al., "Sex workers' experiences and occupational conditions post-implementation of end-demand criminalization in Metro Vancouver, Canada," *Canadian Journal of Public Health = Revue Canadienne De Sante Publique*, October 2019, vol. 110, no. 5, pp. 575-583

[48] K.A. Pataki, K.M. Robison, "The Concept of Choice," *in* L. Walker, G. Gaviria, K. Gopal (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 39-43

[49] See, for instance, C. Breakstone, "'I Don't Really Sleep': Street-Based Sex Work, Public Housing Rights, and Harm Reduction Notes," *CUNY Law Review*, 2015 2014, vol. 18, no. 2, pp. 337-374; I. de Vries, J.A. Reid, A. Farrell, "From Responding to Uncertainties and Ambiguities to More Constructive and Inclusive Debates on Commercial Sex and Sex Trafficking," *Victims & Offenders*, Routledge, April 3, 2023, vol. 18, no. 3, pp. 599-600

[50] Instead of, for instance, giving priorities to the interests of "*real estate developers, municipal and national politicians, and business owners*" to make street-sex work disappear, E. Bernstein, *Temporarily Yours: Intimacy, Authenticity, and the Commerce of Sex*, University of Chicago Press, November 1, 2007, p. 164. See also P. Hubbard, "Cleansing the Metropolis: Sex Work and the Politics of Zero Tolerance," *Urban Studies*, SAGE Publications Ltd, August 1, 2004, vol. 41, no. 9, pp. 1687-1702; P. Hubbard, R. Matthews, J. Scoular, "Regulating sex work in the EU: prostitute women and the new spaces of exclusion," *Gender, Place & Culture*, April 2008, vol. 15, no. 2, pp. 137-152

[51] C. Harcourt, B. Donovan, "The many faces of sex work," *Sexually Transmitted Infections*, June 1, 2005, vol. 81, no. 3, p. 204

private actors][52] *to a great degree and transformed into a technique of power and administration*."[53] The regulation of sex work is one of these topics. Traditionally, it was divided into three categories: prohibitionism, abolitionism, and regulationism. Under the regulationism approach,[54] sex work is seen as a "*necessary evil*;"[55] thus, it is legal but is regulated under strict conditions. The regulation can be implemented at a local level: Sex work is considered a public nuisance and, therefore, is limited to specific areas. To summarize, it is an administrative system of control based on territory management and hygiene control.[56] Abolitionism was developed in reaction to these controls, starting in the United Kingdom, to abolish the Contagious Diseases Acts. In 1886, the acts were repealed, and various strategies were then developed to "abolish" sex work.[57] Finally, the prohibitionist approach sees sex work as a social evil and criminalizes all of its aspects, including the sex workers themselves.[58] It is the main US

[52] J. Kantola, J. Squires, "From state feminism to market feminism?," *International Political Science Review*, SAGE Publications Ltd, September 1, 2012, vol. 33, no. 4, pp. 382-400

[53] A. Kondakov, D. Zhaivoronok, "Re-assembling the feminist war machine: State, feminisms and sex workers in Russia," *in* S. Dewey, I. Crowhurst, C.O. Izugbara (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, p. 252

[54] Also called the old French model. It was in effect from 1802 to 1946, until the Marthe Richard law. It included the regulation of brothels, a national database of prostitutes, mandatory declaration of activity and, monthly mandatory medical visits. This approach was also adopted in the United Kingdom through the Contagious Diseases Acts of 1864. The state increased its control over sex workers to limit the spread of sexually transmitted diseases.

[55] M. Darley et al., "France," *in* S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, p. 62

[56] M. Wijers, "Fifteen years lifting of the ban on brothels The struggle of policy makers between sex workers as agents or victims," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 487

[57] The laws were based on a double standard, supporting stereotypes regarding female and male sexuality, and led to violations of the dignity and basic civil liberties of sex workers. Later on, the campaign fused with and began to be mainly run by religious groups and bourgeois feminists. It resulted in the promotion of sexuality restriction and the patriarchal family to protect a different kind of double standard and enhance a negative moral view on sex work. Sex workers were considered "lost girls" that would need to be redirected onto the "right path" to become "good women." For a complete analysis of the abolitionist movement, see J.R. Walkowitz, *Prostitution and Victorian Society: Women, Class, and the State*, Cambridge University Press, 1980

[58] Through direct criminalization, such as by forbidding the selling of sex, such as in Romania, if done on a repeated basis, A. Danet, "Romania," *in* S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, pp. 258-271; or indirect criminalization, by forbidding loitering, such as the offense introduced in France by Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, Article 225-10-1 of the Code pénal, later on repealed by Loi n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, Article 15. In Spain, administrative ordinances were adopted by municipalities to fine sex workers for loitering, such as in Murcia and Granada, C. Villacampa Estiarte, "A vueltas con la prostitución callejera: ¿Hemos abandonado definitivamente el prohibicionismo suave?," *Estudios penales y criminológicos*, Servicio de Publicaciones, 2015, no. 35, pp. 413-455; E. Boza Moreno, "La prostitución en España: el limbo de la alegalidad," *Estudios Penales y Criminológicos*, September 8, 2019, vol. 39

approach, although the regulation actually depends on each state.[59]

425. Unfitted historical divisions. However, all of these systems have been criticized, particularly under anti-trafficking and human rights frameworks. First, regulationism rests on "*disciplinary mechanisms*,"[60] employed by police and medical workers that infringe the basic human rights of sex workers and are based on a discrimination between genders. This policy does not consider assistance for sex workers suffering from exploitation.[61] Second, abolitionism refers to all sex workers as trafficked victims, leading to what the literature calls the "*rescue industry*"[62] or "*carceral feminism*."[63] A qualification of sex workers as victims has led them to be locked up in "rehabilitation centers" or repatriated against their will.[64] This is counter to the anti-trafficking framework: Assistance should be provided on a "*consensual and informed basis*,"[65] the reflection period is meant to support the victim in making their own choice,[66] and their repatriation should "*preferably be voluntary*."[67] Third, prohibitionism creates offenses against sex workers while some might be victims of trafficking. This policy is opposed to the non-punishment provision: States may "*provide for the possibility of not imposing penalties on victims for their involvement in unlawful activities*."[68] The ECHR reasserted that states must effectively implement the policy,[69]

[59] In general, "*Prostitution is illegal in every state in the [United States] except for a few rural counties in Nevada, where it is legal and regulated*," R. Russo, "Online Sex Trafficking Hysteria: Flawed Policies, Ignored Human Rights, and Censorship," *Cleveland State Law Review*, March 13, 2020, vol. 68, no. 2, p. 323

[60] C. Plumauzille, "Prostitution," *op. cit.* note 27, p. 593

[61] Sex workers can choose this practice and be victims of trafficking, M. Jakšić, "« Tu peux être prostituée et victime de la traite »," *Plein droit*, March 18, 2013, vol. 96, no. 1, pp. 18-22

[62] L.M. Agustín, *Sex at the margins: migration, labour markets and the rescue industry*, Zed Books, 2nd ed., 2008; G. Soderlund, "Running from the Rescuers: New U.S. Crusades Against Sex Trafficking and the Rhetoric of Abolition," *NWSA Journal*, October 2005, vol. 17, no. 3, pp. 64-87

[63] E. Bernstein, "Militarized Humanitarianism Meets Carceral Feminism: The Politics of Sex, Rights, and Freedom in Contemporary Antitrafficking Campaigns," *Signs: Journal of Women in Culture and Society*, The University of Chicago Press, September 1, 2010, vol. 36, no. 1, pp. 45-71; K.K. Hoang, "Perverse Humanitarianism and the Business of Rescue: What's Wrong with NGOs and What's Right about the 'Johns'?," *in* A.S. Orloff, R. Ray, E. Savcı (eds.), *Perverse Politics? Feminism, Anti-Imperialism, Multiplicity*, Emerald Group Publishing Limited, Political Power and Social Theory, 1st ed., January 1, 2016, vol. 30, pp. 19-43; A. Ahmed, M. Seshu, "'We have the right not to be 'rescued'...': When Anti-Trafficking Programmes Undermine the Health and Well-Being of Sex Workers," *Anti-Trafficking Review*, June 1, 2012, no. 1

[64] A. McClintock, "Sex Workers and Sex Work: Introduction," *Social Text*, Duke University Press, 1993, no. 37, p. 8

[65] Article 12.7 of the Warsaw Convention

[66] Article 13 of the Warsaw Convention

[67] Article 16.2 of the Warsaw Convention

[68] Article 26 of the Warsaw Convention, Article 8 of Directive 2011/36/EU

[69] ECHR, *V.C.L. and A.N. v. the United Kingdom*, February 16, 2021, 77587/12 and 74603/12

and it is recognized by international soft law instruments.[70]

426. Recent divisions. Consequently, new models have been developed. Today, the opposition between the Nordic model and the decriminalization model is materialized as two moral "*polarized approaches*."[71] The neo-abolitionist model rests on the radical feminist perspective and on the provisions of the anti-trafficking frameworks to discourage the demand for services or products linked to trafficking.[72] As the demand is seen as the cause of sex work, customers should be criminalized.[73] On the contrary, the decriminalization of sex work, complemented by a labor regulation and a recognition of social rights,[74] supports the liberal feminist perspective.[75]

427. Regulation of sex work and its relationship—conflation or distinction—with

[70] See, for instance, General Assembly, "Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons," UN, July 30, 2010, ¶ 30 of the Plan, A/RES/64/293; Office of the High Commissioner for Human Rights, "Recommended Principles and Guidelines on Human Rights and Human Trafficking," UN, 2010, principle 7

[71] L. Armstrong, "Decriminalisation of sex work in the post-truth era? Strategic storytelling in neo-abolitionist accounts of the New Zealand model," *Criminology & Criminal Justice*, SAGE Publications, July 1, 2021, vol. 21, no. 3, p. 3

[72] As such, it is also called the end-demand model. See Articles 6 and 19 of the Warsaw Convention; Article 18.1 and 4 of Directive 2011/36/EU. It should be underlined that the texts do not focus on sexual exploitation and consider it important to discourage the demand for services and products linked to any kind of exploitation.

[73] Although research is criticizing the consideration of clients as the new focus for criminal law, see, for instance, J.L. Mosley, "The 'john': Our new folk devil," *in* S. Dewey, I. Crowhurst, C.O. Izugbara (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 352-365; T. Sanders, B.G. Brents, C. Wakefield, *Paying for sex in a digital age: US and UK perspectives*, Routledge, 2020; S. Berger, "No End in Sight: Why the 'End Demand' Movement is the Wrong Focus for Efforts to Eliminate Human Trafficking," *Harvard Journal of Law and Gender*, 2012, vol. 35, pp. 540-542. The ban against the purchase of sex was originally passed in Sweden in 1999, then in various Nordic countries (Finland in 2006, Iceland, and Norway in 2009), leading to its nickname as "the Nordic model." In France, a similar ban was enacted in 2016, fully criminalizing clients of sex workers, Loi n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées. It modified Article 225-12-1 of the Code pénal and created Article 611-1. Persons soliciting or obtaining sexual services for a fee from minors were already criminalized. Similarly, some Spanish municipalities passed ordinances to criminalize clients, C. Villacampa Estiarte, "A vueltas con la prostitución callejera," *op. cit.* note 58, pp. 413-455; E. Boza Moreno, "La prostitución en España," *op. cit.* note 58

[74] C. Villacampa Estiarte, "Políticas De Criminalización De La Prostitución," *op. cit.* note 28, p. 86

[75] The Netherlands decriminalized organizing sex work and enhanced sanctions against coercive sex work in 1999, S. Altink, I. van Liempt, M. Wijers, "The Netherlands," *in* S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, p. 62; Germany declared sex work legal by the 2001 Prostitutionsgesetz, complemented by the 2016 Prostituiertenschutzgesetz to improve labor rights of sex workers, although it also extended the means of control (registration, licensing, control of the place of exercise, …). See I. Hunecke, "Germany," *in* S.Ø. Jahnsen, H. Wagenaar (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, pp. 107-121. Their effectiveness is highly criticized due to local implementation, R. Pates, "Liberal Laws Juxtaposed with Rigid Control: an Analysis of the Logics of Governing Sex Work in Germany," *Sexuality Research and Social Policy*, September 2012, vol. 9, no. 3, p. 214. However, those frameworks focus on the legality of the sex work contract and the decriminalization of related offenses. They did not focus on the adoption of special measures to recognize labor rights for sex workers. New Zealand was the first country in the world to adopt a full

human trafficking is part of states' legal sovereignty. However, the extended criminal policy of the United States to repress trafficking, based on a prohibitionist approach, has had impacts abroad supporting criminal imperialism.

§2. US sex trafficking policy: impacts on foreign sovereignties

428. The United States' extended criminal policy to repress sex trafficking facilitated by digital actors has had unintended consequences, making online investigations more difficult. Moreover, it has affected the regulation and moderation of sex work (I), including abroad. Therefore, it is interesting to consider these consequences in relation to the ECHR standards (II).

I. The consequences of an extended criminal policy on sex trafficking

429. The chilling effect. In the United States, digital actors face increased liability since FOSTA.[76] Being seen as facilitators of human trafficking hinders their reputation. Therefore, the risk of liability[77]—legal[78] or extralegal, just "*to be on the safe side*"[79]—created an incentive to develop content moderation. The risk of liability is a normal element of law; the fear of sanctions supports compliance with the rules. However, the vagueness of criminal definitions and liability frameworks can lead to a chilling effect,

decriminalization policy, Prostitution Reform Act, 2003, developing the labor rights of sex workers, L. Armstrong, "Decriminalisation and the rights of migrant sex workers in Aotearoa/New Zealand: Making a case for change," *Women's Studies Journal*, December 2017, vol. 31, no. 2, pp. 69-76. Recently, further European governments decided to adopt a decriminalization policy, such as Belgium (decriminalization, recognition of labor rights in discussion), Loi modifiant le Code pénal en ce qui concerne le droit pénal sexuel, 2022, see J.-M. Hausman, "La prostitution des personnes majeures dans la réforme du droit pénal sexuel belge : les premiers jalons d'un modèle néo-réglementariste," *Actualité juridique Pénal*, Dalloz, January 2023, p. 23 ; and Cataluña (adoption of a motion by the Parliament to not criminalize sex work), S. Brull i Ortega, "El Parlament pide no criminalizar a quienes ejercen la prostitución 'libre y voluntariamente,'" *ElNacional.cat*, July 7, 2022, online https://www.elnacional.cat/es/politica/parlament-pide-no-criminalizar-ejercen-prostitucion-libre-voluntariamente_784329_102.html (retrieved on September 20, 2022); La Vanguardia, "El Parlament rechaza la criminalización del trabajo sexual voluntario," *La Vanguardia*, July 7, 2022, online https://www.lavanguardia.com/politica/20220707/8392910/parlament-rechaza-criminalizacion-trabajo-sexual-voluntario.html (retrieved on September 20, 2022)

[76] D. Blunt, A. Wolf, N. Lauren, *Erased The Impact of FOSTA-SESTA*, Hacking//Hustling, 2020, p. 33

[77] F. Schauer, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," *Boston University Law Review*, January 1, 1978, vol. 58, pp. 696-698; E.B. Laidlaw, "Private Power, Public Interest: An Examination of Search Engine Accountability," *International Journal of Law and Information Technology*, March 1, 2009, vol. 17, no. 1, pp. 130-131

[78] Including with regard to corporate social responsibility, E.B. Laidlaw, "Online Platform Responsibility and Human Rights," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 66

[79] T. McGonagle, "Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 561

an incentive to over-compliance and moderation as well as "*the wrongful suppression of speech*."[80] The chilling effect doctrine was first developed in the United States[81] and is defined as "*when individuals seeking to engage in activity protected by the First Amendment*[82] *are deterred from so doing by governmental regulation not specifically directed at that protected activity*."[83] The ECHR also relies on this concept,[84] to highlight disproportionate measures on freedom of expression,[85] including by law.[86]

430. Moderating sex trafficking and sex work. For this reason, digital actors are incentivized to moderate sex trafficking as illegal content. However, illegal content can rest on "*broad and ambiguous laws*,"[87] and its online detection is far from easy.

---

[80] F. Schauer, "Fear, Risk and the First Amendment," *op. cit.* note 77, p. 732

[81] US Supreme Court, *Wieman v. Updegraff*, December 15, 1952, 344 U.S. 183; US Supreme Court, *Gibson v. Florida Legislative Investigation Committee*, March 25, 1963, 372 U.S. 539. The concept was initially developed to deal with anti-communist state measures, J. Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," *Berkeley Technology Law Journal*, 2016, vol. 31, no. 1, p. 125

[82] "*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*."

[83] F. Schauer, "Fear, Risk and the First Amendment," *op. cit.* note 77, p. 693. As such, "*The potential deterrent effect of a vague, or more commonly, an overbroad statute, was seen as reason enough to bend traditional rules of standing-a litigant would be allowed to attack such a statute, even though his own conduct could validly be proscribed by a legislative enactment more narrowly and clearly drafted*," *Ibid.* p. 685

[84] ECHR, *Goodwin v. the United Kingdom*, March 27, 1996, no. 17488/90, ¶ 39

[85] Especially regarding press and media freedom, ECHR, *Fatullayev v. Azerbaijan*, April 22, 2010, no. 40984/07, ¶ 102; ECHR, *Mosley v. the United Kingdom*, May 10, 2011, no. 48009/08, ¶ 126

[86] ECHR, *Smith and Grady v. the United Kingdom*, September 27, 1999, 33985/96, 33986/96, ¶ 127

[87] For instance, regarding hate speech, see Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "Report," Human Rights Council, General Assembly, UN, May 16, 2011, ¶ 26, A/HRC/17/27; T. Gillespie, "Content moderation, AI, and the question of scale," *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, p. 3; V.L. Gutiérrez Castillo, "El control europeo del ciberespacio ante el discurso de odio: análisis de las medidas de lucha y prevención," *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, Universidad de Sevilla, 2020, vol. 22, no. 45, pp. 291-310. At the European level, see the definition in Committee of Ministers, "Recommendation No. R (97) 20 to member states on 'hate speech,'" Council of Europe, October 30, 1997. The concept is not explicitly defined in the EU. The 2016 EU Code of conduct on countering illegal hate speech online relies on the offenses concerning racism and xenophobia set by Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law sets, Article 1. Similarly, for the offense of child pornography; for a classification, see M. Taylor, G. Holland, E. Quayle, "Typology of Paedophile Picture Collections," *The Police Journal*, April 2001, vol. 74, no. 2, pp. 97-107. At the legal level, a definition can be found in the 2000 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, Article 2.c. Questions remain regarding pornography starring adults pictured as children or animated pornography picturing children. Finally, on the definition of terrorism, see Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and A. Galán Muñoz, "Unión Europea y represión penal del discurso terrorista. ¿Origen, excusa o posible referente restrictivo?," *in* J. León Alapont (ed.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Homenajes y Congresos, 2020, pp. 351-388; R. Serra Cristóbal, "El control del *terror speech* en la red. El papel de las empresas proveedoras de servicios de internet," *in* J. León Alapont (ed.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Homenajes y Congresos, 2020, pp. 761-784

Identification of sex trafficking patterns is difficult even for trained experts. It supposes to prove the following elements: a process, such as a recruitment advertisement, coercive means or the minority of the victims, and the exploitative conditions of work. Obviously, either of the two latter types of information is not likely to appear online, which requires extensive training for moderators and the establishment of clear guidelines on trafficking indicators, which is also unlikely. However, FOSTA simplified this difficulty by reasserting the conflation with sex work.[88] In the United States, sex trafficking does not require proving exploitation as long as the purpose is commercial sex, and the new FOSTA offense explicitly conflates sex trafficking and sex work.[89] It requires digital actors to delete both types of content, erasing the difficulties in spotting sex trafficking. Global moderation of sex trafficking, which is obviously legal, is made easier by a US conflation with sex work, which is not always illegal.

431. Impact on sex work in the United States. Since 1996, the Internet has been used by sex workers to advertise,[90] "*form professional and social networks,*"[91] and perform new sexual services.[92] The US policy focused on the advertisement of trafficked victims, thus principally affecting mainstream direct sex work. The US cases and amendments had a "*ripple effect*";[93] the pressures on websites "*deplatformed*" sex

[88] A. Sanchez, "FOSTA: A Necessary Step in Advancement of the Women's Rights Movement," *Touro Law Review*, 2020, vol. 36, no. 2, p. 654

[89] 18 USC § 2421A

[90] R. Russo, "Online Sex Trafficking Hysteria," *op. cit.* note 59, p. 325. In general, research shows that the Internet "*offer[s] significant improvements in labor conditions and autonomy*" for a category of sex workers, T. Sanders et al., *Internet sex work - Beyond the gaze*, Springer Berlin Heidelberg, 2017. However, they face new barriers and risks, such as digital literacy, online harassment, etc., J. Swords, M. Laing, I.R. Cook, "Platforms, sex work and their interconnectedness," *Sexualities*, SAGE Publications Ltd, September 28, 2021, vol. 0, no. 0, p. 17. The Internet offers to lessen search costs, bargaining costs and policing and enforcing costs (ensuring enforcement of the agreement), N. Cowen, R. Colosi, "Sex work and online platforms: what should regulation do?," *Journal of Entrepreneurship and Public Policy*, Emerald Publishing Limited, January 1, 2020, vol. 10, no. 2, pp. 394-395 citing O. Lobel, "Coase and the Platform Economy," *in* J.J. Infranca, M. Finck, N.M. Davidson (eds.), *The Cambridge Handbook of the Law of the Sharing Economy*, Cambridge University Press, Cambridge Law Handbooks, 2018, pp. 67-77

[91] Creation of support platforms, such as forums or "bad date lists," to flag dangerous or non-respectful clients, D. Blunt, A. Wolf, "Erased: The impact of FOSTA-SESTA and the removal of Backpage on sex workers," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 119; L. Chamberlain, "FOSTA: A Hostile Law with a Human Cost," *Fordham Law Review*, 2019, vol. 87, no. 5, p. 2204

[92] T. Sanders, B.G. Brents, C. Wakefield, *Paying for sex in a digital age*, *op. cit.* note 73, pp. 35-36. Four kinds of sex work can be differentiated: "*in-person, direct sexual experiences […] at-a-distance, indirect 'live' experiences […] indirect purchasing or consumption of material […] asynchronous consumption and interaction*," J. Swords, M. Laing, I.R. Cook, "Platforms, sex work and their interconnectedness," *op. cit.* note 90, p. 2

[93] J. Khodarkovsky, A.N. Russo, L.E. Britsch, "Prosecuting sex trafficking cases in the wake of the Backpage takedown and the world of cryptocurrency," *Department of Justice journal of federal law and practice USA*, 2021, vol. 69, no. 3, p. 6

workers from their main online spaces.[94] This effect extended to Internet choke points[95] such as financial actors,[96] application distributors,[97] and cloud services[98] contributing to the exclusion of sex workers, either directly by being banished[99] or indirectly by affecting the terms of service of other platforms.[100] However, the United States adopts a prohibitionist framework;[101] as sex work is illegal, it is not collateral damage.[102] It is a mere exercise of their criminal sovereignty, although criminal law is not directly

---

[94] D. Blunt, Z. Stardust, "Automating whorephobia: sex, technology and the violence of deplatforming," *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, pp. 350-366. It includes advertising websites, platforms used to screen clients and reach out for support, for a list, see #SurvivorsAgainstSESTA, "Platforms which Discriminate Against Sex Workers," *#SurvivorsAgainstSESTA*, April 7, 2018, online https://survivorsagainstsesta.org/platforms-discriminate-against-sex-workers/ (retrieved on March 6, 2021). As "*the online commercial sex market is fractured*," it increased the costs of sex workers operations, J. Khodarkovsky, A.N. Russo, L.E. Britsch, "Prosecuting sex trafficking cases in the wake of the Backpage takedown and the world of cryptocurrency," *op. cit.* note 93, p. 6; D. Blunt, Z. Stardust, "Automating whorephobia," p. 362. "*Sites like Eros.com have increased their scrutiny for new members, requiring more forms of identification and higher advertising prices*," D. Blunt, A. Wolf, N. Lauren, *Erased The Impact of FOSTA-SESTA*, *op. cit.* note 76, p. 19. The increase of costs and reduction of income leads to a more limited autonomy and safety, supporting "*the power of clients and would-be managers*," D. Blunt, A. Wolf, "Erased," *op. cit.* note 91, p. 121; K. Albert et al., "FOSTA in legal context," *Columbia Human Rights Law Review*, Columbia University. School of Law, 2021, vol. 52, no. 3, p. 1090

[95] N. Tusikov, "Revenue Chokepoints: Global Regulation by Payment Intermediaries," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 213. Also known as "*Internet-infrastructure companies*," J.M. Balkin, "Free speech is a triangle," *Columbia Law Review*, Columbia Law Review Association, Inc., 2018, vol. 118, no. 7, pp. 2013-2014

[96] Visa, MasterCard, but also Paypal, D. Blunt, A. Wolf, N. Lauren, *Erased The Impact of FOSTA-SESTA*, *op. cit.* note 76, p. 18

[97] J. Porter, "Google is kicking 'sugar dating' apps out of the Play Store," *The Verge*, July 29, 2021, online https://www.theverge.com/2021/7/29/22599561/google-play-store-sugar-daddy-apps-dormant-developer-accounts-policy-change (retrieved on August 7, 2021)

[98] E. Garland, "How FOSTA/SESTA Will Change the Future of Indie and Feminist Porn," *Vice*, August 15, 2018, online https://www.vice.com/en/article/zmk89y/how-fostasesta-will-change-the-future-of-indie-and-feminist-porn (retrieved on May 15, 2021)

[99] D. Blunt, A. Wolf, "Erased," *op. cit.* note 91, p. 120

[100] E. Pilipets, S. Paasonen, "Nipples, memes, and algorithmic failure: NSFW critique of Tumblr censorship," *New Media & Society*, December 15, 2020, p. 1

[101] Such extension of the understanding of sex trafficking was also supported by the end-demand and neo-abolitionist movements, which hypothesize that erasing content from any erotic service will erase sex trafficking processes, C.A. Jackson, J. Heineman, "Repeal FOSTA and Decriminalize Sex Work," *Contexts*, August 2018, vol. 17, no. 3, p. 74. As the authors underline, however, such a hypothesis is highly criticized by the literature, see, for instance, R. Weitzer, "Flawed Theory and Method in Studies of Prostitution," *Violence Against Women*, July 2005, vol. 11, no. 7, pp. 933-949; S.-Y. Cho, A. Dreher, E. Neumayer, "Does Legalized Prostitution Increase Human Trafficking?," *World Development*, January 2013, vol. 41, pp. 67-82; R. Weitzer, "Sex Trafficking and the Sex Industry: The Need for Evidence-Based Theory and Legislation," *Journal of Criminal Law and Criminology*, 2013, vol. 101, no. 4, p. 1336; E. Albright, K. D'Adamo, "Decreasing Human Trafficking through Sex Work Decriminalization," *AMA Journal of Ethics*, January 2017, vol. 19, no. 1, pp. 122-126; E. Jeffreys, "Public encounters with whorephobia: Making sense of hostility toward sex worker advocates," *in* S. Dewey, I. Crowhurst, C.O. Izugbara (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, p. 513

[102] K. Albert, "Enough About FOSTA's 'Unintended Consequences'; They Were Always Intended," *Techdirt.*, July 29, 2021, online https://www.techdirt.com/articles/20210728/13245147264/enough-about-fostas-unintended-consequences-they-were-always-intended.shtml (retrieved on August 7, 2021)

applied. However, the moderation on sex work was directed not only at content linked to their services but also affected advocacy on sex work,[103] leading to a limited democratic debate on the topic.[104]

432. Collateral damages abroad. These consequences reached abroad, including in countries where sex work is legal or is not criminalized. Backpage was operated at a global level. The consequences of the US extended criminal policy reached Canada,[105] Europe,[106] Australia,[107] South America,[108] and New Zealand:[109] Worldwide, FOSTA "*incentivizes platforms to forbid sex workers from using the platform for their work*."[110] This surveillance is directed mainly at the deletion of advertisements for sex work.[111]. Digital actors continued to use the same vocabulary

[103] For instance, FOSTA "*led to the cancellation of the largest sex worker conference in the [United States]*," B. Chapman-Schmidt, "'Sex Trafficking' as Epistemic Violence," *Anti-Trafficking Review*, 2019, no. 12, p. 180; "*People who identified as both a sex worker and an [Activist, Organizer, Protester] experienced the negative impacts of platform policing both more intensely and more frequently*," D. Blunt et al., *Posting into the Void: studying the impact of shadowbanning on sex workers and activists*, Hacking//Hustling, 2020, p. 30

[104] In particular, less data is available online, making more difficult research on sex work that takes place through online recruitment of participants or observation of online spaces, T. Sanders, B.G. Brents, C. Wakefield, *Paying for sex in a digital age*, *op. cit.* note 73; T. Sanders et al., *Internet sex work - Beyond the gaze*, *op. cit.* note 90; H.L. Barakat, E.M. Redmiles, "Community Under Surveillance: Impacts of Marginalization on an Online Labor Forum," SocArXiv, September 24, 2021

[105] A. Tierney, "How the US 'Sex Trafficking' Crackdown Is Hurting Sex Workers in Canada," *Vice*, April 12, 2018, online https://www.vice.com/en/article/9kggwe/how-the-us-sex-trafficking-crackdown-is-hurting-sex-workers-in-canada (retrieved on July 4, 2022); E. McCombs, "'This Bill Is Killing Us': 9 Sex Workers On Their Lives In The Wake Of FOSTA," *HuffPost*, May 11, 2018, online https://www.huffpost.com/entry/sex-workers-sesta-fosta_n_5ad0d7d0e4b0edca2cb964d9 (retrieved on March 20, 2021)

[106] Such as in the United Kingdom, M. Smith, J. Mac, *Revolting prostitutes: the fight for sex workers' rights*, Verso, 2018, p. 127; C. Nast, "Under the threat of new laws, British sex workers fear for their websites and their safety," *Wired UK*, July 17, 2018, online https://www.wired.co.uk/article/adult-work-vivastreet-fosta-law (retrieved on April 7, 2023); and in Germany and Switzerland, C. Barwulor et al., "'Disadvantaged in the American-dominated Internet': Sex, Work, and Technology," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan, ACM, May 6, 2021, pp. 1-16

[107] J. Musto et al., "Anti-Trafficking in the Time of FOSTA/SESTA: Networked Moral Gentrification and Sexual Humanitarian Creep," *Social Sciences*, February 8, 2021, vol. 10, no. 2, p. 70; S. Smiley, A. Lavoipierre, "Australian sex workers struggle to survive after US bans online advertising," *ABC.net*, June 6, 2018, online https://www.abc.net.au/news/2018-06-07/fosta-the-us-law-punishing-australian-sex-workers/9842722 (retrieved on March 6, 2021)

[108] D. Blunt, A. Wolf, N. Lauren, *Erased The Impact of FOSTA-SESTA*, *op. cit.* note 76

[109] E. Tichenor, "'I've Never Been So Exploited': The consequences of FOSTA-SESTA in Aotearoa New Zealand," *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 102-109

[110] C. Matula, "Any Safe Harbor in a Storm: SESTA-FOSTA and the Future of § 230 of the Communications Decency Act," *Duke Law & Technology Review*, 2020, vol. 18, p. 359

[111] E. Pilipets, S. Paasonen, "Nipples, memes, and algorithmic failure," *op. cit.* note 100, p. 14. For instance, Reddit deleted several feeds of content dedicated to sex work and escorting, A. Romano, "A new law intended to curb sex trafficking threatens the future of the internet as we know it," *Vox*, April 13, 2018, online https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom (retrieved on March 6, 2021); TikTok and Instagram prohibited "*driving traffic to external sites like Patreon and OnlyFans*," C. Bronstein, "Deplatforming sexual speech in the age of FOSTA/SESTA," *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, p. 373. Sex workers started to use Linktree as

as FOSTA in their terms of services,[112] "*cut[ting] off [sex workers'] access to harm reduction tools made available through the Internet*."[113] Finally, the moderation of sex work was broadened to include sex workers' general use of online services. For instance, "*sex workers' Google Drive files [were] being locked or deleted,*"[114] and payment platforms intensified regulation of "*any content or transactions that may be perceived to promote or facilitate prostitution*."[115] Once it is linked to sex work, the sharing of personal data leads to blocking services across platforms, including those not linked to their sex worker occupation.[116]

433. Collateral damage in content moderation. To moderate a phenomenon, a definition is needed,[117]so digital actors delimit sex work, despite the lack of a straightforward definition. Sex work is usually understood as the exchange of sexual

an alternative, which soon also modified its terms of service, S. Cole, "Linktree Is Kicking Many Sex Workers Off Its Site," *Vice*, January 14, 2022, online https://www.vice.com/en/article/jgmjpk/linktree-banned-removed-inappropriate-use-sex-work (retrieved on January 21, 2022)

[112] Facebook, E.J. Born, "Too Far and Not Far Enough: Understanding the Impact of FOSTA," *New York University Law Review*, 2019, vol. 94, no. 6, p. 1649; Google through Playstore, ETX Daily Up, "Google bannit les applications de type 'Sugar Daddy' dans une nouvelle mise à jour," *Ladepeche.fr*, July 30, 2021, online https://www.ladepeche.fr/2021/07/30/google-bannit-les-applications-de-type-sugar-daddy-dans-une-nouvelle-mise-a-jour-9704136.php (retrieved on August 7, 2021); camming websites, H.M. Stegeman, "Regulating and representing camming: Strict limits on acceptable content on webcam sex platforms," *New Media & Society*, SAGE Publications, November 27, 2021, pp. 9-10

[113] R. Russo, "Online Sex Trafficking Hysteria," *op. cit.* note 59, p. 318. Such as support or screening forums, like Facebook groups, E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *Northwestern University Law Review*, 2020, vol. 115, no. 2, p. 530

[114] E. Garland, *How FOSTA/SESTA Will Change the Future*, *op. cit.* note 98, furthermore, "*often without warning*," H. Tripp, "All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims," *Penn State Law Review*, 2019, vol. 124, no. 1, p. 237

[115] N. Tusikov, "Censoring Sex: Payment Platforms' Regulation of Sexual Expression," *in* M. Deflem, D. M. D. Silva (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, p. 75

[116] D. Blunt et al., *Posting into the Void*, *op. cit.* note 103, p. 24

[117] But it also has been argued that "*The question of paid sexuality is not only taken into account by the law: It is constructed through it*," in particular depending on how it is defined, E. Lê, "La construction juridique de la prostitution," *op. cit.* note 33, p. 141

services for benefits.[118] However, what is "sex?"[119] How should "work" be defined?[120] Both of these questions are decided by digital actors.[121] To make moderation easier, many of them broaden sex work to include sexuality and nudity:[122] "*Sex is presumed guilty until proven innocent*."[123] Supported by FOSTA,[124], "*Social media identified it as*

[118] No international legal definition exists. Various definitions exist in the United States, based on state regulations. 18 USC § 1591.e.3 defines a "commercial sex act" as "*any sex act, on account of which anything of value is given to or received by any person*." The French definition was set by the Cour de Cassation: "*Prostitution consists of lending oneself, in exchange for payment, to physical contact of any kind, in order to satisfy the sexual needs of others*," Cour de Cassation, Chambre criminelle, March 27, 1996, no. 95-82016. In Spain, it was defined by the case law as "*the provision of services of a sexual nature in exchange for an economic consideration, which can be evaluated pecuniarily*," Tribunal Supremo. Sala Segunda, de lo Penal, July 26, 2016, no. 1847/2015

[119] Does it include erotic forms of art and care for the body? Also known as "indirect" forms of sex work, C. Harcourt, B. Donovan, "The many faces of sex work," *op. cit.* note 51, pp. 202-203: lap dancing, strip-teasing, tantric massage, BDSM (Bondage/Discipline, Domination/Submission, Sadism/Masochism), etc. Does it include physical forms of sexuality or virtual forms such as phone sex or camming? For instance, a 2022 French case law said that camming or selling nude pictures and videos is not "prostitution," Cour de cassation, Chambre criminelle, May 18, 2022, no. 21-82283

[120] It could be considered depending on the time dedicated to it, tax payment, but it is usually based on the earnings. Consequently, is it only a monetary payment or could it include goods, accommodation, or even protection in the framework of marriage? If it is money, what form should it take (payment after service, previous deposit, donation, etc.)? Should it include any kind of remuneration or one that is consistent with market prices? Should it be non-negotiable?

[121] For instance, "*the kinky social network FetLife changed its terms of service to ban the advertisement of escorts and "consensual blackmail and financial domination" fantasies*," E. Witt, "After the Closure of Backpage, Increasingly Vulnerable Sex Workers Are Demanding Their Rights," *The New Yorker*, June 8, 2018, online https://www.newyorker.com/news/dispatch/after-the-closure-of-backpage-increasingly-vulnerable-sex-workers-are-demanding-their-rights (retrieved on March 20, 2021). Similarly, "*Instagram ban hashtags like #femdom and even #women—while #maledom remains available*," J. York, *Silicon values: the future of free speech under surveillance capitalism*, Verso, 2021, p. 173 (femdom/maledom stands for female/male domination). Moreover, digital actors mainly include pornography in sex work, E. Garland, *How FOSTA/SESTA Will Change the Future*, *op. cit.* note 98; D. Leloup, F. Reynaud, "OnlyFans, Pornhub… Le monde bancaire régulateur de facto de l'industrie pornographique," *Le Monde.fr*, August 24, 2021, online https://www.lemonde.fr/pixels/article/2021/08/24/onlyfans-pornhub-le-monde-bancaire-regule-de-facto-de-l-industrie-pornographique_6092199_4408996.html (retrieved on September 7, 2021)

[122] For instance, on Facebook, "*until very recently, users attempting to report content using the platform's flagging tool were given an option that read: "This is nudity or pornography," with "sexual arousal," "sexual acts," and "people soliciting sex" as possible choices*," which makes the conflation very clear, J. Cook, "Instagram's Shadow Ban On Vaguely 'Inappropriate' Content Is Plainly Sexist," *HuffPost*, April 29, 2019, online https://www.huffpost.com/entry/instagram-shadow-ban-sexist_n_5cc72935e4b0537911491a4f (retrieved on March 6, 2021)

[123] R. Gayle, "Thinking Sex: Notes for a Radical Theory of the Politics of Sexuality," *in* R. Gayle (ed.), *Deviations: a Gayle Rubin reader*, Duke University Press, 2011, p. 144

[124] And by the pressure of Internet choke points such as financial institutions, application stores, search engines, etc. Following FOSTA, various digital actors edited their terms of service, broadening the limits of the moderation of sexual content, B. Ruberg, "'Obscene, pornographic, or otherwise objectionable': Biased definitions of sexual content in video game live streaming," *New Media & Society*, SAGE Publications, June 1, 2021, vol. 23, no. 6, p. 5: from Microsoft to reading apps, A. Romano, *A new law intended to curb sex trafficking*, *op. cit.* note 111; S. Rahman, "Trouble in Romancelandia: Online Censorship of Romance and Erotica," *BOOK RIOT*, December 3, 2021, online https://bookriot.com/online-censorship-of-romance-and-erotica/ (retrieved on December 9, 2021). See, for instance, the Tumblr case, K. Jarrett, B. Light, "Puritanisme sexuel et capitalisme numérique," *Revue Française de Socio-Économie*, La Découverte, 2020, vol. 25, no. 2, tran. F. Vörös, p. 170. Morever, eBay "*banned the sale of "sexually oriented materials" […] and closed its "Adults Only" category to new listings in the United States*," following potential pressures from its new payment processor, J. Dorris,

an easy target, […conflating] trafficking with sex, sex with a lack of safety."[125] When they were unable to moderate their content, some websites shut down to avoid liability.[126] However, these policies led to questionable moderation decisions, even before FOSTA. First, the policies questions the moderation of art,[127] and second, moderating content linked to sexual orientation and gender identity affects the LGBTQIA+ community.[128] Third, nudity, often conflated with sexuality, is directed mainly at women's bodies, leading to increased control and censorship.[129] Finally, moderation expanded to surprising content, including non-explicit words "*such as 'sensual' [and] 'touch'.*"[130] This leads to a very difficult framework for people who sought to provide sex education content.[131] It might be a mere "*reflection of American*

"The Queer Past Gets Deleted on eBay," *The New Yorker*, August 27, 2021, online https://www.newyorker.com/culture/cultural-comment/the-queer-past-gets-deleted-on-ebay (retrieved on September 9, 2021)

[125] C. Are, "The Shadowban Cycle: an autoethnography of pole dancing, nudity and censorship on Instagram," *Feminist Media Studies*, Routledge, May 19, 2021, vol. 0, no. 0, p. 14. Instagram demoted "inappropriate" posts ("sexually suggestive"), while not contrary to its terms of service, J. Cook, *Instagram's Shadow Ban On Vaguely 'Inappropriate' Content Is Plainly Sexist*, *op. cit.* note 122. Discord blocked "adult content" on its phone version, and Twitch "*revoked the ability for hot tub streamers to make money off advertisements*," D. Barnett, "2021 Year In Review: Sex Online," *Electronic Frontier Foundation*, December 29, 2021, online https://www.eff.org/deeplinks/2021/12/year-review-sex-online (retrieved on January 6, 2022). Amazon made erotic books disappear from rankings, S. Rahman, *Trouble in Romancelandia*, *op. cit.* note 124.

[126] Such as Pounced, dedicated to the furry community, E.J. Born, "Too Far and Not Far Enough," *op. cit.* note 112, p. 1648

[127] P. Petricca, "Commercial Content Moderation: An opaque maze for freedom of expression and customers' opinions," *Rivista internazionale di Filosofia e Psicologia*, December 30, 2020, vol. 11, no. 3, p. 317

[128] It stands for lesbian, gay, bisexual, transgender, queer (or questioning), intersex, and asexual/aromantic/agender people. The "+" symbol highlights that other minorities are included. For instance, Tumblr flagged non-explicit LGBTQIA+ content as pornography, C. Southerton et al., "Restricted modes: Social media, content classification and LGBTQ sexual citizenship," *New Media & Society*, SAGE Publications, May 1, 2021, vol. 23, no. 5, pp. 925-926. Facebook deleted post-mastectomy photos, including those that were meant to inform on transitioning processes, N. Tusikov, "Censoring Sex," *op. cit.* note 115, p. 64. In "*Canada, where similar rules existed, the content most susceptible to anti-pornography enforcement was actually erotic content geared toward the LGBTQ community*," E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *op. cit.* note 113, p. 518.

[129] For instance, both on Facebook and Instagram, female nipples are deemed sensitive, while male ones are not. It led to the deletion of art pieces such as *L'origine du monde* by Courbet, of historical pictures, such as the picture *Terror of War*, and of activism posts on breastfeeding, F. Stjernfelt, A.M. Lauritzen, *Your post has been removed: tech giants and freedom of speech*, SpringerOpen, 2020, p. 97. Instagram also blocked "*the hashtag #curvy, a term often associated with body positivity movements*," K. Tiidenberg, E. van der Nagel, *Sex and social media*, 2020, pp. 53-54

[130] J. Musto et al., "Anti-Trafficking in the Time of FOSTA/SESTA," *op. cit.* note 107, p. 68. The author of this thesis also experienced similar censorship when using the Microsoft software to transcribe speech: French words such as "jouir" (meaning "to use" but also "to orgasm," in the context, it was standing for "to use human rights") and "profonde" (meaning "deep", here standing for "high inequality") were transcribed with asterisks instead of words.

[131] A. Djoupa, "Tribune contre la censure de l'éducation sexuelle sur Instagram," *MadmoiZelle.com*, June 9, 2021, online https://www.madmoizelle.com/parler-deducation-sexuelle-sur-instagram-et-en-faire-son-metier-cest-vivre-avec-la-peur-au-ventre-1137662 (retrieved on June 10, 2021)

values,"[132] with moderation rules based on "*what people in the US find offensive*,"[133] while "*a majority of the users on Twitter, Facebook, and Google are abroad*."[134]

434. US extended criminal policy on sex trafficking supports its prohibitionist approach to sex work and foreign prohibitionist and neo-abolitionist policies, whose goal is to eradicate sex work. However, the policy affects sex workers in countries in which sex work is legal or decriminalized. Theoretically, states have legal sovereignty over sex work regulation, but practical matters are influenced by US policies. As such, this is an example of US criminal imperialism. Therefore, the regulation of "*discourse [here, by content moderation] is not separate from nor against power but is, in fact, a way of exercising it:*"[135] "*Sex is always political*."[136] Nonetheless, the legal actions of the United States and the moderation of content by digital actors could be challenged by European human rights standards.

II. The conformity of US policies to European standards

435. Sovereignty and freedom of expression. By applying the territorial limits of sovereignty, states can seize a website as property only in their territory. Thus, the seizure of Backpage[137] is part of US criminal policy, legitimized by its sovereignty. However, the consequences of this policy were not limited to the US territory. Although the United States is not part of the CPHR, it might be theoretically interesting to apply the criteria set by the ECHR to all of these consequences. First, US policy can hinder the independence of states and their sovereignty to regulate speech. Second, the

[132] S.T. Roberts, *Derrière les écrans*, La Découverte, October 15, 2020, p. 119; S. Paasonen, K. Jarrett, B. Light, *NSFW: sex, humor, and risk in social media*, The MIT Press, 2019, p. 40; N. Tusikov, "Censoring Sex," *op. cit.* note 115, p. 76; T. Mirrlees, "GAFAM and Hate Content Moderation: Deplatforming and Deleting the Alt-right," *in* M. Deflem, D. M. D. Silva (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, p. 94. On the contrary, it can also be considered that "*It's not American values […] but the values of a very particular demographic*," J. York, *Silicon values*, *op. cit.* note 121, p. 161

[133] A.E. Waldman, *Disorderly Content*, SSRN Scholarly Paper, ID 3906001, Social Science Research Network, August 16, 2021, p. 32

[134] M. Ammori, "The 'new' 'New York Times': free speech lawyering in the age of Google and Twitter," *Harvard Law Review*, The Harvard Law Review Association, 2014, vol. 127, no. 8, p. 2263. This extension of US values might not be limited to users, but also extends to moderators, as this work is highly delocalized abroad, J. Breslow, "Moderating the 'worst of humanity': sexuality, witnessing, and the digital life of coloniality," *Porn Studies*, Routledge, July 3, 2018, vol. 5, no. 3, pp. 225-240

[135] J. Berman, "(Un)Popular Strangers and Crises (Un)Bounded: Discourses of Sex-trafficking, the European Political Community and the Panicked State of the Modern State," *European Journal of International Relations*, SAGE Publications Ltd, March 1, 2003, vol. 9, no. 1, p. 47

[136] R. Gayle, "Thinking Sex," *op. cit.* note 123, p. 137

[137] The company is run by individuals located in the United States (although it is the property of a foreign company).

consequences of US policies threaten fundamental rights, particularly freedom of expression and information.[138] The ECHR decreed that states have a positive obligation to prevent human rights violations, even when they occur outside Europe;[139] "*Article 10 rights […] are enshrined 'regardless of frontiers'*."[140]

436. State blocking order.[141] First, the impossibility of using a website in Europe is equivalent to a blocking procedure.[142] Freedom of expression also protects "*means of transmission*."[143] The first decision of the ECHR on website blocking[144] focused on the collateral effect of the decision, which resulted in limiting access to blogs other than the offending one. Similarly, the seizure of Backpage blocked access not only to traffickers but also to any other advertisers, including foreign legal sex workers. Such an interference should be "*prescribed by law*," pursue a legitimate aim, and be "*necessary in a democratic society*."[145] The Backpage seizure relied on a statutory

[138] Article 10 of the CPHR. Under ECHR case law, freedom of expression includes the "*right to freedom to receive information*," ECHR, *Leander v. Sweden*, March 26, 1987, no. 9248/81, ¶ 74

[139] ECHR, *Soering v. the United Kingdom*, July 7, 1989, no. 14038/88

[140] ECHR, *Cox v. Turkey*, May 20, 2010, no. 2933/03, ¶ 31. Similarly, Article 19.2 of the 1966 International Covenant on Civil and Political Rights on freedom of expression applies "*regardless of frontiers*." Therefore, states should not "*disproportionately [burden] information and expression from outside their borders*," M.K. Land, "Toward an International Law of the Internet," *Harvard International Law Journal*, 2013, vol. 54, no. 2, p. 438

[141] First, a request to the ECHR should not be manifestly ill funded. A 2013 decision of the ECHR develops how a request could be manifestly ill funded regarding sanctions (including the seizure of the website) on the website's owners for offenses committed by users: here, the owners of the Pirate Bay for copyright violations by its users, ECHR, *Neij and Sunder Kolmisoppi v. Sweden (The Pirate Bay)*, February 19, 2013, no. 40397/12. The court considered the sanctions proportional and the request manifestly ill funded primarily on the basis that "*the applicants had not taken any action to remove the torrent files in question, despite having been urged to do so*." By applying this perspective to Backpage, it must be remembered that the website cooperated with law enforcement authorities. Therefore, this argument must be rejected.

[142] The first Protocol of the CPHR protects the right to property (Article 1), which is the most direct one that might be violated regarding a seizure. However, the seizure of Backpage did only not have a foreign impact per se, on the individual owners, but had also an impact on foreign users: the FBI seized the main Backpage websites (.com and .us) and, for instance, its equivalent in the three main European countries of this thesis (.fr, .es and .ro), US District Court, District of Arizona, *Miscellaneous Relief, US v. Lacey and others*, April 9, 2018, 2:18-cr-00422-SPL, pp. 59-60. It should be highlighted that if case law exists on the search and seizure of hardware (on the basis of Article 8 on the right to privacy, ECHR, *Modestou v. Greece*, March 16, 2017, no. 51693/13; ECHR, *Bože v. Latvia*, May 18, 2017, no. 40927/05; ECHR, *Trabajo Rueda v. Spain*, May 30, 2017, no. 32600/12), no such case law has been found on the seizure of a website. However, the court recognizes that domain names are indeed protected by Article 1 of the first protocol of the CPHR as a property, ECHR, *Paeffgen Gmbh v. Germany*, September 18, 2007, 25379/04, 21688/05, 21722/05, 21770/05

[143] ECHR, *Autronic Ag v. Switzerland*, May 22, 1990, no. 12726/87, ¶ 47

[144] Complain regarding the blocking of all Google Sites in Turkey to block one specific blog for "*insulting the memory of Atatürk*," ECHR, *Ahmet Yildrim v. Turkey*, December 18, 2012, no. 3111/10, ¶ 8. The argument developed by the ECHR to consider the proportionality of the measure was also applied by the CJEU to check the "knowledge" of the owners regarding the infringing content, CJEU, *Stichting Brein v. Ziggo BV, XS4ALL Internet BV*, June 14, 2017, C-610/15

[145] Article 10.2 of the CPHR. It should be highlighted that the ECHR confuses all three criteria. A similar confusion is made in ECHR, *Cengiz and Others v. Turkey*, December 1, 2015, 48226/10 and 14027/11,

basis[146] that has had been subject to various judicial proceedings, so the decision was foreseeable. Therefore, the proportionality of the decision relies on the balance between the two competing interests, for which states have a wide margin of appreciation.[147] The closure of Backpage was meant to prevent crime (sex trafficking) and to protect US morals (sex work). However, the seizure opposes the territorial integrity of foreign countries and the protection of other people's rights to legally exercise sex work abroad. The ECHR seems to consider primarily the quantity of blocked legal and illegal content.[148] Regarding Backpage, not all content was commercial sex, and not all commercial sex content could have qualified as trafficking.[149] Thus, the proportionality of the seizure could be questioned, especially when it affected sex workers who were operating under non-criminalizing frameworks. However, the ECHR usually recognizes the status of the victim in relation to the website's owner[150] and hardly recognizes the status in relation to its user,[151] depending on the nature of the content and whether it is linked to a topic of public interest.[152] This

as the unlawfulness is based on the proportionality of the measure. The court particularly studies the breadth of the statutory basis, ECHR, *Engels v. Russia*, June 23, 2020, no. 61919/16, ¶ 27. The website was never subject to judicial proceedings, and the judicial control did not check if a less far-reaching measure had been available. The importance of a judicial analysis of the circumstances is reiterated in ECHR, *Mariya Alekhina and Others v. Russia*, July 17, 2018, no. 38004/12. The court also pays attention to the implementation of the decision: For instance, IP-based blocking will by default extend to further content, ECHR, *Bulgakov v. Russia*, June 23, 2020, no. 20159/15, ¶ 34.

[146] 18 USC § 982.a.1 on criminal forfeiture

[147] ECHR, *Ashby Donald and Others v. France*, January 10, 2013, no. 36769/08, ¶ 40

[148] ECHR, *Yildrim*, *op. cit.* note 144, ¶ 66. The measure should "*strictly [target] the illegal content and ha[ve] no arbitrary or excessive effects*," and "*The wholesale blocking of access to an entire website is an extreme measure*," ECHR, *Vladimir Kharitonov v. Russia*, June 23, 2020, no. 10795/14, ¶¶ 38, 46. Therefore, "*A measure blocking access to an entire website has to be justified on its own, separately and distinctly from the justification underlying the initial order targeting illegal content*," ECHR, *Ooo Flavus and others v. Russia*, June 23, 2020, 12468/15, 23489/15 and 19074/16, ¶ 38. A similar approach is developed by the CJEU regarding the specification of a blocking order, CJEU, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH*, March 27, 2014, C-314/12; P. Valcke, A. Kuczerawy, P.-J. Ombelet, "Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 110

[149] For instance, one study concluded that only 5.5% of 1.5 million Backpage escort advertisements were likely to be linked to trafficking, A. Dubrawski et al., "Leveraging Publicly Available Data to Discern Patterns of Human-Trafficking Activity," *Journal of Human Trafficking*, January 2, 2015, vol. 1, no. 1, pp. 65-85. In another study based on a smaller set of data, "*Approximately 10% of the posts analyzed revealed an indicator of the broader concept of commercial sexual exploitation*," which does not mean it is equivalent to sex trafficking, D. Bounds et al., "Uncovering Indicators of Commercial Sexual Exploitation," *Journal of Interpersonal Violence*, December 2020, vol. 35, no. 23-24, pp. 5607-5623

[150] ECHR, *Kharitonov*, *op. cit.* note 148, ¶ 46

[151] Especially considering that the Internet offers various options to obtain a certain service, ECHR, *Akdeniz and Others v. Turkey*, March 11, 2014, no. 20877/10

[152] ECHR, *Donald*, *op. cit.* note 147, ¶ 39. As such, states have a wide margin of appreciation regarding commercial content, while it is highly limited regarding political speech or topics of public interest, ECHR, *Wingrove v. the United Kingdom*, November 25, 1996, no. 17419/90, ¶ 58. Regarding political speech,

notion is flexible,[153] and only purely commercial topics and commercial advertisements are not of public interest.[154] Thus, sex workers' advertisements would not have been protected, and even the closure of such a website in Europe could hardly be protected by freedom of expression based on a user's request.

437. Protecting speech. Second, speech regulation is currently developed by private companies through "*soft censorship*,"[155] and digital actors are proxies for states' speech regulation goals.[156] However, the ECHR applies only to states[157] that have hardly any positive obligation to protect speech from private commercial decisions.[158] Nevertheless, to measure US influence on European sovereignties through digital actors, the ECHR case law will be applied to digital actors. Freedom of expression applies "*not only to 'information' or 'ideas' that are favorably received […], but also to those that offend, shock, or disturb*."[159] While various complaints were filed to protect

content is protected as long as it does not prompt to violence, ECHR, *Selahattin Demirtas v. Turkey (3)*, July 9, 2019, no. 8732/11, ¶ 30

[153] B. Danlos, "Le débat d'intérêt général dans la jurisprudence de la Cour EDH relative à la liberté d'expression," *LEGICOM*, October 4, 2017, vol. 58, no. 1, pp. 14-15. Especially since it depends on the case circumstances, ECHR, *Axel Springer Ag v. Germany*, February 7, 2012, no. 39954/08

[154] Advertisements linked to a public interest debate are protected by the CPHR, see ECHR, *Animal Defenders International v. the United Kingdom*, April 22, 2013, no. 48876/08

[155] A. Löwstedt, "Fighting Censorship: A Shift from Freedom to Diversity," *in* M. Deflem, D.M.D. Silva (eds.), *Sociology of Crime, Law and Deviance*, Emerald Publishing Limited, April 23, 2021, p. 12. Different from hard censorship, defined as a "*state measure to control the flow of information and opinions*," P.F. Docquir, "La confrontation entre droits fondamentaux et puissances privées vues à travers le prime de la liberté d'expression," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 76

[156] J.M. Balkin, "Old-school/New-school speech regulation," *Harvard Law Review*, The Harvard Law Review Association, 2014, vol. 127, no. 8, p. 2298

[157] Especially regarding freedom of expression, they have negative obligations to not restrict protected speech: the *ratione personae* jurisdiction of the ECHR lies on a state violation, Article 34 of the CPRH. Similarly in the United States, the First Amendment is limited to government measures, F. Pasquale, "Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power," *Theoretical Inquiries in Law*, January 1, 2016, vol. 17, p. 506. See recently, US Supreme Court, *Manhattan Community Access Corp. v. Halleck*, June 17, 2019, no. 17-1702, *587 U.S.*

[158] Also called the horizontal effect of the convention, J. Barata i Mir, "Libertad de expresión, regulación y moderación privada de contenidos," *Teoría y derecho: revista de pensamiento jurídico*, Tirant lo Blanch, 2022, no. 32, p. 104; W. Benedek, M.C. Kettemann, *Liberté d'expression et internet*, Conseil de l'Europe, 2014, p. 25. For instance, when a private company restricted the distribution of leaflets in a shopping center, the ECHR "*does not find that the authorities bear any direct responsibility for this restriction on the applicants' freedom of expression*," ECHR, *Appleby and Others v. the United Kingdom*, May 6, 2005, no. 44306/98, ¶ 41. On the contrary, for a recognition of the protection of freedom of expression by the state between private violations, see ECHR, *Ozgur Gundem v. Turkey*, March 16, 2000, no. 23144/93, ¶¶ 42-46 regarding violent private pressures against a newspaper company; ECHR, *Fuentes Bobo v. Spain*, February 29, 2000, no. 39293/98, ¶ 38 regarding the violation of an employee's freedom of expression by its employer; and ECHR, *Dink v. Turkey*, September 14, 2010, 2668/07, 6102/08, 30079/08, 7072/09, 7124/09, ¶ 106 regarding the pressures of individuals on another through a criminal complaint

[159] ECHR, *Handyside v. the United Kingdom*, December 7, 1976, no. 5493/72, ¶ 49. In particular, "*It would be incompatible with the underlying values of the Convention if the exercise of Convention rights*

sex expression,[160] it is not strictly protected[161] due to the absence of any uniform European moral.[162] To be protected, sex expression must prove "*its merit as a work of art or as a contribution to public debate*."[163] Therefore, content linked to sex trafficking is obviously not protected under the CPHR.[164] On the contrary, commercial sex content would hardly be protected, since there is no European consensus on its regulation.[165]

---

by a minority group were made conditional on its being accepted by the majority," ECHR, *Bayev and Others v. Russia*, June 20, 2017, no. 67667/09, ¶ 70

[160] The publication of a schoolbook including sex education content, ECHR, *Handyside*, *op. cit.* note 159; the exhibition of paintings starring crude sexual relations, ECHR, *Müller and Others v. Switzerland*, May 24, 1988, no. 10737/84; the preview of content on a pornography website, ECHR, *Perrin v. the United Kingdom*, October 18, 2005, no. 5446/03; the diffusion of a pornographic movie, ECHR, *V.D. and C.G. v. France*, June 22, 2006, no. 68238/01; the organization of workshops abortion decriminalization and sexually transmitted diseases prevention, ECHR, *Women on Waves and Others v. Portugal*, February 3, 2009, no. 31276/05; the translation and publication of the French pornographic novel, ECHR, *Akdaş v. Turkey*, February 16, 2010, no. 41056/04; the diffusion of a press article on a sex offense, ECHR, *Aleksey Ovchinnikov v. Russia*, December 16, 2010, no. 24061/04; the exhibition of photographs of young girls and women in sexual poses and acts, ECHR, *Karttunen v. Finland*, May 10, 2011, no. 1685/10; the diffusion of leaflets against homosexuality, ECHR, *Vejdeland and Others v. Sweden*, February 9, 2012, no. 1813/07; the diffusion of information on homosexuality, ECHR, *Bayev*, *op. cit.* note 159

[161] The ECHR rarely recognizes a violation of freedom of sex expression. Indeed, "*Wider margin of appreciation is generally available […] when regulating freedom of expression in relation to matters liable to offend intimate personal convictions within the sphere of morals*," ECHR, *Müller*, *op. cit.* note 160, ¶ 35; ECHR, *Wingrove*, *op. cit.* note 152, ¶ 58

[162] On the contrary, the court actively protects sex expression when relying on a "*clear European consensus [such as] about the recognition of individuals' right to openly identify themselves as gay*," ECHR, *Bayev*, *op. cit.* note 159, ¶ 66. By resting its case law on the existence or not of a consensus, it "*legitimizes its control*," M. Guyomar, "Souveraineté des États et responsabilité partagée dans l'application de la Convention européenne des droits de l'homme," *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, p. 2

[163] ECHR, *Otto-Preminger-Institut v. Austria*, September 20, 1994, no. 13470/87, ¶ 56; for instance, by contributing to information on reproductive rights, ECHR, *Women on Waves*, *op. cit.* note 160, p. 43.

[164] Similarly, the US First Amendment does not protect "*speech integral to criminal conduct*," A. Sanchez, "FOSTA," *op. cit.* note 88, p. 656. Content "*inextricably intertwined with*" the offense of trafficking is not protected, E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *op. cit.* note 113, p. 513; US Supreme Court, *Giboney v. Empire Storage & Ice Co.*, April 4, 1949, 336 U.S. 490

[165] In the United States, advertisements for sex work are considered commercial speech, which is not as strictly protected. Its regulation is constitutional under various conditions, in particular if it concerns illegal activity, which sex work is in most US states, A. Sanchez, "FOSTA," *op. cit.* note 88, p. 658; US Supreme Court, *Central Hudson Gas & Electric Corp. v. Public Service Commission*, June 20, 1980, 447 U.S. 557. The three other conditions are: "*Whether the government has asserted a substantial interest in regulating the speech […] whether 'the regulation directly advances the governmental interest asserted' [and] whether the regulation is 'more extensive than necessary to serve that interest'*." As such, one court found that sex work advertisements "*by their nature contributed to the problem of commoditized sex*" and thus were not protected, E. Goldman, "Why FOSTA's Restriction on Prostitution Promotion Violates the First Amendment (Guest Blog Post)," *Technology & Marketing Law Blog*, March 19, 2018, online https://blog.ericgoldman.org/archives/2018/03/why-fostas-restriction-on-prostitution-promotion-violates-the-first-amendment-guest-blog-post.htm (retrieved on March 18, 2021); N. Wolfe, "Coyote Publishing, Inc. v. Miller: Blurring the Standards of Commercial and Noncommercial Speech," *Golden Gate University Law Review*, January 3, 2012, vol. 42, no. 1; US Court of Appeals, Ninth Circuit, *Coyote Publishing Inc. v. Miller*, March 11, 2010, no. 07-16633, *598 F.3d 592*. On the contrary, one court underlined that, by application of the strict interpretation of offenses, if sex work is illegal, the selling or offering of classified advertisement appearing to encourage sex work with an adult was not illegal under state law, leading to the protection of such content (as long as there is no knowledge of the minority of the person advertised), US District Court, M.D. Tennessee, Nashville Division,

However, the political content on sex work would be strictly protected as political speech.[166]

438. Moderating content. Consequently, moderation by digital actors could be questioned under Article 10 of the CPHR. As this study applies CPHR standards to digital actors as new enforcers of speech law, the equivalent of law would be their terms of service and all documents related to content moderation. The legal basis should be accessible and foreseeable. Regarding the former, it must be underlined that not all of these documents are available to the public. Concerning the latter, terms of service might be vague and might change regularly without any specific procedure legitimized by democratic or pluralist values.[167] However, "*the issue with the quality of*

Backpage.Com, LLC v. Cooper, January 3, 2013, 3:12-cv-00654, *939 F. Supp. 2d 805*; M.-H. Maras, "Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?," *Journal of Internet Law*, November 1, 2017, vol. 21, no. 5, p. 19.

[166] Similarly, in the United States, political speech around sex work should be protected. Advocacy for illegal actions is protected as long as it is not "*directed to inciting or producing imminent lawless action and is [not] likely to incite or produce such action*," US Supreme Court, *Brandenburg v. Ohio*, June 9, 1969, 395 U.S. 444. According to ECHR case law, moderation of nudity or sexually explicit content would be framed in the moral values of each digital actor, benefiting from a wide margin of appreciation. However, when moderation broadens to non-extreme or widely recognized artistic freedom or when it reduces minorities' content, it would trigger an interference in freedom of expression. Regarding sex speech, in the United States, the limit to the protection of the First Amendment is obscenity. It supposes to check "*(a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest […] (b) whether the work depicts or describes, in a patently offensive way, sexual conduct […] and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value*," G.R. Stone, "Sex and the First Amendment: The Long and Winding History of Obscenity Law," *First Amendment Law Review*, 2019, vol. 17, pp. 141-143, set in US Supreme Court, *Miller v. California*, June 21, 1973, 413 U.S. 15; US Supreme Court, *Paris Adult Theatre I v. Slaton*, June 21, 1973, 413 U.S. 49. However, the Miller test is also prone to criticism, in particular on the definition of "community" on Internet, C.W. Daum, "Sex, Laws, and Cyberspace: Organized Interest Litigation Before the U.S. Supreme Court," *The Justice System Journal*, Taylor & Francis, Ltd., 2006, vol. 27, no. 3, p. 307. "*Nowadays, only those sexual expressions deemed especially extreme, such as pedophilia, are recognized as obscenity*," E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *op. cit.* note 113, pp. 520-521. Consequently, most sex speech moderated by digital actors would still be protected under the First Amendment if this regulation had been based on a federal statute.

[167] For instance, Twitch terms of service refer to "common sense," a vague concept that hides the actual perspective adopted in the documents: "*the hegemonic, heteronormative common sense of […] white, straight, cisgender men*," B. Ruberg, "'Obscene, pornographic, or otherwise objectionable,'" *op. cit.* note 124, p. 14. The Facebook Community Standards, Facebook, "Facebook Community Standards," *Transparency Center*, 2022, online https://transparency.fb.com/policies/community-standards/ (retrieved on October 5, 2022), are more developed. For instance, in the category of "human exploitation," Facebook prohibits "*content geared towards the: recruitment of potential victims through force, fraud, coercion, enticement, deception, blackmail or other non-consensual acts; facilitation of human exploitation by coordinating, transporting, transferring, harboring or brokering of victims prior or during the exploitation; exploitation of humans by promoting, depicting or advocating for it*." While sexual solicitation is forbidden, Facebook allows "*expressing desire for sexual activity, promoting sex education, discussing sexual practices or experiences, or offering classes or programs that teach techniques or discuss sex*." It should be highlighted that the French translation is of poor quality. However, they still rely on vague concepts. In the "child sexual exploitation" category: "sexualized costume." In the category of "human exploitation," it uses the term "human trafficking" and other legally defined offenses without mentioning the definition or the legal basis (sex trafficking, forced marriage,

law is secondary to the question of necessity."[168] Moderation relies increasingly on "public order" justifications, such as the protection of users and consumers, especially minors, and the repression of offenses. In particular, "*trafficking, a transgressive practice that calls into question this sovereign performance, becomes an ideal site at which […] control can be legitimated and practiced*."[169] Moderation of content linked to human trafficking is legitimized by the "*prevention of […] crime*" and the "*protection of the reputation or rights of others*."[170] However, moderating sex work advertisements and sex expression is justified under the "*protection of […] morals*," with a wider margin of appreciation for sovereigns.[171] The deletion of protected content as an interference with freedom of expression must be justified by a "*pressing social need*."[172] In the absence of a specific case, a few elements are highlighted. First, judicial review is almost nonexistent;[173] moreover, the implementation of sanctions is highly criticized as the result of a double standard depending on the publisher of the content[174] and the type of content.[175]. Second, the basis for deletion might not be a violation of community

domestic servitude, bonded labor, etc.). They also extend to questionable content. In the "child sexual exploitation" category: "*open-mouth kissing*." In the "adult nudity and sexual activity" category: "*uncovered female nipples*," sex toys placed upon the mouth (except in the context of advertisements).

[168] ECHR, *Bayev*, *op. cit.* note 159, ¶ 63

[169] J. Berman, "(Un)Popular Strangers and Crises (Un)Bounded," *op. cit.* note 135, p. 52

[170] Article 10 of the CPHR

[171] Although it "*goes hand in hand with a European supervision by the Court*," ECHR, *Nilsen and Johnsen v. Norway*, November 25, 1999, no. 23118/93, ¶ 43

[172] It must be "*proportionate to the legitimate aim*," and the justifications of the moderator should be "*relevant and sufficient*," ECHR, *Sunday Times v. the United Kingdom (no. 1)*, April 26, 1979, no. 6538/74, ¶ 62. In this assessment, the ECHR focuses particularly on the potential chilling effect of the interference. It takes into account the nature and severity of sanctions, ECHR, *Morice v. France*, April 23, 2015, no. 29369/10, ¶ 127; the adoption of a less-interfering solution (limiting restriction to public spaces), ECHR, *Mouvement raëlien suisse v. Switzerland*, July 13, 2012, no. 16354/06, ¶ 75; the existence, scope, and effectiveness of a judicial review, ECHR, *Association Ekin v. France*, July 17, 2001, no. 39288/98, ¶ 61; as well as practical difficulties to implement it, ECHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, February 2, 2016, no. 22947/13, ¶ 86; the quality of the website (commercial or non-commercial), ECHR, *Pihl v. Sweden*, February 7, 2017, no. 74742/14, ¶ 35; and the unforeseeable quality of a vaguely worded law, ECHR, *Delfi AS v. Estonie*, June 16, 2015, no. 64569/09, ¶ 20. The court therefore applies a global assessment of the case, looking for a general balance.

[173] In particular, the transparency of sanctions might be limited due to the practice of "shadowbanning," which "*partially or entirely blocks the reach of some content without notifying the creators of that content*," K. Tiidenberg, E. van der Nagel, *Sex and social media*, *op. cit.* note 129, p. 53; C. Are, "The Shadowban Cycle," *op. cit.* note 125, p. 2

[174] For instance, "*Porn stars and other sex workers say the accounts they've maintained for years are facing a level of scrutiny that others - like celebrities and influencers who similarly post provocative images and videos – don't*," O. Steadman, "Porn Stars Vs. Instagram: Inside The Battle To Remain On The Platform," *BuzzFeed News*, October 18, 2019, online https://www.buzzfeednews.com/article/otilliasteadman/porn-stars-instagram-account-takedowns-jessica-jaymes (retrieved on March 6, 2021); C. Are, S. Paasonen, "Sex in the shadows of celebrity," *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, pp. 411-419

[175] For instance, "*Nudity and sexuality are easily banned, whereas […] blatant racism, discrimination, or harmful circulation of misinformation […] often remains up on the platform*," K. Tiidenberg, E. van der

guidelines but might rest on undefined terms, such as “inappropriate.” However, as mainly commercial entities, digital actors enjoy a large margin of appreciation to decide what should be accessible on the spaces they offer.

439. Conclusion of the section. The state’s criminal sovereignty applied to human trafficking includes the power to independently decide whether sex work should be conflated with or distinguished from it. For instance, the US prohibitionist approach underscores its extended criminal policy on online sex trafficking, which affects sex work. Since digital actors are mainly based in the United States, their priorities are significantly connected to US policies. However, as many digital actors operate worldwide, their implementation of these policies affects foreign sovereignties regarding sex work by materially shaping the new realities of sex work. Digital actors further conflate sexuality and nudity in cyberspace to facilitate moderation, while silencing the complexity of the phenomenon of human trafficking. This criminal imperialism seems to clash, in part, with European standards for the protection of freedom of expression. Although the proportionality of the seizure of Backpage can be questioned regarding ECHR standards, online users are not broadly protected from blocking orders. The wide margin of appreciation given to sovereigns for the protection of morals and the vagueness and variability of its criteria do not allow one to plainly consider the evolution of content moderation as contrary to freedom of expression. Such consideration would be made on a case-by-case basis, highly influenced by context. Therefore, US criminal imperialism softly affects European sovereignties, since a definition of offenses and inappropriate expression depends on local values. This impact is even softer when it is embedded in artificial intelligence tools.

Section 2. US code imperialism: fighting sex trafficking with artificial intelligence

440. Code is sovereignty. Lessig relied on the expression “*code is law*.”[176] In opposition to cyber libertarians who denied the possibility for law, particularly state law,

Nagel, *Sex and social media*, *op. cit.* note 129, p. 60. But also harassment, C. Are, “The Shadowban Cycle,” *op. cit.* note 125, p. 5. For instance, Tumblr is “*more responsive to banning sex workers than*” to blocking blogs of the extreme right Nazis, D. Blunt, A. Wolf, N. Lauren, *Erased The Impact of FOSTA-SESTA*, *op. cit.* note 76, p. 37.

[176] L. Lessig, *Code*, Basic Books, 2nd ed., 2006, p. 1

to regulate cyberspace,[177] Lessig saw cyberspace as a place to exercise power. Extended coercion does not apply only through traditional legal tools. In cyberspace, the main regulatory tool is code,[178] which embeds rules and values. Consequently, this tool leads to "*competing sovereigns*,"[179] depending on who can control code. While code regulates users' experiences, sovereigns face each other to regulate code. As a result, not all sovereigns are equal, in opposition to the theory of sovereignty. As the Internet was developed in the United States[180] and is highly structured today by digital actors who are influenced by US policies, code imperialism highlights "*how US dominance of code—and other forms of digital architecture—usurps other countries' sovereignty*."[181] Similarly, the use of certain systems to repress human trafficking, particularly artificial intelligence, has gone global since artificial intelligence was developed in the United States. Again, this situation threatens the independence of European sovereignties.

441. Artificial intelligence. Regulating code faces a first challenge: the absence of unique and harmonized definitions. Artificial intelligence[182] was originally defined as "*the construction of computer programs that perform tasks that are currently best accomplished by humans because they require high-level mental processes such as perceptual learning, memory organization, and critical reasoning*."[183] Artificial intelligence comprises two elements: a physical body (hardware) and an immaterial component (software).[184] In particular, it must be distinguished from the notion of

[177] D.G. Post, "Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace," *Journal of Online Law*, 1995, pp. 1-11
[178] L. Lessig, *Code*, *op. cit.* note 176, p. 24
[179] *Ibid.* p. 26
[180] See *supra* 414.
[181] M. Kwet, "Digital colonialism: US empire and the new imperialism in the Global South," *Race & Class*, SAGE Publications Ltd, April 1, 2019, vol. 60, no. 4, p. 6. The author adds that "*This structural form of domination is exercised through the centralized ownership and control of the three core pillars of the digital ecosystem: software, hardware, and network connectivity*," *Ibid.* p. 2. It must be underlined that the author uses the term "*digital colonialism*," but to harmonize with prior examples of US dominance and to focus on regulation of artificial intelligence, this study prefers the term "code imperialism."
[182] Turing is credited with establishing the link between computers and intelligence, A. Turing, "Computing machine and intelligence," *Mind*, October 1, 1950, vol. LIX, no. 236, pp. 433-460. Yet the term was coined by McCarthy at the 1956 Dartmouth College Conference. The use of the concept of "intelligence" within computing science is criticized, as "*Intelligence is defined as having the ability to create something that does not exist. But a computer does not create anything by itself*," L. Julia, O. Khayat, *L'intelligence artificielle n'existe pas*, First éditions, 2019, p. 151; K. Crawford, *Atlas of Ai: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, pp. 4-8
[183] Y. Meneceur, *L'intelligence artificielle en procès: Plaidoyer pour une réglementation internationale et européenne*, Bruylant, 2020, p. 48 This definition is used within the Council of Europe, Ad hoc committee on artificial intelligence, "Feasibility Study," Council of Europe, December 17, 2020, ¶ 5, CAHAI(2020)23
[184] S. Merabet, H. Barbier, *Vers un droit de l'intelligence artificielle*, Dalloz, Nouvelle Bibliothèque de Thèses, 2020, vol. 197, pp. 17-18

algorithms.[185]. Indeed, "*the basic ingredient of artificial intelligence is algorithms, which can be described as a procedure for solving a problem in a finite number of steps,*[186] *[but] not all algorithms can be considered an example of artificial intelligence*."[187] However, both systems are used before and during investigations and to regulate content to repress trafficking.

442. To consider how artificial intelligence systems can hamper the independence of European sovereignties, they should first be explained to ensure an understanding of their origin and functioning (§1). Later on, their potential impact on sovereignties is studied in parallel with their regulation (§2).

§1. Developing artificial intelligence to repress human trafficking

443. Artificial intelligence systems have both been developed to assist law enforcement authorities in investigating human trafficking (I) and to automate the moderation of illegal content (II).

I. Artificial intelligence to assist law enforcement authorities

444. The need for automatic tools. Once data become available to repress cyber human trafficking, a challenge lies in their processing.[188] Processing online public data faces the characteristics of big data: its volume, its velocity, and its variety, to which could be added to other challenges such as its veracity or its visibility.[189] Data are

[185] Although the word is now part of our everyday vocabulary, "*This notion has been known since antiquity, as can be seen in the writings of Diophantus of Alexandria or Euclid dating from the 4th century BC*," P. Hernert, *Les algorithmes*, Presses universitaires de France, 2002, p. 5. The origin of the concept is said to come from "*the Latinized nickname of a 9th century Persian mathematician, Al-Khwârizmî, who is credited with popularizing the world's first algebra textbook in the West*," J.-B. Duclercq, "Le droit public à l'ère des algorithmes," *Revue du droit public*, Lextenso, September 1, 2017, no. 5, p. 1401. Etymologically, algorithms are therefore closely connected to arithmetic.

[186] Definitions in the literature are not harmonized, similarly for "artificial intelligence." In the EU, the concept does not seem to be defined. Within the Council of Europe, there are many different definitions: European Commission for the Efficiency of Justice, "European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment," Council of Europe, December 4, 2018, p. 69; F. Zuiderveen Borgesius, "Discrimination, Artificial Intelligence and Algorithmic Decision-Making," Council of Europe, 2018, p. 8; Committee of experts on internet intermediaries, "Algorithms and human rights Study on the human rights dimensions of automated data processing techniques and possible regulatory implications," Council of Europe, 2017, p. 5; Committee of Ministers, "Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems," Council of Europe, April 8, 2020, ¶¶ 2, Annex

[187] W. Barfield, "Towards a law of artificial intelligence," *in* W. Barfield, U. Pagallo (eds.), *Research handbook on the law of artificial intelligence*, Edward Elgar Publishing, 2018, p. 4

[188] See *supra* Part 1. Title 2. Chapter 1. Section 2. .

[189] E. Velasco Núñez, C. Sanchís Crespo, *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019, p. 252

plentiful and fast-changing, making them difficult to be analyzed by a human brain in the investigation time frame. Consequently, the development of artificial intelligence systems to conduct this work is encouraged. This automatic processing could allow artificial intelligence systems to react more quickly and more proactively as well as to follow the movements of the victims, who are becoming more mobile.[190] An anti-trafficking strategy adapted for the repression of cyber trafficking includes the "*amassment of data by law enforcement to pursue anti-trafficking investigations, [the] augmentation of traditional surveillance techniques and tools, and [the] advancement of collaborative arrangements and technological innovation in the form of automated or algorithmic techniques*."[191]

445. The existing tools. From the available research dedicated to building these tools, three groups of systems can be identified. The first group aims to cross-reference classified advertisements that have been identified previously as likely to constitute trafficking with similar features to track the geographical movements of victims over time and to discover clusters.[192] The second group extracts advertisements to determine which ones are most likely to cover trafficking processes. The first criterion established for this goal is the identity of the phone number in several advertisements[193] combined with other information such as the identity of a pseudonym or photographs.[194] Scholars have developed various typologies of

[190] M. Latonero et al., *Human Trafficking Online The Role of Social Networking Sites and Online Classifieds*, Center on Communication Leadership & Policy, University of Southern California, September 2011, p. 29

[191] J.L. Musto, d. boyd, "The Trafficking-Technology Nexus," *Social Politics*, 2014, vol. 21, no. 3, p. 463; S. Milivojević, "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, p. 36

[192] E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, Thesis, Carnegie Mellon University, 2012; M. Ibanez, D. Suthers, "Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources," *47th Hawaii International Conference on System Sciences*, Waikoloa, HI, IEEE, January 2014, pp. 1556-1565, online http://ieeexplore.ieee.org/document/6758797/ (retrieved on October 9, 2020)

[193] M. Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Center on Communication Leadership & Policy, University of Southern California, November 2012

[194] H. Wang et al., "Data integration from open internet sources to combat sex trafficking of minors," *Proceedings of the 13th Annual International Conference on Digital Government Research - dg.o '12*, College Park, Maryland, ACM Press, 2012, p. 245, online http://dl.acm.org/citation.cfm?doid=2307729.2307769 (retrieved on December 29, 2020)

indicators for this aim.[195] The last group[196] seeks to visualize the set of extracted advertisements and the links that may exist between them.[197] Thus, a precise data analysis must be developed to create these connections, and requests can be conducted within a graph. Modeling the connections between advertisements is intended to reveal potential underlying trafficking networks.

446. Extracted data. The data extracted and categorized are multiple and includes the content of classified advertisements, such as name, age, city, phone number, external links, et cetera. Additionally, the systems will also select specific keywords as indicators or red flags of potential exploitation. In fewer cases, photographs are analyzed.[198] Finally, the systems extract metadata, for instance, the URL of the advertisement,[199] the date and time of posting,[200] and the name of the

[195] For developments, see, for instance, M. Hultgren, *An exploratory study of the indicators of trafficking in online female escort ads*, Thesis, San Diego State University, 2015; M. Hultgren et al., "Using Knowledge Management to Assist in Identifying Human Sex Trafficking," *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, IEEE, January 2016, pp. 4344-4353, online http://ieeexplore.ieee.org/document/7427725/ (retrieved on December 26, 2020)

[196] M. Ibanez, D. Suthers, "Detecting Covert Sex Trafficking Networks in Virtual Markets," *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining: ASONAM 2016 : San Francisco, CA, USA, August 18-21, 2016*, Institute of Electrical and Electronics Engineers, 2016, online http://ieeexplore.ieee.org/servlet/opac?punumber=7736513 (retrieved on October 9, 2020)

[197] D.R. Silva et al., "Data integration from open internet sources and network detection to combat underage sex trafficking," *Proceedings of the 15th Annual International Conference on Digital Government Research - dg.o '14*, Aguascalientes, Mexico, ACM Press, 2014, pp. 86-90, online http://dl.acm.org/citation.cfm?doid=2612733.2612746 (retrieved on January 16, 2021)

[198] For instance, the Marinus Analytics software can search a database of advertisements based on a picture of the victim. Other systems will be able to extract photos and study their composition to recognize tattoos, hair or eye color, body type, etc., P. Szekely et al., "Building and Using a Knowledge Graph to Combat Human Trafficking," *in* M. Arenas et al. (eds.), *The Semantic Web - ISWC 2015: 14th International Semantic Web Conference, Bethlehem, PA, USA, October 11-15, 2015, Proceedings, Part II*, Springer International Publishing, Lecture Notes in Computer Science, 2015, vol. 9367, pp. 205-211. Moreover, studies focus on the recognition of the backgrounds of photos to identify the hotels where they were taken, A. Stylianou et al., "TraffickCam: Crowdsourced and Computer Vision Based Approaches to Fighting Sex Trafficking," *2017 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Washington, DC, USA, IEEE, October 2017, pp. 1-8, online https://ieeexplore.ieee.org/document/8457947/ (retrieved on December 26, 2020); D. Roe-Sepowitz et al., *Online Advertisement Truth Set Sex Trafficking Matrix: A tool to Detect Minors in Online Advertisements*, Research Brief, Arizona State University School of Social Work, Office of sex trafficking intervention Research, November 2018; A. Stylianou et al., "Hotels-50K: A Global Hotel Recognition Dataset," *Proceedings of the AAAI Conference on Artificial Intelligence*, July 2019, vol. 33, pp. 726-733, https://ojs.aaai.org/index.php/AAAI/article/view/3863

[199] Uniform Resource Locator, A. Dubrawski et al., "Leveraging Publicly Available Data," *op. cit.* note 149, pp. 65-85

[200] M. Hultgren, *An exploratory study of the indicators of trafficking*, *op. cit.* note 195

account.[201] In rare cases, location data can be extracted.[202]

447. The origin of artificial intelligence systems. Almost exclusively, existing artificial intelligence systems come from the United States. The idea of developing artificial intelligence tools to combat human trafficking was first implemented by scholars in 2012.[203] Later, their elaboration was framed into the Defense Advanced Research Projects Agency,[204] meaning that research was directly funded and oriented by the US government. Its Memex program[205] provides academics with open-source data mining software to improve the cost, effectiveness, and accuracy of artificial intelligence systems used by law enforcement agencies, especially against trafficking.[206] Artificial intelligence is said to be used by "*over 200 law enforcement agencies*,"[207] including "*investigators for the district attorney of New York*."[208] In parallel, American private actors are developing systems with the same

[201] M. Ibanez, D. Suthers, "Detecting Covert Sex Trafficking Networks," *op. cit.* note 196
[202] C.A. Mattmann et al., "Multimedia Metadata-based Forensics in Human Trafficking Web Data," *WSDM'16 workshop proceedings*, San Francisco, USA, Interfacultary Research Institutes, Institute for Logic, Language and Computation (ILLC)IEEE, February 22, 2016
[203] E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, *op. cit.* note 192; M. Latonero, *Technology-Facilitated Trafficking*, *op. cit.* note 193
[204] P. Szekely et al., "Building and Using a Knowledge Graph," *op. cit.* note 198, pp. 205-211; C. Pellerin, "DARPA Program Helps to Fight Human Trafficking," *U.S. Department of Defense*, 2017, online https://www.defense.gov/News/News-Stories/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ (retrieved on January 14, 2022); Department of Justice, "National Strategy to Combat Human Trafficking," US, January 2017, p. 11
[205] R. Kapoor, M. Kejriwal, P. Szekely, "Using contexts and constraints for improved geotagging of human trafficking webpages," *Proceedings of the Fourth International ACM Workshop on Managing and Mining Enriched Geo-Spatial Data - GeoRich '17*, Chicago, Illinois, ACM Press, 2017, pp. 1-6, online http://dl.acm.org/citation.cfm?doid=3080546.3080547 (retrieved on January 16, 2021); M. Kejriwal, P. Szekely, "Information Extraction in Illicit Web Domains," *Proceedings of the 26th International Conference on World Wide Web*, Perth Australia, International World Wide Web Conferences Steering Committee, April 3, 2017, pp. 997-1006, online https://dl.acm.org/doi/10.1145/3038912.3052642 (retrieved on January 16, 2021); M. Kejriwal, P. Szekely, "An Investigative Search Engine for the Human Trafficking Domain," *in* C. d'Amato et al. (eds.), *The Semantic Web – ISWC 2017: 16th International Semantic Web Conference, Vienna, Austria, October 21-25, 2017, Proceedings, Part II*, Springer International Publishing, Lecture Notes in Computer Science, 2017, vol. 10588, p. 247; M. Kejriwal, P. Szekely, C. Knoblock, "Investigative Knowledge Discovery for Combating Illicit Activities," *IEEE Intelligent Systems*, January 2018, vol. 33, no. 1, pp. 53-63; M. Kejriwal, P. Szekely, "Knowledge Graphs for Social Good: An Entity-centric Search Engine for the Human Trafficking Domain," *IEEE Transactions on Big Data*, 2019, vol. 14, no. 8, pp. 1-15
[206] In particular, it can "*generate color-coded heat maps of different countries that locate where the most sex advertisements are being posted online at any given time*," L. Greenemeier, "Human Traffickers Caught on Hidden Internet," *Scientific American*, February 8, 2015, online https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/ (retrieved on January 8, 2021); DARPA, "Memex," no date, online https://www.darpa.mil/about-us/timeline/memex (retrieved on April 27, 2021)
[207] M. Kejriwal et al., "FlagIt: A System for Minimally Supervised Human Trafficking Indicator Mining," *ArXiv:1712.03086 [cs]*, December 5, 2017, p. 5, online http://arxiv.org/abs/1712.03086 (retrieved on April 10, 2021)
[208] C. Pellerin, *DARPA Program Helps to Fight Human Trafficking*, *op. cit.* note 204

goal.[209]Additionally, similar systems are being developed outside the United States, such as in Canada[210] and the United Kingdom,[211] and the American systems are directly exported, including to some countries in Europe, such as in the United Kingdom and Ireland.[212]

448. The use of American artificial intelligence systems by law enforcement authorities within the EU appears now to be merely a potential risk. On the contrary, digital actors' artificial intelligence systems are already in use worldwide.

II. Artificial intelligence to assist digital actors

449. The need for automatic tools. Major digital actors in the United States are now the gatekeepers of online content linked to human trafficking. However, the volume of uploaded data amounts to big data; there is a problem of "*scale of operation*."[213] Each specific piece of content should be qualified to determine if whether it is licit or not regarding the terms of service and the law. Therefore, artificial intelligence systems were developed to support this work. These can be named "*algorithmic commercial content moderation*" and can be defined as "*systems that classify user-generated content based on either matching or prediction, leading to a decision and governance outcome*."[214]

450. The scale of artificial intelligence for moderation. Moderation can happen

[209] For instance, the Spotlight program of the NGO Thorn; or Marinus Analytics, a company created on the basis of the work of E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, *op. cit.* note 192; Marinus Analytics, "About," *Marinus Analytics*, no date, online https://www.marinusanalytics.com/about (retrieved on October 4, 2022)

[210] Mila, "AI for Combating Human Trafficking in Canada," *Mila*, 2021, online https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/ (retrieved on May 1, 2021); Mila, "Infrared," *Mila*, no date, online https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/ (retrieved on July 5, 2023)

[211] X. L'Hoiry, A. Moretti, G.A. Antonopoulos, "Identifying sex trafficking in Adult Services Websites: an exploratory study with a British police force," *Trends in Organized Crime*, May 5, 2021; L. Giommoni, R. Ikwu, "Identifying human trafficking indicators in the UK online sex market," *Trends in Organized Crime*, September 17, 2021

[212] Marinus Analytics, *About*, *op. cit.* note 209

[213] P. Petricca, "Commercial Content Moderation," *op. cit.* note 127, p. 310; T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018, p. 97. In April 2022, every minute, more than two million Snaps are shared on SnapChat, more than one million pieces of content are shared on Facebook, more than 300.000 tweets are shared on Twitter, more than 60.000 photos are shared on Instagram, 500 hours of video are uploaded to Youtube, Statista, "User-generated internet content per minute 2022," *Statista*, April 2022, online https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (retrieved on October 17, 2022)

[214] R. Gorwa, R. Binns, C. Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, SAGE Publications Ltd, January 1, 2020, vol. 7, no. 1, p. 3

ex ante, before the publication of the content, or *ex post*, after its publication and, in general, after a user's report. However, "*Algorithms do not moderate alone*."[215] They can be used for two main goals: "*proactive detection of content and automated evaluation of that content*."[216] In the latter case, they decide on the viability of the content. In the former case, they only flag content, and human moderators must decide on their deletion. Regarding proactive detection of content, artificial intelligence supports the work of humans.[217] This co-moderation allows humans to "*clean up after technology: They correct mistakes, reconsider automatic moderation decisions, and act on content [artificial intelligence] erroneously let slip through the cracks*."[218] However, digital actors are still cautious about sharing information on the division of work between technology and humans. This transparency is reduced even more when the moderation work is outsourced[219] or divided among various layers.[220]

451. Digital actors fighting against human trafficking. First, digital actors support the development of artificial intelligence tools dedicated to the repression of cyber trafficking or associated offenses, primarily sexual offenses against minors.[221]

---

[215] A.E. Waldman, *Disorderly Content*, *op. cit.* note 133, p. 12

[216] E.J. Llansó, "No amount of 'AI' in content moderation will solve filtering's prior-restraint problem," *Big Data & Society*, SAGE Publications Ltd, January 1, 2020, vol. 7, no. 1, p. 2

[217] A.M. Battesti, "La coopération des plateformes," *Legipresse*, 2019, vol. N° 61, no. HS1, p. 47. It was one of the recommendations of the French Conseil national du numérique to impose a human intervention for *ex ante* moderation, CNNum, "Ambition numérique Pour une politique française et européenne de la transition numérique - Rapport remis au Premier Ministère," République française, June 2015, p. 87

[218] A.E. Waldman, *Disorderly Content*, *op. cit.* note 133, p. 12

[219] K. Klonick, "The new governors: the people, rules, and processes governing online speech," *Harvard Law Review*, 2018, vol. 131, p. 1634. It is particularly complicated to provide a number of human moderators. It also questions the quality of those new job positions due to poor working conditions, high expectations for results, and a large amount of stress and mental health issues deriving from the moderation of violent content, see, for instance, N. Smyrnaios, E. Marty, "Profession « nettoyeur du net »," *Reseaux*, La Découverte, October 10, 2017, vol. n° 205, no. 5, pp. 56-90; S.T. Roberts, *Derrière les écrans*, *op. cit.* note 132; T. Gillespie, *Custodians of the internet*, *op. cit.* note 213, p. 120

[220] For instance, Facebook relies on "*three basic tiers of content moderators: 'Tier 3' moderators, who do the majority of the day-to-day reviewing of content; 'Tier 2' moderators, who supervise Tier 3 moderators and review prioritized or escalated content; and 'Tier 1' moderators, who are typically lawyers or policymakers based at company headquarters*," K. Klonick, "The new governors," *op. cit.* note 219, pp. 1639-1640

[221] For instance, a partnership was developed between Google and the US National Center for Missing and Exploited Children to enable the latter to use a recognition program originally developed for YouTube to spot child pornography online. A similar partnership exists with Microsoft, which developed the PhotoDNA program, meant to match images to spot the same pictures of child pornography, B. Westlake, M. Bouchard, R. Frank, "Comparing Methods for Detecting Child Exploitation Content Online," *2012 European Intelligence and Security Informatics Conference*, Odense, Denmark, IEEE, August 2012, p. 156, online http://ieeexplore.ieee.org/document/6298826/ (retrieved on February 9, 2021). This program is also used by other digital actors, such as Twitter, J. Charpenet, "Plateformes digitales et Etats : la corégulation par les données. Le cas des requêtes gouvernementales," *Revue internationale de droit économique*, 2019, vol. 2019/2, no. XXXIII, p. 380

For instance, "*Facebook created algorithms that analyze language, phone numbers, and images used on its platform in order to identify victims of online sex trafficking, with a particular focus on child victims*."[222] Major digital actors host hackathons "*to develop and test tools to combat online child sex trafficking*."[223] However, the primary goal of digital actors is not to act as law enforcement authorities in detecting illegal content but to moderate the content they host according to their terms of service. Therefore, the artificial intelligence systems[224] are designed to flag or delete content linked to sex trafficking, sex work, and sexuality or nudity as well as violence, fighting words, et cetera.

452. Mixed results from moderation. Despite declarations of good results,[225] artificial intelligence systems created to moderate these categories[226] are both overinclusive[227] and underinclusive, thereby questioning their efficacy.[228] Over inclusive results are not new, and FOSTA is just another justification to increase moderation of gray content. However, it remains questionable when these moderation

[222] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020, p. 45

[223] K. Guilbert, "Chasing shadows: can technology save the slaves it snared?," *Reuters*, June 21, 2018, online https://www.reuters.com/article/us-technology-trafficking-fight-insight-idUSKBN1JH005 (retrieved on March 18, 2021)

[224] It also must be underlined that digital actors share the detection of most violent content, such as "*extreme terrorist images and videos*," to make sure that the content is deleted on all platforms, T. Dias Oliva, "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression," *Human Rights Law Review*, December 9, 2020, vol. 20, no. 4, p. 627

[225] Zuckerberg considers that Facebook's systems "*proactively identify 96% of the nudity*," C. Are, "The Shadowban Cycle," *op. cit.* note 125, p. 3

[226] These results are obviously not limited to systems meant to spot sex trafficking, sex work, and nudity. For instance, TikTok developed a system to flag and reduce bullying. Instead, the result was the viral circulation of flagged accounts among "*chiefly people with disabilities and LGBTQ people*," leading to the opposite consequence, Glaad, *Social media safety index*, 2021, p. 9. Similarly, Twitter's system to delete fighting words results in the silencing of drag queens instead of violent, extreme right-wing speech, D.O. Thiago, A.D. Marcelo, A. Gomes, "Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online," *Sexuality & Culture*, Springer Nature B.V., 2021, vol. 25, no. 2, pp. 700-732

[227] In the case of overly inclusive systems, for example, when Tumblr decided to ban nudity, an automated system was used to clean the platform: It flagged "*pictures of whales, dolphins and Garfield being labeled as sexually explicit*," E. Pilipets, S. Paasonen, "Nipples, memes, and algorithmic failure," *op. cit.* note 100, p. 2 ; "*art, images of political protests, and utterly innocuous images of fully clothed women*," E. Morgan, "On FOSTA and the Failures of Punitive Speech Restrictions," *op. cit.* note 113, p. 529; and also "*people swimming, Disney characters, photos of vases, desserts, collarbones, knitting projects, and even personal text posts about sexual identity*," K. Tiidenberg, E. van der Nagel, *Sex and social media*, *op. cit.* note 129, p. 75. The YouTube system leads to systematic demonetization (although not deletion) of content "*featuring even such innocuous words as 'gay' or 'lesbian' or 'LGBTQ'*," Glaad, *Social media safety index*, *op. cit.* note 226, p. 19.

[228] Q. Van Enis, "Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression," *in* Q. Van Enis, C. de Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, pp. 136-137

rules are fully implemented by automatic systems or if they are checked by only a few human moderators located overseas, in the United States, or overseas, for instance, in the Philippines, where values are different. Furthermore, the broadening of illicit content based on terms of service—the conflation of sex trafficking with sex work and with sexuality and nudity—does not lead to the actual deletion of all of this content. In particular, even when sex trafficking and sex work are prohibited and moderated *ex ante*, they may remain on the platform. Indeed, users, including perpetrators of offenses, develop adaptation strategies. Key words will evolve[229] or their spelling will be changed,[230] and emoticons will be used instead.[231] Alternatively, content will migrate to other spaces that are less regulated.[232]

453. Origin of the systems. As with the artificial intelligence systems created for law enforcement authorities, these systems devised for use by digital actors have been developed mainly developed in the United States. Moreover, they are part of the confidential domain of the companies, making it difficult to obtain information on the data used to train the systems and the criteria established by their designers. Nevertheless, a few elements should be mentioned to question the values embedded in these systems. For instance, some rely on the ImageNet, an image database categorization system, to train their tools, which was mainly developed by US researchers. This database classified binary gender through human body images, thus "*naturalizing gender as a biological construct, which is binary, and transgender or gender non-binary people are either nonexistent or placed under categories of sexuality*."[233] Differently, the deletion of nudity, including only female nipples, on

[229] R. Gorwa, R. Binns, C. Katzenbach, "Algorithmic content moderation," *op. cit.* note 214, p. 5. For instance, Backpage's "*Strip Term From Ad filter appears to have been ineffective at deleting suspicious pricing due to the many possible variations involved*," Permanent subcommittee on investigations, *Backpage.com's knowing facilitation of online sex trafficking*, Committee on Homeland Security and Governmental Affairs, US, January 10, 2017, p. 33. Similarly, while Vivastreet created an automated tool to erase sex work from its platform based on certain keywords, advertisements were not deleted or only modified, L. Motet, "Vivastreet : les dessous de la prostitution par petites annonces," *Le Monde.fr*, February 2, 2017, online https://www.lemonde.fr/les-decodeurs/article/2017/02/02/vivastreet-les-dessous-de-la-prostitution-par-petites-annonces_5073149_4355770.html (retrieved on May 18, 2022)

[230] C. Callanan et al., *Rapport Filtrage d'Internet Equilibrer les réponses à la cybercriminalité dans une société démocratique*, Open Society Institute, October 2009, p. 118. For instance, if Twitter bans specific hashtags, the words will still be used without the hashtag, S. Paasonen, K. Jarrett, B. Light, *NSFW*, *op. cit.* note 132, pp. 17-22

[231] C. Stokel-Walker, "'What Does Seggs Mean?' The Rise of Sex Euphemisms on Social Media," *Vice*, February 2, 2022, online https://www.vice.com/en/article/7kbwx4/tiktok-instagram-shadowban-sex (retrieved on March 1, 2022); H.L. Barakat, E.M. Redmiles, "Community Under Surveillance," *op. cit.* note 104, p. 9

[232] E. Pilipets, S. Paasonen, "Nipples, memes, and algorithmic failure," *op. cit.* note 100, p. 6

[233] K. Crawford, *Atlas of Ai*, *op. cit.* note 182, p. 138

Instagram is impossible when pictures are closed,[234] which can lead to the conclusion that nipples alone were not considered as to be illicit but only when found linked to a woman, by, for example, the categorization of the face. This highlights specific values established by the programmers in the code.

454. American systems of artificial intelligence did not consider European standards to embed values in their code. Setting aside questions regarding freedom of expression, the use of artificial intelligence systems triggers the protection of other values established by criminal and digital laws. Artificial intelligence is "*simply the latest technologies*" at the core of the "*fights for time sovereignty*."[235] Since code "*has the power to usurp legal, institutional, and social norms impacting the political, economic and cultural domains of society*,"[236] European sovereignties are at risk of losing further independence, particularly considering the general lack of regulation of artificial intelligence systems.

§2. Regulating artificial intelligence to repress human trafficking

455. Artificial intelligence: the necessity of regulation. For years, the literature has called for the regulation of artificial intelligence due to its risks for society. The main risks are those of discrimination in applying automated systems;[237] those linked to the use of big data to train the systems, such as the protection of personal data,[238] the use

[234] T. Gillespie, *Custodians of the internet*, *op. cit.* note 213, p. 167
[235] K. Crawford, *Atlas of Ai*, *op. cit.* note 182, p. 85
[236] M. Kwet, "Digital colonialism," *op. cit.* note 181, p. 6
[237] F. Zuiderveen Borgesius, *Discrimination, Artificial Intelligence and Algorithmic Decision-Making*, *op. cit.* note 186. In particular, biases can originate from six sources: "*a misalignment between the world as it is and the values or objectives to be encoded*" (historical bias), an inadequate definition and sample of the development population (representation bias), inadequate features and labels (measurement bias), an inadequate combination of populations (aggregation bias), an inadequate model iteration and evaluation (evaluation bias), and an inadequate use or interpretation (deployment bias), A. Beduschi, M. McAuliffe, "Artificial intelligence, migration and mobility: Implications for policy and practice," *in* International Organization for Migration (ed.), *World Migration Report 2022*, May 21, 2020, p. 292. To sum up, biases can derive from humans involved with the system (designer, user) or from its data components (in particular, the training data). As such, for instance, due to human bias, the studied systems focus on sites offering mainly advertisements for sexual services provided by women, not allowing for reflection on potential male victims of trafficking in similar advertisements but located on different sites. As a technical bias, in the functioning of the systems to detect trafficking, the importance of the ethnicity criterion should be given special attention. In particular regarding racist discrimination, see S.U. Noble, *Algorithms of oppression: how search engines reinforce racism*, New York University Press, 2018; sexist discrimination, see C. Criado-Perez, *Invisible women: data bias in a world designed for men*, Abrams Press, 2019
[238] Committee of experts on internet intermediaries, *Algorithms and human rights*, *op. cit.* note 186, p. 12

of quality data,[239] and the reproduction of patterns;[240] the lack of transparency on their functioning and use;[241] and the risk of dissolving liabilities in cases of prejudice.[242] These risks are increased with the reduction of human intervention, particularly when using machine learning. This term "*refers to a category of [artificial intelligence] approaches in which algorithms automatically learn patterns from large amounts of data*."[243] It can be supervised, in which the system "*is presented with example inputs and their desired outputs*," or unsupervised, which leaves the system "*on its own to find structure in its input*."[244] Some law enforcement systems are based on unsupervised learning, particularly in the classification of extracted data and in the determination of advertisements considered to be at risk.[245] Moderation systems are also heavily based on machine learning and "*updated through iterative software updates*."[246] They shape "*users' behavior by distinguishing between legitimate and illegitimate expression*" through the identification of patterns and the making of predictions "*without having to explicitly reveal the norms being applied*."[247] Primarily, there is a risk of reduced independence.[248] These systems are orienting and will orient the decisions of law enforcement authorities, with the risk that humans will trust the

[239] European Union Agency for Fundamental Rights., "Data quality and artificial intelligence: mitigating bias and error to protect fundamental rights.," Publications Office, EU, 2019, p. 2, online https://data.europa.eu/doi/10.2811/546219 (retrieved on June 8, 2021)
[240] Défenseur des droits, CNIL, "Algorithmes : prévenir l'automatisation des discriminations," France, 2020, p. 4
[241] F. Pasquale, *The black box society: the secret algorithms that control money and information*, Harvard University Press, 2015; M. Perel, N. Elkin-Koren, "Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement," *Florida Law Review*, 2017, vol. 69, p. 180; J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," *Big Data & Society*, SAGE Publications Ltd, June 1, 2016, vol. 3, no. 1, pp. 1-12
[242] A. Matthias, "The responsibility gap: Ascribing responsibility for the actions of learning automata," *Ethics and Information Technology*, September 1, 2004, vol. 6, no. 3, p. 176
[243] H. Surden, "Ethics of AI in Law: Basic Questions," *in* M.D. Dubber, F. Pasquale, S. Das (eds.), *The Oxford Handbook of Ethics of AI*, Oxford University Press, July 9, 2020, p. 722
[244] M. Broussard, *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018, p. 93
[245] L. Li et al., "Detection and Characterization of Human Trafficking Networks Using Unsupervised Scalable Text Template Matching," *IEEE International Conference on Big Data*, December 2018, pp. 3111-3120, https://ieeexplore.ieee.org/document/8622189; M. Kejriwal et al., "FlagIt," *op. cit.* note 207; H. Alvari, P. Shakarian, J.E.K. Snyder, "Semi-supervised learning for detecting human trafficking," *Security Informatics*, December 2017, vol. 6, no. 1, p. 1
[246] K. Klonick, "The new governors," *op. cit.* note 219, p. 1637. See also N. Elkin-Koren, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence," *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, pp. 1-13
[247] N. Elkin-Koren, "Contesting algorithms," *op. cit.* note 246, p. 6
[248] In particular, "*Studies show that human beings rely on automated decisions even when they suspect system malfunction*," D.K. Citron, "Technological Due Process," *Washington University Law Review*, January 1, 2008, vol. 85, no. 6, p. 1271

software rather than their own expertise.[249] The systems are also defining what the user will see online through content moderation and personalization, chaining the user to a "filter bubble" and limiting pluralism of opinion.[250]. On a broader level, a risk is posed to the autonomy of law with the new definition of legal categories and regimes by artificial intelligence systems.[251] However, artificial intelligence could further reduce the autonomy of the sovereign states, an element that has been hardly mentioned in the literature.

456. Despite the need for artificial intelligence systems to combat cyber trafficking, these tools are not neutral. They depend "*entirely on a […] set of political and social structures*"[252] and "*[anchor] public values*,"[253] but the question remains about who should define these values. The states' (lack of) ability to develop, use, and regulate artificial intelligence systems, therefore, can affect their sovereignty due to the interconnectedness of new technologies. In particular, artificial intelligence systems to repress cyber trafficking might influence both European criminal sovereignty (I) and digital sovereignty (II).[254]

I. Threatening European criminal sovereignty

457. Defining human trafficking for artificial intelligence systems. Despite its international definition, the concept of human trafficking is not fully harmonized. First, the Palermo Protocol was adapted and broadened by European texts,[255] adding types of exploitation and suppressing the criterion of a transnational process. Second, including within Europe, national definitions highlight a wide variety of transpositions.[256]. For instance, compared to the French definition, the Spanish code

[249] L. Viaut, "Droit et algorithmes : réflexion sur les nouveaux processus décisionnels," *Petites affiches*, September 4, 2020, no. 177-178, p. 8
[250] E. Pariser, *The filter bubble: how the new personalized web is changing what we read and how we think*, Penguin Books, 2014
[251] J.-B. Prévost, "La fabrique des données : à propos du codage numérique du droit et de ses limites," *Gazette du Palais*, January 22, 2019, no. 03, p. 84
[252] K. Crawford, *Atlas of Ai*, *op. cit.* note 182, p. 8
[253] J. van Dijck, "Guarding Public Values in a Connective World: Challenges for Europe," *op. cit.* note 26, p. 175 In particular, their development by digital actors supports their power "*through the invisible mechanisms underlying the platform ecosystem, such as the steering of data flows, […] invisible selection criteria, and algorithmic lock-ins that facilitate path dependency*," *Ibid.* p. 177
[254] Part of this work was published in S. Lannier, "Using US Artificial Intelligence to Fight Human Trafficking in Europe. Potential Impacts on European Sovereignties," *Eucrim*, 2023, vol. 01/2023
[255] Warsaw Convention and Directive 2011/36/EU
[256] See *supra* 19. The case law also highlights the potential for multiple interpretations of the concept, L. Esser, C. Dettmeijer-Vermeulen, "The Prominent Role of National Judges in Interpreting the International Definition of Human Trafficking," *Anti-Trafficking Review*, 2016, vol. 6, pp. 91-105; E.

defines the exchange or transfer of control over victims as "action" and forced marriage as "exploitation." The French code defines the situation of vulnerability as based on "*age, illness, infirmity, physical or mental disability, or pregnancy*," while the Spanish code defines it as "*when the person concerned has no real or acceptable alternative but to submit to the abuse*."[257] In Romania, the code does not list forms of exploitation.[258] In Belgium, coercive means are not an element of the offense but an aggravating circumstance.[259] The comparison is particularly noticeable between European definitions and the US code, which considers trafficking only with respect to peonage, slavery, involuntary servitude or forced labor, and sex trafficking.[260] Therefore, a system of artificial intelligence to repress human trafficking should adapt to national definitions. However, the definition used for artificial intelligence systems remains the American one, since the United States is the origin country of these systems.

458. Establishing criminal priorities. Another problem lies in the fact that the development of these systems depends on a country's criminal realities and priorities, especially regarding the types of exploitation. For instance, in Europe, there is an increasing focus on trafficking for labor exploitation.[261] However, systems of artificial intelligence developed in the United States focus on the repression of trafficking for (mainly domestic) sexual exploitation.[262] As the existing systems are mainly American, they affect worldwide priorities in the fight against the complex and multifaceted phenomenon of trafficking. This situation supports the continuous focus on sexual

Coreno, "Finding the Line between Choice and Coercion: An Analysis of Massachusetts's Attempt to Define Sex Trafficking," *Northeastern University Law Review*, 2021, vol. 13, no. 1, pp. 124-174

[257] Article 177bis of the Código penal and Article 225-4-1 of the Code pénal

[258] Article 210 of the Codul penal

[259] Articles 433 quinquies and 433 septies of the Belgium Code pénal

[260] 18 USC § 1590 and § 1591

[261] GRETA, "Guidance note on preventing and combatting trafficking in human beings for the purpose of labour exploitation," Council of Europe, December 2020, GRETA(2020)12; European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," EU, April 14, 2021, pp. 7-8, COM(2021) 171 final

[262] Most papers are misleading as they target human trafficking in general while their content specifically focuses on sex trafficking, see, for instance, M. Ibanez, D. Suthers, "Detection of Domestic Human Trafficking Indicators," *op. cit.* note 192, pp. 1556-1565; A. Dubrawski et al., "Leveraging Publicly Available Data," *op. cit.* note 149, pp. 65-85; P. Szekely et al., "Building and Using a Knowledge Graph," *op. cit.* note 198, pp. 205-211. Law enforcement systems analyze classified advertisements almost exclusively. In particular, the systems emphasize the identification of minor victims, B. Westlake, M. Bouchard, R. Frank, "Comparing Methods for Detecting Child Exploitation Content Online," *op. cit.* note 221, pp. 156-163; H. Wang et al., "Data integration from open internet sources to combat sex trafficking of minors," *op. cit.* note 194, p. 245; D. Roe-Sepowitz et al., *Online Advertisement Truth Set Sex Trafficking Matrix*, *op. cit.* note 198

exploitation,[263] which has been highly criticized as a narrowly focused conception of human trafficking.[264]

459. Conflating sex trafficking and sex work. At the crossroads of defining human trafficking and establishing criminal policy priorities, these tools also embed a specific American policy: their approach to sex work. To qualify as adult sex trafficking, the US Code requires only a commercial sex act as the purpose. However, proof is required for "*means of force, threats of force, fraud, [or] coercion*."[265] Nevertheless, indicators of trafficking in sex workers' advertisements hardly take this element into account; they rely only on indirect potential flags of exploitation,[266] since it is obviously rare to find explicit proof of coercion in the advertisements). Furthermore, many US scholars conflate trafficking and sex work, not framing their work within this debate, and, therefore, implicitly applying the US official positioning.[267] Researchers and sex workers joined in their criticism of the criteria as being unable to detect victims of trafficking instead as discriminating among sex workers.[268] Similarly, most digital

[263] Only two European papers tried to develop systems applied to job advertisements, with limited success, R. McAlister, "Webscraping as an Investigation Tool to Identify Potential Human Trafficking Operations in Romania," *Proceedings of the ACM Web Science Conference on ZZZ - WebSci '15*, Oxford, United Kingdom, ACM Press, 2015, pp. 1-2, online http://dl.acm.org/citation.cfm?doid=2786451.2786510 (retrieved on November 28, 2020); A. Volodko, E. Cockbain, B. Kleinberg, "'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers," *Trends in Organized Crime*, 2020, no. 23, pp. 7-35

[264] J. Chuang, "Giving as Governance? Philanthrocapitalism and Modern-Day Slavery Abolitionism," *UCLA law review*, August 1, 2015, vol. 62, p. 1522

[265] 18 USC § 1591(a)

[266] Setting aside criteria linked to underage victims: shared management, geographic displacements, E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, *op. cit.* note 192; shared phone number, M. Latonero, *Technology-Facilitated Trafficking*, *op. cit.* note 193; inconsistencies in the story, third party language, ethnicity, potential restricted movement ("in calls only"), M. Ibanez, D. Suthers, "Detection of Domestic Human Trafficking Indicators," *op. cit.* note 192, pp. 1556-1565; unconventional sex advertised, disguised phone number, transient language, M. Hultgren, *An exploratory study of the indicators of trafficking*, *op. cit.* note 195. On the contrary, considering weak signals of coercion such as "*physical injury, subjected to violence, timid, forced to have sex, women beaten*" in tweets, S. Andrews, B. Brewster, T. Day, "Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online," *Security Informatics*, December 2018, vol. 7, no. 1, p. 3; and "*impairment (vulnerability) under the influence of drugs or alcohol, symptoms of mental illness or impairment*," D. Bounds et al., "Uncovering Indicators of Commercial Sexual Exploitation," *op. cit.* note 149, pp. 5607-5623

[267] On the contrary, explicitly trying to differentiate between consensual sex work and sexual exploitation, see E. Simonson, *Semi-Supervised Classification of Social Media Posts: Identifying Sex-Industry Posts to Enable Better Support for Those Experiencing Sex-Trafficking*, Master thesis, Massachusetts Institute of Technology, April 7, 2021; B. Cartwright et al., *Deploying artificial intelligence to detect and respond to the use of digital technology by perpetrators of human trafficking*, International CyberCrime Research Centre - Simon Fraser University, April 2022

[268] R. Kjellgren, "Good Tech, Bad Tech: Policing Sex Trafficking with Big Data," *International Journal for Crime, Justice and Social Democracy*, March 1, 2022, vol. 11, no. 1, pp. 149-166; M. Draughn, "No Ground Truth: Sex Trafficking and Machine Learning," *Windypundit*, July 27, 2022, online

actors embed in their artificial intelligence systems a prohibitionist approach through the automated deletion of content that includes sexual service solicitation. It is easier to conflate the two when programming software to repress human trafficking, as the components of human trafficking rarely will be visible in online content. Since sex work also might be difficult to spot, the broadening of moderation to sexuality and nudity facilitates binary decision-making, independently from context. Consequently, this conflation is embedded in the functioning of most systems of artificial intelligence. Therefore, their use in Europe, particularly in countries where sex work policies are different, could affect the independence of criminal sovereignty.

460. Considering criminal realities. A last example of the embedding of US criminal sovereignty in these tools lies in the criteria used to detect at-risk advertisements. These advertisements were identified on the basis of American experts[269] and databases.[270] The criteria focus on the detection of domestic sex trafficking, but, they might be unsuitable for European criminal realities: European trafficking is highly intra-regional,[271] and, within the EU, only 37% of the victims suffered domestic trafficking.[272] According to the UNODC, in Western and Southern Europe, sexual exploitation accounted for only 45% of the victims detected in 2020.[273]

---

https://windypundit.com/2022/07/no-ground-truth-sex-trafficking-and-machine-learning/ (retrieved on August 23, 2022)

[269] Including from law enforcement authorities, H. Alvari, P. Shakarian, J.E.K. Snyder, "Semi-supervised learning for detecting human trafficking," *op. cit.* note 245, p. 1; A. Dubrawski et al., "Leveraging Publicly Available Data," *op. cit.* note 149, pp. 65-85 (although the keywords highlighted could be seen as very lightly linked to human trafficking: "nice," "body," etc.); collaboration with actual investigators and domain experts, M. Kejriwal, P. Szekely, C. Knoblock, "Investigative Knowledge Discovery for Combating Illicit Activities," *op. cit.* note 205, pp. 53-63; M. Kejriwal, P. Szekely, "Knowledge Graphs for Social Good," *op. cit.* note 205, pp. 1-15; collaboration with "experimented" experts, E. Tong et al., "Combating Human Trafficking with Multimodal Deep Models," *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Vancouver, Canada, Association for Computational Linguistics, July 2017, pp. 1547-1556, online https://aclanthology.org/P17-1142 (retrieved on February 10, 2023). However, the research is not transparent about the status and experience of these experts.

[270] For instance, D. Roe-Sepowitz et al., *Online Advertisement Truth Set Sex Trafficking Matrix*, *op. cit.* note 198, that relies on 461 advertisements of confirmed underage victims; or L. Li et al., "Detection and Characterization of Human Trafficking Networks," *op. cit.* note 245, pp. 3111-3120; L. Wang et al., "Sex Trafficking Detection with Ordinal Regression Neural Networks," *ArXiv:1908.05434 [cs, stat]*, January 11, 2020, online http://arxiv.org/abs/1908.05434 (retrieved on May 20, 2021), that rely on the database Trafficking10K developed by Marinus Analytics.

[271] UNODC, *Global report on trafficking in persons 2022*, UN, January 2023, p. 160

[272] European Commission, "Commission Staff Working Document Statistics and trends in trafficking in human being in the European Union in 2019-2020 Accompanying the document Report on the progress made in the fight against trafficking in human beings (Fourth Report)," EU, December 19, 2022, p. 9, SWD(2022) 429 final

[273] UNODC, *Global report on trafficking in persons 2022*, *op. cit.* note 271, p. 159. However, these criteria could better fit the Central and South-Eastern Europe region, where 79% of detected victims

Although indicators were published by the UNODC,[274] they are dedicated to the detection of victims in general and are not operational for their programming into artificial intelligence systems. Therefore, non-American research relies mainly on criteria established in the United States,[275] although criminal realities differ. Finally, it must be underlined that artificial intelligence systems reproduce what they are programmed to detect: They encode systematic patterns.[276] This leads to reproducing criteria already criticized without debate or adaptation to national context and crime evolution.

461. Artificial intelligence tools are useful to detect trafficking. Nevertheless, they are not neutral; since they were developed mainly developed in the United States, they highlight and reproduce the American definition of sex trafficking, the American prohibitionist policies, and American priorities regarding the repression of human trafficking. If these artificial intelligence tools are used in Europe, the limitations of these systems would hinder the full independence of European states' criminal sovereignty. Furthermore, these tools might threaten European digital sovereignty.

II. Threatening European digital sovereignty

462. Data and technical sovereignties. The concept of digital sovereignty highlights the contradiction between the theoretical independence of states and the "de facto *disparities of power among states, which, in turn, might limit their capacity to act, to regulate and to freely adopt decisions*."[277] Data sovereignty is understood as

come from domestic trafficking processes and 63% of them are trafficked for sexual exploitation, *Ibid.* pp. 148-149

[274] UNODC, "Human trafficking indicators," UN, 2020, online https://www.unodc.org/pdf/HT_indicators_E_LOWRES.pdf (retrieved on October 10, 2021)

[275] B. Seiler, *Analyse de la traite d'êtres humains sur Internet : le cas de la prostitution en Suisse romande*, Mémoire de maîtrise, Université de Lausanne, July 2017; B. Cartwright et al., *Deploying artificial intelligence*, *op. cit.* note 267; L. Giommoni, R. Ikwu, "Identifying human trafficking indicators," *op. cit.* note 211. In particular, some American research uses the same criteria for the US and Canadian contexts, A. Dubrawski et al., "Leveraging Publicly Available Data," *op. cit.* note 149, pp. 65-85; R. Rabbany, D. Bayani, A. Dubrawski, "Active Search of Connections for Case Building and Combating Human Trafficking," *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, London United Kingdom, ACM, July 19, 2018, pp. 2120-2129, online https://dl.acm.org/doi/10.1145/3219819.3220103 (retrieved on May 1, 2021)

[276] M. Veale, *Algorithms in the Criminal Justice System*, The Law Society Commission on the Use of Algorithms in the justice System, The Law Society of England and Wales, July 2019, pp. 18-24

[277] T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, p. 6

"*the ability to store and process certain types of data*."[278] Traditional sovereignty centers on exercising control over data. Interpreted through the lens of human rights, sovereignty includes the protection of the population through their personal data. As such, data, especially personal data, are a "*genuine power issue between States*."[279] The EU's digital sovereignty rests on an innovative approach to protect these data. However, European digital sovereignty also encompasses technical sovereignty through the regulation of certain aspects of technologies. This sovereignty is of particular interest regarding artificial intelligence due to its specific characteristics and risks. Therefore, protecting the technical sovereignty must rest on standards other than those from the personal data protection framework, developed particularly within the EU.

463. The development of artificial intelligence systems to combat human trafficking should be framed by EU legislation to protect its data sovereignty (I) and technical sovereignty (II). When facing American systems, their adaptation to European standards should be at the core of their exportation.

A. Questioning the protection of data sovereignty

464. Use of personal (and sensitive) data. Personal data are defined in the EU framework as "*any information relating to an identified or identifiable natural person*."[280] The veracity of the data is not relevant as long as a person is identifiable.[281] Even when a pseudonym is used, other information can make a person identifiable,[282] and law enforcement authorities can request complementary data from other sources to

[278] K. Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet*, 2012, vol. 4, no. 3-4, p. 62

[279] M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 22

[280] Article 4.1 of the GDPR and Article 3.1 of Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data

[281] Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data," EU, June 20, 2007, p. 7. Indeed, it is in the interest of the perpetrators to age the minor victims or to lie about the ethnic origin of certain victims certain nationalities carry underlying sexual stereotypes that are often racist and sexist (for example, the naivety and passivity of some nationalities in Asian countries), T. Sanders et al., "The Point of Counting: Mapping the Internet Based Sex Industry," *Social Sciences*, Science Publishing Group, October 22, 2018, vol. 7, no. 5, p. 239

[282] O. Tambou, J.F. López Aguilar, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, Droit administratif no. 28 28, 2020, p. 78, referring to Y.-A. de Montjoye et al., "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, January 30, 2015, vol. 347, no. 6221, pp. 536-539

achieve this aim.[283] Digital actors' moderation systems and business models are supported mainly by the processing of personal data. As personal data are widely interpreted by the CJEU,[284] it is clear that the extracted data from both types of systems can qualify as personal data and then affect data sovereignty. Data sovereignty is further triggered by processing sensitive data, which requires particular guarantees. Sensitive data are defined as data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, […] genetic data, biometric data […], data concerning health, or data concerning a natural person's sex life or sexual orientation*."[285] Regarding law enforcement systems, it seems evident that, while not all extracted data are sensitive, some are. This would include data indicating racial or ethnic origin, with information on nationality, country, or region of origin; data on the health of the person, including weight or evidence of physical violence; and data on the sexual life of the person, when the advertisements list the sexual services that may be performed. Regarding moderation systems, they can flag political opinions around sex work, content linked to a person's intimate life, et cetera.

465. Applicable framework: law enforcement. Law enforcement systems are dedicated to the detection and investigation of human trafficking. They are used by "*a public authority or any entity with public powers*."[286] As such, the data protection regime lies in Directive 2016/680.[287] Although the Directive establishes more lenient obligations than those in the GDPR,[288] it still lists main principles to be embedded by design, which are summarized as follows: lawful and fair processing, delimited by specific purposes; limitation of the collection and conservation of data; data accuracy,

[283] CJEU, *Patrick Breyer v. Bundesrepublik Deutschland*, October 19, 2016, C-582/14, ¶ 49. However, it must be underlined that its very applicability could be compromised "*if no individual can be formally identified or if the regulation is seen as focusing on raw input data, the protection offered by the regulatory framework could be considered inapplicable to [an algorithm] that would map [...] behaviors attributable to general groups of individuals*," Y. Meneceur, *L'intelligence artificielle en procès*, *op. cit.* note 183, p. 290. This caveat could be applied to the systems aimed at determining the geographic "hot spots" of risky ads.

[284] For instance, ECJ, *Bodil Lindqvist*, November 6, 2003, C-101/01

[285] Article 9.1 of the GDPR and Article 10 of the Directive 2016/680. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, 1981), updated by the amending protocol of 2018, adds "*personal data relating to offenses, criminal proceedings and convictions, and related security measures*," Article 6.1

[286] O. Tambou, J.F. López Aguilar, *Manuel*, *op. cit.* note 282, pp. 99-100

[287] Article 2.2 of the GDPR and Article 1.1 of the Directive 2016/680

[288] In particular regarding the principle of transparency, and information and deletion obligations, the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, O. Tambou, J.F. López Aguilar, *Manuel*, *op. cit.* note 282, pp. 130-131, 188-194, 202

integrity, and confidentiality; and the liability of data processors.[289] However, when artificial intelligence systems are developed in the United States for American use, they do not fall within the scope of the European framework. Therefore, it is doubtful that personal data protection is embedded from the start of their development. Since the transparency principle is absent from the directive, the guarantees to control the use of these systems are particularly relevant to balance the interference with the right to privacy. Another important point is the localization of the processed data. Indeed, it would be particularly sensitive to store European data related to criminal investigations in the United States if the systems use a cloud version saved on US servers. The Directive provides for the possibility of transferring data outside the EU;[290] specifically, the EU–US Data Protection Umbrella Agreement was signed between the EU and the US on this matter in 2016.[291] A few months earlier, the Privacy Shield[292] established a supposedly adequate level of data protection for data transfers for commercial and civil purposes, but it was invalidated by the CJEU.[293] On the contrary, the lawfulness of the Umbrella Agreement has not been questioned. As these artificial intelligence systems process large quantities of data, including, sensitive data, the effectiveness of safeguards when data are transferred abroad should be the focus of scrutiny.

466. Applicable framework: digital actors. Digital actors' systems might be used to identify human trafficking content. When that is the main goal of these systems, the question will rest in the interpretation of the concept of "*body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses*."[294] If member states regulate a protocol of cooperation to require digital actors to use their systems to detect human trafficking and to transfer this information to law enforcement authorities, the Directive 2016/680 could apply. Nevertheless, until now, these systems were used mainly for general content moderation. As such, the GDPR applies. Two concepts will be particularly useful to regulate artificial intelligence: automated

[289] Article 4 of Directive 2016/680
[290] Articles 35 to 40 of Directive 2016/680
[291] Agreement between the United States and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses, 2016
[292] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176)
[293] CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*, July 16, 2020, C-311/18
[294] Article 3.7.b of the Directive 2016/680

decision-making[295] and profiling. The former would be applicable when content moderation is fully automated, and the latter when the processing means "*to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements*."[296] In both situations, the GDPR offers additional rights to the user, including information on "*the logic involved* […] *to ensure fair and transparent processing,"*[297] a right to obtain human intervention, and a limitation on the use of sensitive data.[298] Therefore, the GDPR is limited only on how the processing through automated means is programmed. However, these concepts "*ha[ve] hardly been applied in practice*,"[299] and these few provisions are insufficient to regulate the specificities of artificial intelligence.[300]

467. The processing of data to identify human trafficking affects EU data sovereignty; in fact, data protection by design is unlikely due to its origin. Furthermore, the frameworks for data protection are highly criticized for not considering the specific risks linked to artificial intelligence. Therefore, the protection of EU digital sovereignty should seek other standards.

B. Questioning the protection of technical sovereignty

468. A proposal for an Artificial Intelligence Act. Due to the limitations of the EU personal data protection framework, the European Commission published a

---

[295] By principle, the GDPR prohibits the imposition of "*a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affect*" the individual, Article 22.1. It could be argued that content moderation and the automatic deletion of content significantly affect an individual and may reduce a fundamental right, their freedom of expression. Exceptions exist when this processing derives from a contract or is based on the user's consent; this condition is checked by the consent to digital actors' terms of service.

[296] Article 4.4 of the GDPR

[297] Articles 13.2.f, 14.2.g and 15.1.h of the GDPR. On the right to information, see L. Edwards, M. Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review*, December 4, 2017, vol. 16, no. 1, pp. 18-84; S. Wachter, B. Mittelstadt, L. Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law*, May 2017, vol. 7, no. 2, pp. 76-99

[298] Article 22.3 and 4 of the GDPR, the latter requires explicit consent from the user or to be "*necessary for reasons of substantial public interest, on the basis of Union or Member State law,*" Article 9.2.a and g

[299] F.J. Zuiderveen Borgesius, "Strengthening legal protection against discrimination by algorithms and artificial intelligence," *The International Journal of Human Rights*, Routledge, November 25, 2020, vol. 24, no. 10, pp. 1579-1580

[300] C. Castets-Renard, "Régulation des algorithmes et gouvernance du machine learning : vers une transparence et 'explicabilité' des décisions algorithmiques ?," *Revue Droit&Affaires*, Revue Paris II Assas, November 2018, no. 15, p. 47

proposal for an Artificial Intelligence Act in 2021[301] was amended by the European Parliament in June 2023[302] This act would apply whenever the systems are used by European users, including law enforcement authorities[303] As these systems are to be used for the repression of offenses[304] they are classified as high-risk and comply with the maximum obligations transparency are excluded for these systems[305] However, it should be underlined that the European Parliament erased from the list of prohibited artificial intelligence systems those based on biometric identification for "*the targeted search for specific potential victims of crime, including missing children*[306] added at the same time the prohibition of systems "*for predicting the occurrence or reoccurrence of an actual or potential criminal or administrative offense based on profiling of a natural person or on assessing personality traits and characteristics, including the person's location*."[307] Facing this draft, it these systems to detect trafficked victims be allowed within the EU. Regarding moderation systems, they are not considered high-risk,[308] while recommender systems of social media that are qualified as very large online platforms are.[309] Furthermore, the lack of transparency requirements and the protection of these systems by intellectual property rights might challenge the access to technical components to ensure a lack of violation of fundamental rights. Nevertheless, to ensure the protection of fundamental rights, the European Parliament

[301] European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, April 21, 2021, COM/2021/206 final. This proposal is coherent with prior recent legal developments pushing towards more use of automated tools to reach policy goals, C. Katzenbach, "'AI will fix this' – The Technical, Discursive, and Political Turn to AI in Governing Communication," *Big Data & Society*, SAGE Publications Ltd, July 1, 2021, vol. 8, no. 2, p. 5. However, regarding detection of terrorism-related content, the new regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online prohibits the requirement to digital actors to use automated tools, Article 5.8

[302] European Parliament, Amendments on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, June 14, 2023, P9_TA(2023)0236. The version including these amendments will be studied.

[303] Article 2.2 of the Artificial Intelligence Act Proposal

[304] Article 7.1 in relation to Annex III.1.6 and 5.c of the Artificial Intelligence Act Proposal

[305] Article 52.1 of the Artificial Intelligence Act Proposal

[306] Article 5.1.d.i of the Artificial Intelligence Act Proposal (European Commission version)

[307] Article 5.1.d a of the Artificial Intelligence Act Proposal

[308] The transparency obligation includes, after the European Parliament amendments, the obligation to provide information on "*which functions are AI enabled, if there is human oversight, and who is responsible for the decision-making process, as well as the existing rights and processes that, according to Union and national law, allow natural persons or their representatives to object against the application of such systems to them and to seek judicial redress against decisions taken by or harm caused by AI systems, including their right to seek an explanation*," Article 52.1 of the Artificial Intelligence Act Proposal.

[309] Annex III.1.5.a b of the Artificial Intelligence Act Proposal

added general principles to guide the development of artificial intelligence systems, including human agency and oversight, technical robustness and safety, privacy and data governance, and transparency.[310] While this act is still under negotiation, the CJEU developed guidelines to regulate automated systems used for law enforcement purposes.[311]

469. CJEU 2017 standards. Since 2017, the CJEU has recognized the possibility for data to be "*subject to analyses by automated means, based on pre-established models and criteria and on cross-checking with various databases*."[312] While the court does not specifically identify the notion of artificial intelligence, the description matches the concept. The court highlights the possible error rate, which is not negligible, especially because the data are not checked during their analysis,[313] as is done with some anti-trafficking systems. Therefore, the CJEU declares that the non-discrimination clause, the limited purposes, and the prohibition of "*any decisions significantly adversely affecting a [person] solely on the basis of automated processing*," established by the data protection framework, are not sufficient guarantees.[314] Then, the court introduces additional ones. First, "*The pre-established models and criteria should be specific and reliable, making it possible […] to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in […] serious transnational crime*." Additionally, these models and criteria must be "*non-discriminatory*." Concerning the source databases, data "*must be reliable, up-to-date and limited to databases used […] against […] serious transnational crime*."[315] Second, the CJEU states a principle of human intervention: "*Any positive result [must] be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the [persons] concerned is adopted*."[316] Finally, reviews of the use of these tools must be planned to verify

[310] Article 4 a of the Artificial Intelligence Act Proposal
[311] A. Sachoulidou, "Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence," *Artificial Intelligence and Law*, February 22, 2023, pp. 42-43
[312] CJEU, *Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data*, July 26, 2017, Opinion 1/15, ¶ 168
[313] *Ibid.* ¶¶ 169-170
[314] *Ibid.* ¶ 171
[315] *Ibid.* ¶ 172. The non-discrimination principle was already considered in the Directive 2016/680, Article 11.3
[316] *Ibid.* ¶ 173. A human intervention principle could already be found in the Directive 2016/680, Article 11.1

compliance with the above principles.[317] As a result, this decision provides new obligations for artificial intelligence systems to comply with European fundamental rights.

470. CJEU 2020 standards. In 2020, the CJEU developed these standards,[318] and the court maintains most of the previous criteria.[319] However, the principle of limitation of the source databases is modified. Indeed, the automated processing studied covered "*generally and indiscriminately, the data of persons using electronic communication systems [therefore applying] to all persons who use electronic communication systems*."[320] To compensate for the lack of objective and subjective data limitations, the court establishes additional safeguards. In particular, the implementation of such a system can take place only "*in the face of a serious threat to national security*."[321] Then, anti-trafficking systems will be unable to extract data in a generalized and indiscriminate way, as they are used in a criminal framework and not as a tool to prevent a threat to national security. As these systems are usually limited to specific websites, they could hardly be seen as generally and indiscriminately extracting data.

471. Conclusion of the section. To summarize, the use in Europe of US artificial intelligence systems is not only a potential development in terms of law enforcement tools to investigate cyber trafficking but is already happening through the worldwide application of digital actors' moderation systems. These artificial intelligence systems threaten the autonomy of European sovereignties by highlighting a clear imperialism of American code. The use of artificial intelligence implies many risks, and it embeds specific values and policies. Its extension through a global application of technical solutions "*amounts to standardizing national legal systems by stripping them of their*

---

317 *Ibid.* ¶ 174

318 W. Maxwell, "La CJUE dessine le noyau dur d'une future régulation des algorithmes," *Légipresse*, 2020, p. 671

319 CJEU, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs v. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées ; and Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministres*, October 6, 2020, C-511/18, C-512/18, C-520/18, ¶¶ 180-182

320 *Ibid.* ¶ 174

321 Additional requirements are the following: "*It is essential that the decision authorizing automated analysis be subject to effective review, either by a court or by an independent administrative body whose decision is binding*," data retention period must be strictly limited; the processing should not be based only on sensitive data; and "*The competent national authority is obliged to publish information of a general nature relating to that analysis*," *Ibid.* ¶¶ 177-191

particularities."[322] As for human trafficking, artificial intelligence systems rely on a specific national definition and representation of criminological realities regarding particular criminal policy priorities and a conception of trafficking that is conflated with sex work. This American framework further impedes digital sovereignty due to the lack of data protection by design. Moreover, the data protection norms do not consider the specificities of artificial intelligence, leading to their inadequacy for the systems studied. The EU is attempting to strengthen its standards applicable to artificial intelligence to protect its technical sovereignty, but these standards are, for now, still limited.

472. Conclusion of the chapter. Today, efforts are being made to implement new power dynamics between sovereigns. In particular, a specific country is taking advantage of its close connection to the new sovereigns, the digital actors. As these digital actors operate worldwide, the American influence is exported through a variety of techniques. First, direct consequences derive from the application of the core powers of sovereignty: coercion and sanctions. By imposing its criminal framework and policies on digital actors, the United States exercises an independent sovereign decision linked to an approach to human trafficking conflated with sex work. However, these actions have also affected foreign jurisdictions. Since sex work is the focus of multiple regulations around the globe, this situation impedes the independence of foreign states, underscoring US criminal imperialism. Second, indirect consequences are implemented by digital actors. As they might be liable for hosting content linked to human trafficking, they moderate this content, and to facilitate this task, they conflate trafficking with sex work as well as sexuality and nudity. It leads to the deletion, as collateral damage, of some portions of political debates and the life experiences of discriminated groups. As moderation happens (almost) worldwide on the basis of (almost) similar rules, it triggers the independence of European sovereignty through the media imperialism of the United States. Finally, the consequences of the extended US policies on human trafficking are also embedded in artificial intelligence systems, both dedicated to supporting the work of law enforcement authorities or of moderation. This situation highlights the imperialism of an American code, both potential and real. These systems embed local values, political approaches, and priorities through the criteria established for their functioning or the data selected to train them. However,

[322] G. Kettani, "Quand l'algorithme écrit le droit : les conséquences de la nouvelle normativité numérique," *Dalloz IP/IT*, Dalloz, 2022, p. 556

both human rights and data protection frameworks seem somewhat inappropriate to protect European sovereignties. They do not consider the interconnectedness of power exercise, the role of digital actors, and their control over cyberspace through code as a medium for ordering states' independence and sovereign powers. They lack comprehensive protection for people as users of the digital actors' services.

473. Conclusion of the title. The theory of sovereignty creates independent entities, particularly in regulating and setting priorities to repress cyber human trafficking. However, this criterion of independence barely fits the relationships that have been developed between states and digital actors as well as between states. Certain national strategies against trafficking denied the independence of digital actors and their role in this fight by triggering their criminal liability. Despite applying broad criteria to reach legal persons' criminal liability, many questions around the application of online intermediaries' liability made the outcome of this strategy uncertain. Furthermore, the definition of human trafficking is barely applicable to the acts and omissions committed by digital actors. Instead of investigating other ways of ordering their means of coercion, states, especially the United States, decided in favor of legal reforms to facilitate the prosecution of digital actors. However, the drafting of both the new online intermediaries' liability and of new criminal offenses questions their positive impact on the repression of human trafficking, as the liability framework creates further uncertainty and questions its proportionality with other public interests, including the protection of fundamental rights. Nevertheless, to avoid liability, digital actors integrated the repression of human trafficking into their own policies; they became the gatekeepers of the Internet by preventing potential victims and traffickers from using their services. This action lessens the actors' independence in establishing their own priorities, and it questions the effectiveness of deletion as a strategy to reduce human trafficking. Going further, embedding these priorities and policies into digital actors questions foreign states' independence, as digital actors apply their solution worldwide. The repression of human trafficking requires national regulations and policies that can vary in a relevant manner. In particular, states must decide on the relationships between the regulation of human trafficking and sex work. Today, the US prohibitionist position has been integrated by digital actors and by coded technologies used to repress human trafficking. When these private policies and these tools expand abroad, the capacity of other states to regulate these topics is reduced, questioning the adequacy of the independence criteria of sovereignty. Their independence is specifically reduced because European human rights frameworks are not appropriate to respond to these threats to sovereignty. Critically, these threats to independence, by exercising coercion between sovereign holders, do not seem to reach their goals of comprehensively repressing cyber human trafficking. However, when enhancing collaboration between sovereigns, a reduction in independence might support the fight

against this phenomenon.

TITLE 2. ENFORCING COLLABORATION BETWEEN SOVEREIGNS TO REPRESS CYBER TRAFFICKING

474. The enforcement of coercion between sovereign actors to repress cyber human trafficking is highly criticized. On the one hand, this state strategy seems to imperfectly achieve its objectives, meaning, the protection of victims and the conviction of traffickers. On the other hand, this strategy threatens the independent sovereignty of the various sovereign actors. As a consequence, by setting aside criminal law and hard sovereignty, new types of relationships are developed to coordinate collaboration among sovereigns in general and anti-trafficking actions in particular. This strategy is specifically developed in Europe within the framework of the EU. From a top-down control mandated by state actors through criminal law, new legal frameworks aim to implement a bottom-up collaboration through rule-of-law principles, including human rights. As van Dijck asks and answers, "*Who is responsible for guarding public values in a digital society? The simple answer to this question is: all of us. But that answer is not very helpful*."[1] Collaboration to order this "all of us" answer, which includes sovereign actors and then connects them to the people, is to be found in various legal disciplines, deriving from a "soft" version of sovereignty. First, corporate social responsibility and compliance systems offer a new mindset to coordinate anti-trafficking actions among sovereigns. The birth of this legal discipline is grounded in the repression of human trafficking; its developments tend to disconnect from this specific aim while still being of use to enhance collaboration among states and digital actors to fight human trafficking (Chapter 1). However, this link between sovereigns is not enough to comprehensively repress the phenomenon; a direct relationship with the people and the enforcement of their human rights are needed to legitimize this coordination of coercion. The connection of digital actors to individuals and collectives through states is required to ensure the comprehensive protection of trafficked victims and the prevention of the phenomenon (Chapter 2).

[1] J. van Dijck, "Guarding Public Values in a Connective World: Challenges for Europe," *in* O. Boyd-Barrett, T. Mirrlees (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, p. 179

Chapter 1. Coordinating coercion through soft sovereignty

475. Private initiatives to repress human trafficking. As states sought to apply hard sovereignty to digital actors for facilitating cyber trafficking, they integrated its repression into their policies.[1] First, they rely on technological solutions to screen their services from being used for trafficking[2] or to monitor their value chains.[3] Second, they fund anti-trafficking initiatives and research to develop digital solutions.[4] Often, these actions are supported by the adoption of anti-trafficking statements,[5] "*shifting human*

[1] C. Fraser, "An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading," *International Journal of Development Issues*, July 4, 2016, vol. 15, no. 2, p. 111

[2] For instance, some hotels (a high-risk sector for trafficking) rely on mobile applications, T. Zhang et al., "A qualitative assessment of hotel employee engagement in anti-human-trafficking initiatives," *International Journal of Hospitality Management*, April 1, 2022, vol. 102, p. 6. In particular, the financial sector can screen transactions to prevent those linked to suspicious services or products linked to trafficking, Department of State, "Trafficking in persons report," US, June 2018, p. 28; Ministère de la Justice, Circulaire de lutte contre le proxénétisme, France, December 18, 2001. However, trafficking is still hardly considered in the forms to report suspicious transactions, G. Farms, *25 Keys to Unlock the Financial Chains of Human Trafficking & Modern Slavery*, UN University, Workshop Breaking the Financial Chains: Disrupting Financial Flows associated with Slavery, Human Trafficking, Forced Labour and Child Labour, March 31, 2017, pp. 15, 19; and transactions are usually of small amounts, leading to lack a of suspicions, OSCE, "Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings," 2014, p. 18

[3] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020, pp. 47, 43; M. Jiang et al., "Digital technology adoption for modern slavery risk mitigation in supply chains: An institutional perspective," *Technological Forecasting and Social Change*, July 1, 2023, vol. 192, p. 122595. These technologies can include block chain technology to protect work contract and monitor the manufacturing of a product to prevent exploitation. However, the efficiency of those tools has been questioned, L. Berg, B. Farbenblum, A. Kintominas, "Addressing Exploitation in Supply Chains: Is technology a game changer for worker voice?," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 49; L. Rende Taylor, E. Shih, "Worker feedback technologies and combatting modern slavery in global supply chains: examining the effectiveness of remediation-oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking," *Journal of the British Academy*, 2019, vol. 7, no. 1, pp. 158-161; D. Lloyd, "Human Trafficking in Supply Chains and the Way Forward," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 831

[4] S. Milivojević, "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* M. Segrave, L. Vitis (eds.), *Gender, Technology and Violence*, Routledge, 2017, p. 32. For instance, "*Google and Googlers (including corporate matching of employee donations, cash grants, and ad grants) contributed over US$5.5 million in 2021 to organizations fighting modern slavery*," Google, "2021 Statement Against Modern Slavery," June 2022. Facebook funds hackathons that led to the development of software meant to "*keep tabs on traffickers as they find new locations on the internet to conduct illegal activity*," M. Kennedy, *Counter-Trafficking Top 40 Tech Against Child Trafficking*, Center for Mind and Culture, May 2019, p. 27

[5] L. Belli, N. Zingales, "Online Platforms' Roles and Responsibilities: a Call for Action," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, pp. 27-30. See, for instance, the Standards of Business Conduct, the Global Human Rights Statement, the Supplier and Partner Codes of Conduct of Microsoft, Google's Policy Against Modern Slavery, and its Employee and Supplier Codes of Conduct.

rights responsibilities from states to private actors."[6] These private norms,[7], although their effectiveness is discussed,[8] reaffirm the independence of digital actors to exercise coercion. These initiatives are increasingly grouped under a collective, led by international organizations[9] or directly by private, including digital, actors.[10]

476. Risks of philanthrocapitalism. Philanthrocapitalism relies on three ideas. First, "*The wealthy […] should take greater responsibility for using their wealth for the common good. […* Second,*] market forces should sort effective social programs from ineffective social programs. […*Third,*] resources should be used in a targeted and*

[6] D. Kinley, J. Tadaki, "From Talk to Walk: The Emergence of Human Rights Responsibilities for Corporations at International Law," *Virginia Journal of International Law*, 2004, vol. 44, no. 4, p. 960

[7] Or "self-regulation" norms as leading to the "*disciplining of one's own conduct by oneself*," J. Black, "Constitutionalising Self-Regulation," *Modern Law Review*, 1996, vol. 59, no. 1, p. 27. Some authors see a parallel with constitutional texts, G. Teubner, "L'auto-constitutionnalisation des ETN ? Sur les rapports entre les codes de conduite « privés » et « publics » des entreprises," *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2015, vol. 75, no. 2015/2, p. 11. In particular, regarding digital actors, see the concept of "digital constitutionalism," N. Suzor, "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms," *Social Media + Society*, SAGE Publications Ltd, July 1, 2018, vol. 4, no. 3, pp. 1-11; G. De Gregorio, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge University Press, Cambridge studies in European law and policy, 2022

[8] In general, S.B. Banerjee, *Corporate social responsibility: the good, the bad and the ugly*, Edward Elgar, 2007, p. 123, and in particular regarding the repression of human trafficking, N. García Rivas, "Responsabilidad penal de las personas jurídicas en la trata sexual y protección de las víctimas," *in* P. Lloria García, J. Cruz Ángeles (eds.), *La violencia sobre la mujer en el S. XXI: género, derecho y TIC*, Aranzadi, Estudios, 2019, pp. 59-80. As such, these texts "*are designed not to protect labor rights or improve working conditions but rather to limit the legal liability*," R.M. Locke, *The Promise and limits of private power: promoting labor standards in a global economy*, Cambridge University Press, Cambridge studies in comparative politics, 2013, p. 51. On the contrary, other authors argue that they might be more effective since voluntarily adopted and more flexible, A. Clapham, *Human rights obligations of non-state actors*, Oxford University Press, The collected courses of the Academy of European Law no. v. 15/1, 2006, p. 233. See also E.B. Laidlaw, "Myth or Promise? The Corporate Social Responsibilities of Online Service Providers for Human Rights," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 140. The transnational aspect of corporate social responsibility is especially interesting, ILO, *Decent work in global supply chains*, IV, Geneva, International Labour Conference 105th Session, 2016, ¶ 121, ILC.105/IV

[9] For instance, the UN Global Compact program, created in 2000, offers a network of companies to coordinate initiatives towards the achievement of the Sustainable Development Goals, including Targets 5.2, 8.7 and 16.2, explicitly aim to repress trafficking, General Assembly, "Resolution 70/1 Transforming our world: the 2030 Agenda for Sustainable Development," UN, September 25, 2015, A/RES/70/1. The program supported the adoption by a community of businesses of the Athens Ethical Principles in 2006, dedicated to acknowledging their role in repressing trafficking. Moreover, the UN Global Initiative to Fight Human Trafficking is a network made up of all stakeholders, including private actors.

[10] For instance, the Global Business Coalition Against Trafficking, within which companies, including Google, are expected to improve the prevention of trafficking in their sphere of control. A network of financial actors exists for the same purpose, the Finance Against Slavery and Trafficking initiative. Particularly against cyber trafficking, the Tech Against Trafficking coalition was created in 2019. Similarly, the Global Emancipation Network, made up of businesses, including Microsoft, means to improve trafficking data worldwide. See T.E. DoCarmo, "Major International Counter-Trafficking Organizations: Addressing Human Trafficking from Multiple Directions," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1429-1444

rational way based on data in order to identify and scale successful social programs."[11] Against this approach, private actions face criticism. On the one hand, they have no means of enforcement,[12] they lack transparency,[13] and the elaboration and adoption of private norms do not conform to democratic values,[14] for which processes legitimize state law. Private actions dilute the applicable norms for the end user, and they standardize norms that should result from national political choices.[15] Thus, they hinder the independence of state sovereigns.[16] On the other hand, the effectiveness of private actions to repress trafficking is questioned.[17] They follow "*a top-down dynamic*," which does not fit with groundwork priorities.[18] Digital actors face price and speed pressures, leading to a necessary balance[19] but potentially overlooking human rights.[20] Monitoring

[11] J. Chuang, "Giving as Governance? Philanthrocapitalism and Modern-Day Slavery Abolitionism," *UCLA law review*, August 1, 2015, vol. 62, p. 1528. Differently, Bernstein develops the notions of redemptive capitalism or capitalist redemption to criticize the actual role of corporations in repressing human trafficking, E. Bernstein, "Redemptive Capitalism and Sexual Investability," *in* A.S. Orloff, R. Ray, E. Savcı (eds.), *Perverse Politics? Feminism, Anti-Imperialism, Multiplicity*, Emerald Group Publishing Limited, Political Power and Social Theory, 1st ed., January 1, 2016, vol. 30, pp. 45-80; E. Bernstein, "Brokered Subjects and Sexual Investability," *in* P. Kotiswaran (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, p. 338

[12] International Council on Human Rights Policy (ed.), *Beyond voluntarism: human rights and the developing international legal obligations of companies*, International Council on Human Rights Policy, 2002, pp. 7, 18. This lack of responsibility is particularly due to the inconsistency in auditing practices, L. Rende Taylor, E. Shih, "Worker feedback technologies," *op. cit.* note 3, p. 135; H.J. Van Buren, J. Schrempf-Stirling, M. Westermann-Behaylo, "Business and Human Trafficking: A Social Connection and Political Responsibility Model," *Business & Society*, February 2021, vol. 60, no. 2, p. 348

[13] International Council on Human Rights Policy (ed.), *Beyond voluntarism*, *op. cit.* note 12, p. 10; K.L. Christ, R.L. Burritt, "Current perceptions on the problem of modern slavery in business," *Business Strategy & Development*, June 2018, vol. 1, no. 2, p. 106

[14] M. Delmas-Marty, *Trois défis pour un droit mondial*, Seuil, Seuil essais, 1998, p. 73. However, sociologist Rosanvallon highlights the rise of a "*competition between democracies [since the] electoral-representative system is in fact confronted with the activity of various forms of counter-democracy*," P. Rosanvallon, *La contre-démocratie: la politique à l'âge de la défiance*, Seuil, Les livres du nouveau monde, 2006, p. 103

[15] H. Schepel, "Constituting Private Governance Regimes: Standards Bodies in American Law," *in* C. Joerges, I.-J. Sand, G. Teubner (eds.), *Transnational governance and constitutionalism*, Hart, International studies in the theory of private law, 2004, pp. 184, 187

[16] S. Eckert, "The Business Transparency on Trafficking and Slavery Act: Fighting Forced Labor in Complex Global Supply Chains," *Journal of International Business and Law*, 2013, vol. 12, no. 2, p. 406. See also J. Nolan, G. Bott, "Global supply chains and human rights: spotlight on forced labour and modern slavery practices," *Australian Journal of Human Rights*, January 2, 2018, vol. 24, no. 1, p. 50

[17] L. Shelley, C. Bain, "Human Trafficking: Fighting the Illicit Economy with the Legitimate Economy," *Social Inclusion*, February 23, 2015, vol. 3, no. 1, p. 141; G. LeBaron, "A Market in Deception? Ethically Certifying Exploitative Supply Chains," *in* D.W. Blight, G. LeBaron, J.R. Pliley (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, pp. 156-178

[18] J. Chuang, "Giving as Governance?," *op. cit.* note 11, p. 1553

[19] ILO et al., *Ending child labour, forced labour and human trafficking in global supply chains*, 8.7 Alliance, 2019, p. 26

[20] L.M. RendeTaylor, M. Latonero, *Updated Guide to Ethics and Human Rights in Anti-Trafficking: Ethical Standards for Working with Migrant Workers and Trafficked Persons in the Digital Age*, Issara

their actions might be inappropriate.[21] "*Multiple layers of contracting*" obstruct effective control over the bottom layers of value chains.[22] Thus, their narrative might be superficial and hamper the global repression against the phenomenon.[23] Then, "*Power needs to be constrained by law*."[24]

477. Corporate social responsibility and compliance. Although many definitions of corporate social responsibility exist,[25] this concept can be understood, from a private perspective, as "*the commitment of […] companies to contribute to increasing the welfare of local and global society, but without forgetting business efficiency or profitability […] to generate wealth*."[26] Thus, it is seen as a private voluntary commitments, going beyond the minimum mandatory legal requirements and lacking enforcement means.[27] From a public perspective, corporate social responsibility, deriving from a soft version of sovereignty, offers a legal tool to instill rule-of-law principles into private actions: compliance. It is a legal system designed to connect private actors to extra-market and economic issues.[28] While the fact that private actors "*can arbitrarily and independently decide the circumstances and the modes in which they need to respect [human] rights*,"[29] which questions states' sovereignty and has

Institute - Bangkok, 2018; L. Berg, B. Farbenblum, A. Kintominas, "Addressing Exploitation in Supply Chains," *op. cit.* note 3, p. 63

[21] D. Lloyd, "Human Trafficking in Supply Chains and the Way Forward," *op. cit.* note 3, pp. 822-823

[22] S. Eckert, "The Business Transparency on Trafficking and Slavery Act," *op. cit.* note 16, p. 404

[23] J. Chuang, "Giving as Governance?," *op. cit.* note 11, p. 1520

[24] International Council on Human Rights Policy (ed.), *Beyond voluntarism*, *op. cit.* note 12, p. 9. See also D. Broeders, L. Taylor, "Does Great Power Come with Great Responsibility? The Need to Talk About Corporate Political Responsibility," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 321

[25] For a list of various definitions, see S.B. Banerjee, *Corporate social responsibility*, *op. cit.* note 8, pp. 16-18. The concept initially meant the responsibility of business natural persons and their initiatives instead of a company liability, N. Seddiki, "Repenser la responsabilité en affaires dans un monde globalisé," *Paix et Securité Internationales*, 2020, no. 8, pp. 188-189. As a close concept, "*The social connection model of responsibility says that individuals bear responsibility for structural injustice because they contribute by their actions to the processes that produce unjust outcomes*," which could also be applied to corporations, I.M. Young, "Responsibility and Global Justice: A Social Connection Model," *Social Philosophy and Policy*, Cambridge University Press, January 2006, vol. 23, no. 1, p. 119

[26] R. Roso Cañadillas, "Prevención: responsabilidad social y penal de las personas jurídicas," *Revista General de Derecho Penal*, Iustel, 2020, no. 33, p. 3. This balance can rely on three kinds of initiatives: First, "*corporations should ensure that they do not contribute to human rights abuses committed by others*"; second, they should not benefit from such abuses; third, they should evaluate the impact of their activities, A. Clapham, *Human rights obligations of non-state actors*, *op. cit.* note 8, pp. 232-233

[27] S.B. Banerjee, *Corporate social responsibility*, *op. cit.* note 8, pp. 16-18

[28] J. Tricot, "L'hypothèse de la gouvernance pénale," *in* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 1025

[29] M. Taddeo, L. Floridi, "The Moral Responsibilities of Online Service Providers," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, p. 26

been criticized, the development of compliance systems to foster cooperation and rule-of-law standards enhances the independence and ordering of each sovereign's power of coercion.

478. Under the current theory of public international law, only states are sovereigns and bear international obligations, including the repression of human trafficking. However, the latter is currently integrated into the policies of digital actors. Private initiatives face criticism that hard sovereignty and criminal law cannot solve, despite fact that they are the foremost solution.[30] By acknowledging the role of private actors in social issues linked to globalization and digitalization, states aim, through soft sovereignty powers and corporate social responsibility, to enhance "*moral responsibilities of [intermediaries] in contemporary societies and aim at building ethical frameworks for [them]*"[31] (Section 1). However, due to traditional compliance limitations in supporting the global repression of cyber trafficking, a specific framework arises in the European Union that is dedicated to digital actors (Section 2).

Section 1. Corporate social responsibility: primary cooperation against human trafficking

479. Various compliance norms around the world are meant to integrate rule-of-law values into private actions. They are particularly applicable for a coordination of each sovereign's coercion to repress human trafficking. This study focuses on the following compliance norms. In 1976, the Organisation for Economic Co-operation and Development (OECD) adopted Guidelines for Multinational Enterprises (updated in 2011), and in 1977, the International Labour Organization (ILO) proclaimed the Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy (updated in 2017). The United Nations has struggled to adopt a text since the 2000s[32] and, in 2011, published the Guiding Principles on Business and Human Rights.[33] The current European Union framework rests on Directive 2013/34/EU

[30] J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation. Can obligatory reporting by corporations prevent trafficking?," *Netherlands Quarterly of Human Rights*, 2016, vol. 34, no. 4, p. 324

[31] G.F. Frosio, "Why keep a dog and bark yourself? From intermediary liability to responsibility," *International Journal of Law and Information Technology*, March 1, 2018, vol. 26, no. 1, p. 8

[32] See, for instance, E. Decaux, "La responsabilité des sociétés transnationales en matière de droits de l'homme," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2005, pp. 789-795; E.B. Laidlaw, "Myth or Promise?," *op. cit.* note 8, p. 139

[33] Annexed to the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, "Report - Guiding Principles on Business and

regarding annual financial statements, consolidated financial statements and related reports of certain types of undertakings, and the European Commission published in 2022 a proposal on corporate sustainability due diligence, which was amended by the European Parliament in June 2023.[34] At the national level, two texts are at the core of compliance systems to repress human trafficking: the California Transparency in Supply Chains Act of 2010[35] and the United Kingdom Modern Slavery Act of 2015. In the EU, Spain adopted compliance norms in its Penal Code in 2015,[36] and France adopted the law on the duty of vigilance of parent companies in 2017.[37] However, both their scope (§1) and content (§2) can be criticized when applied to trafficking prevention and repression.

§1. Corporate social responsibility's scope: adaptation to human trafficking

480. Corporate social responsibility norms can be applied to frame the repression of human trafficking by private actors. However, both the material (I) and subjective (II)

Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," Human Rights Council, UN, 2011, A/HRC/17/31. The Guidelines are based on a three-pillar structure: "*The state duty to protect against third-party human rights abuses, the corporate responsibility to respect human rights of those affected by their operations, and the right of victims to an effective remedy if human rights abuses do occur*," K. Yiannibas, L. Roorda, "Introduction," *in* J.J. Alvarez Rubio, K. Yiannibas (eds.), *Human rights in business: removal of barriers to access to justice in the European Union*, Routledge, 2017, p. 2. This text "*influenced leading and global instruments for transnational business governance*," K. Buhmann, "Neglecting the Proactive Aspect of Human Rights Due Diligence? A Critical Appraisal of the EU's Non-Financial Reporting Directive as a Pillar One Avenue for Promoting Pillar Two Action," *Business and Human Rights Journal*, January 2018, vol. 3, no. 1, p. 34. However, nowadays, "*The EU wants to become the global standard*," P.-H. Conac, "Sustainable Corporate Governance in the EU: Reasonable Global Ambitions?," *La Revue Européenne du Droit*, October 27, 2022, vol. 4, no. 1, p. 112

[34] European Commission, Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, 2022; European Parliament, Amendments on the proposal for a directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, June 1, 2023, P9_TA(2023)0209. The version of the text studied includes the amendments of the European Parliament.

[35] Various proposals were published for a federal application in the United States, but were not adopted: the Business Supply Chain Transparency on Trafficking and Slavery Act of 2015 and the Business Supply Chain Transparency on Trafficking and Slavery Act of 2020

[36] Article 31 bis of the Código penal, modified by the Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. This reform is copying a criticized Italian text, M. Abel Souto, "Blanqueo de dinero y responsabilidad penal de las personas jurídicas," *in* J. del Vicente Remesal, E. Bacigalupo Zapater, D.-M. Luzón Peña (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, pp. 1423-1424

[37] Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre. This mechanism was previously recognized by case law, S. Akorri, "La responsabilité pénale des entreprises transnationales : de l'influence du droit international sur le droit national," *Actualité juridique Pénal*, Dalloz, 2018, p. 556. The law derives from the scandal of the collapse of the Rana Plaza and the call of many NGOs for a new regulation, G. Delalieux, "La loi sur le devoir de vigilance des sociétés multinationales : parcours d'une loi improbable," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 648-665

scopes of the studied norms question their application to this goal.

I. Material scope: including human trafficking

481. Preventing human trafficking. Three types of corporate social responsibility norms can be differentiated: those applicable to specific topics (such as the repression of human trafficking), to general human rights standards, and to specific sectors.[38] Few texts on corporate social responsibility refer explicitly to human trafficking. The Directive 2013/34/EU requires disclosure information necessary to understand the undertaking's impacts on sustainability matters,[39] including human rights.[40]. The standards to be developed by the European Commission refer particularly to the Charter of Fundamental Rights,[41] which includes the prohibition of human trafficking.[42] Prior to the last version of this directive, the Commission already included "*processes and measures for preventing trafficking*"[43] as indicators of the protection of human rights. Although the prohibition of human trafficking is not mentioned directly, the last version of the directive details indicators to protect human rights that could be used to prevent human trafficking, such as ensuring "*equal treatment and opportunities for all*" and improving working conditions.[44] The 2022 proposal on corporate sustainability due diligence lists human rights in an annex,[45] including the prohibition of human trafficking.[46] By contrast, the main texts to explicitly mention human trafficking are the

[38] N. Phillips, G. LeBaron, S. Wallin, *Mapping and Measuring the Effectiveness of Labour-related Disclosure Requirements for Global Supply Chains*, Research Department Working Paper, no. 32, International Labour Office, June 2018, pp. 14-15
[39] Article 19a.1 of Directive 2013/34/EU
[40] Article 2.17 of Directive 2013/34/EU
[41] Article 29b.2.b.iii of Directive 2013/34/EU
[42] Article 5.3 of the Charter of Fundamental Rights of the EU
[43] European Commission, "Communication Guidelines on non-financial reporting (methodology for reporting non-financial information)," EU, July 5, 2017, p. 17, (2017/C 215/01). The lack of mention of human trafficking and forced labor in the text of the directive has been criticized, J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation," *op. cit.* note 30, p. 336
[44] Article 29b.2.b.i and ii of Directive 2013/34/EU
[45] Article 3.c of the 2022 proposal on corporate sustainability due diligence
[46] Part I, Section 1.14 of Annex I of the 2022 proposal on corporate sustainability due diligence. The proposal explicitly complements the anti-trafficking framework, European Commission, Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, *op. cit.* note 34, p. 6. It should also be analysed positively that the EU framework groups the mitigation of climate change with the protection of human rights, including trafficking. Indeed, some links start to be drawn between climate change and trafficking, Special Rapporteur on trafficking in persons, especially women and children, "Report - Addressing the gender dimensions of trafficking in persons in the context of climate change, displacement and disaster risk reduction," General Assembly, UN, July 15, 2022, ¶¶ 44-46, A/77/170; M.V. Smith, "Applying the United Nations Trafficking Protocol in the Context of Climate Change. Comments," *Chicago Journal of International Law*, 2021, vol. 22, no. 1, pp. 298-334

Section 1714.43 of the California Civil Code, introduced in 2010 by the Transparency in Supply Chains Act, and the United Kingdom Modern Slavery Act.[47] However, this approximation of slavery and human trafficking under the umbrella concept[48] of "modern slavery" suffers some criticism.

482. Trafficking as modern slavery: criticism. Human trafficking and slavery are different legal concepts,[49] although they might be linked in practice.[50] In particular, "*trafficking is best understood as a process and slavery, forced labor, [and] servitude, as possible outcomes*."[51] Nonetheless, the two concepts are combined under the undefined notion of modern slavery in the United Kingdom framework. The concept was born sociologically,[52] but it does not amount to a legal definition. Legal texts and their case law recognize that *de iure* and *de facto* slavery are two different

[47] Section 54.1 of the 2015 Modern Slavery Act. Definitions of the two offenses can be found in Sections 1 to 4 of the Act.

[48] Modern slavery can be defined as "*an umbrella term that emphasizes the commonalities between human trafficking, forced labor and slavery. Essentially, these are all situations of exploitation in which a person cannot refuse or leave an exploitative situation due to threats, violence, coercion, deception or abuse of power*," F. David, K. Bryant, J.J. Larsen, "Migrants and their vulnerability to human trafficking, modern slavery and forced labour," IOM, 2019, p. 8

[49] They also have roots in different historical perspectives, I. Chatzis, "Traite, esclavage et travail forcé au XXIe siècle : un état des lieux," *Diplomatie*, December 2020, no. 106, pp. 31-37; J. Allain, "Genealogies of human trafficking and slavery," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, pp. 9-10

[50] See, *supra* 68.

[51] E. Kenway, *The truth about modern slavery*, Pluto Press, 2021, p. 19

[52] Bales theorized the differences between old and modern slavery. The former assumed an asserted legal ownership, high purchase costs, low profits, a shortage of potential slaves, long-term relationships, the maintenance of slaves, and important ethnic differences. The latter supposes a lack of legal ownership, low purchase costs, high profits, a surplus of potential slaves, short-term relationships, the disposal of slaves, and non-important ethnic differences, K. Bales, *Disposable people new slavery in the global economy*, University of California Press, 2012, p. 15. See also C. Villacampa Estiarte, "La moderna esclavitud y su relevancia jurídico-penal," *Revista de Derecho Penal y Criminología*, Facultad de Derecho, 2013, no. 10, pp. 301-303. For a critic, see S. Scarpa, "The Nebulous Definition of Slavery: Legal Versus Sociological Definitions of Slavery," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 140. In particular, Kenway criticizes the differences between the two concepts and the use of the notion of modern slavery as "*There is nothing 'modern' about it per se: It is simply the continuation of exploitation by subtler means than legal ownership*," E. Kenway, *The truth about modern slavery*, *op. cit.* note 51, p. 7

phenomena,[53] but no legal text defines modern slavery.[54] While the notion encompasses slavery, servitude, forced and compulsory labor, and human trafficking, according to the United Kingdom text, scholars have found it to be "*a term in search of legal clarity*."[55] However, the concepts of slavery, trafficking, and modern slavery are often discussed indiscriminately by private actors, media, and even scholars.[56] This creates "*unhelpful caricatures of modern slavery, for example, as good/bad for business, as simply an economic externality, or by invoking modern slavery in a nebulous, superficial, or undefined way*."[57] The "*slavery and human trafficking statements*" required by the United Kingdom law became "*modern slavery statements*,"[58] that highlight "*actions performed by [the] companies upon [their] workers*" instead of initiatives to assist them, and the "*metaphor*" of modern slavery barely provides any substantial change.[59] The concept supports "*an emotive issue*"[60] and "*generates an illusion of political consensus*," while forms of exploitation and definitions of human trafficking still face differences under national laws, leading to "*a*

[53] E. Pérez Alonso, "Tratamiento jurídico-penal de las formas contemporáneas de esclavitud," *in* E. Pérez Alonso (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 334-336. In particular, Appels Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*, June 12, 2002, IT-96-23 & IT-96-23/1-A; Inter-American Court of Human Rights, *Hacienda Brasil Verde Workers v. the Federative Republic of Brazil*, October 20, 2016; ECHR, *Rantsev v. Cyprus and Russia*, January 7, 2010, no. 25965/04. Thus, "*Jurisprudence holds that the laws defining slavery and enslavement, designed to punish those who exploit in the most egregious manner, now overlap with laws defining trafficking short of exploitation*," N. Siller, "'Modern slavery': does international law distinguish between slavery, enslavement and trafficking?," *Journal of international criminal justice*, Oxford University Press, May 1, 2016, vol. 14, no. 2, p. 426

[54] N. Siller, "'Modern slavery'," *op. cit.* note 53, p. 406

[55] J. Nolan, G. Bott, "Global supply chains and human rights," *op. cit.* note 16, p. 47

[56] J. Winterdyk, B. Perrin, P.L. Reichel, "Introduction," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 7. See, for instance, L. Dryjanska, "Toward a Sustainable Theory of Human Trafficking and Contemporary Slavery," *in* L. Walker, G. Gaviria, K. Gopal (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, p. 23; J. Fernández Márquez, "Esclavitud, trata de personas y explotación: una perspectiva desde los derechos humanos," *El Cotidiano*, Universidad Autónoma Metropolitana, Unidad Azcapotzalco, 2018, vol. 34, no. 209, p. 48

[57] R. Caruana et al., "Modern Slavery in Business: The Sad and Sorry State of a Non-Field," *Business & Society*, SAGE Publications Inc, February 1, 2021, vol. 60, no. 2, p. 252. See also J. O'Connell Davidson, "Absolving the State: the Trafficking-Slavery Metaphor," *Global Dialogue*, Summer/Autumn 2012, vol. 12, no. 2, p. 39

[58] See, for instance, Google, *2021 Statement Against Modern Slavery*, *op. cit.* note 4; Mastercard, "Modern Day Slavery & Human Trafficking Statement," *Mastercard*, 2021, online https://www.mastercard.us/en-us/vision/who-we-are/careers/mastercard-modern-slavery-and-human-trafficking-statement.html (retrieved on July 8, 2022)

[59] I. Ras, C. Gregoriou, "The Quest to End Modern Slavery: Metaphors in corporate modern slavery statements," *Anti-Trafficking Review*, September 26, 2019, no. 13, p. 113

[60] S. Machura et al., "Recognizing Modern Slavery," *Journal of Human Trafficking*, Routledge, July 3, 2019, vol. 5, no. 3, p. 206

hugely contentious and highly political concept."[61] The notion of modern slavery lacks an emphasis of the role of private actors "*in creating and maintaining conditions that foster the coercive exploitation of workers*."[62] Thus, "*It is rather a term of advocacy encompassing each time different forms of severe exploitation*."[63] While some corporate social responsibility norms apply almost exclusively to the repression of human trafficking, their implementation by private actors continues to fluctuate due to the frequent relationship of trafficking with the legal concept of slavery and the non-legal notion of modern slavery.

483. Protecting human rights. On the contrary, most compliance frameworks rely only on a general reference to human rights as indicators to measure corporate social responsibility. In particular, international texts refer to the "*International Bill of Human Rights*,"[64] which makes no reference to the prohibition of human trafficking and refers only to the prohibition of some forms of exploitation.[65] Only the repression and prevention of forced and compulsory labor are explicitly introduced in some texts.[66] Similarly, the French law mentions only "*serious violations of human rights and fundamental freedoms*."[67] Despite the lack of allusion to human trafficking as a human rights violation and the criticism of the use of broad categories for the objective scope

---

[61] J. O'Connell Davidson, "New slavery, old binaries: human trafficking and the borders of 'freedom'," *Global Networks*, 2010, vol. 10, no. 2, pp. 257-258

[62] J. Chuang, "Giving as Governance?," *op. cit.* note 11, p. 1525. It also hides "*the state's role in constructing the conditions under which some groups become vulnerable to various forms of abuse and exploitation*," J. O'Connell Davidson, "Absolving the State," *op. cit.* note 57, p. 31

[63] I. Chatzis, "Traite, esclavage et travail forcé au XXIe siècle," *op. cit.* note 49, p. 43

[64] Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, *Guiding Principles on Business and Human Rights*, *op. cit.* note 33, ¶ 12; OECD, *Guidelines for multinational enterprises*, 2011, p. 32. The OECD framework is more extended than the UN one as it mentions other issues such as the protection of the environment, employment, and industrial relations, the repression of corruption, and the protection of consumers' interests, B. Lecourt, "Vers une directive sur le devoir de vigilance des sociétés - Résolution du Parlement européen du 10 mars 2021 contenant des recommandations à la Commission sur le devoir de vigilance et la responsabilité des entreprises, P9_TA-PROV(2021)0073, (2020/2129(INL)," *Revue des sociétés*, Dalloz, 2021, p. 2. On the contrary, the ILO tripartite declaration only refers to the ILO's Declaration on Fundamental Principles and Rights at Work, based on the principles at the basis of the organization's work, set in the Declaration of Philadelphia in 1944, S. Olarte Encabo, "El desafío del trabajo decente en las cadenas mundiales de suministros. Respuesta internacional, estatal, sindical y social," *in* M.I. Ramos Tapia et al. (eds.), *Formas contemporáneas de esclavitud y derechos humanos en clave de globalización, género y trata de personas*, Tirant lo Blanch, Homenajes & congresos, 2020, p. 100. For a critic of this text, see A. Supiot, *L'esprit de Philadelphie la justice sociale face au marché total*, Seuil, 2010

[65] Slavery and servitude from Article 4 of the Universal Declaration of Human Rights and Article 8 of the ICCPR; forced or compulsory labor from Article 2.b of the ILO's Declaration on Fundamental Principles and Rights at Work

[66] OECD, *OECD Guidelines*, *op. cit.* note 64, p. 35; ILO, "Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy," UN, March 2017, ¶¶ 23-24

[67] Article L225-102-4.I¶3 of the Code de commerce

of compliance systems, the general mention of human rights is more comprehensive than the reduction of corporate social responsibility to the repression of slavery and human trafficking. The improvement in human rights would lead to limiting vulnerabilities, which are partly at the origin of trafficking. Generally, trafficking, as a human rights violation, would be included in these frameworks.[68]

484. Preventing offenses. Differently, the Spanish framework targets only the prevention of offenses for which legal persons can be liable.[69] Therefore, private actors are not required to study their global impact on human rights or their impact on or links to human trafficking processes. They merely must seek to prevent the commission within the company of an offense of human trafficking. However, every offense is linked to a protected "legal value" (*bien jurídico*). Criminal sanctions are subsidiary; only violations of main values are to be accepted.[70] Thus, all offenses are supposed to be linked to fundamental rights or core values protected by the Spanish legal framework.[71] Indirectly, the criminal framework, including the requirement of compliance to avoid corporate liability, is meant to protect fundamental rights. However, this approach is limited by the narrow list of offenses for which corporations can be criminally liable, and these offenses do not include those against workers' rights. Since corporations cannot be held liable for these potential violations, they are not incentivized to monitor them.[72] Furthermore, it has been argued that control obligations should be limited to legal ones to ensure that criminal liability can be triggered. While respectful of the principle of strict interpretation of criminal law, this tactic leads to a lack of consideration of contractual obligations, such as a violation of a prevention program.[73] Finally, the

[68] For instance, the French law on the duty of vigilance is mentioned as a tool to encourage private actors to order their actions with State's priorities, including on the repression of human trafficking, CNCDH, "Avis sur la traite des êtres humains à des fins d'exploitation économique," October 15, 2020, p. 16

[69] Article 31 bis.5.1° of the Código penal

[70] M. Cabanes Ferrando, *La trata de seres humanos: concepto desde el marco normativo: una aproximación al delito*, J.M. Bosch Editor, 2022, pp. 170-172

[71] However, scholars are far from agreeing on the legal value protected by the offense of human trafficking. The three main positions frame the offense as a protection to moral integrity, liberty, or dignity. For a summary, see *Ibid.* pp. 175-219

[72] M. Gómez Tomillo, "Algunos déficits en la regulación de la responsabilidad penal de las personas jurídicas: en particular los delitos contra la seguridad e higiene en el trabajo," *in* J. del Vicente Remesal, E. Bacigalupo Zapater, D.-M. Luzón Peña (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, pp. 1636-1637; M.J. Dolz Lago, "Apuntes sobre las penas con dimensión laboral en el régimen español de responsabilidad penal de las personas jurídicas," *in* Fiscalía General del Estado (ed.), *La responsabilidad penal de las personas jurídicas: homenaje al Excmo. Sr. D. José Manuel Maza Martín*, Ministerio de Justicia, 2018, p. 108

[73] J.G. Fernández Teruelo, "Responsabilidad penal de las personas jurídicas: el contenido de las obligaciones de supervisión, organización, vigilancia y control referidas en el art. 31 bis 1. b) del Código

violation of the compliance system should prove a type of fault: "*a) organizational faults (faults due to the absence or insufficiency in the legal entity of bodies for the selection, training, and monitoring of the activity carried out by the directors or legal representatives (*culpa in constituiendo*); b) faults in the selection of managers or employees or in their continuous training subsequent thereto (*culpa in eligendo vel in instruiendo*); c) control faults (fault due to the absence of supervision or monitoring, by the body in charge thereof, of the actions of the directors or legal representatives (*culpa in vigilando*)*."[74] As this compliance system is integrated with criminal liability, it is limited by design.[75]

485. Human trafficking, whether mentioned explicitly or considered to be a human rights violation, is included in major compliance systems. However, these hardly consider the impact of digitalization on human rights[76] or the role of private digital actors. Consequently, the subjective scope of these compliance systems should be studied.

II. Subjective scope: limiting human trafficking

486. Recipients of supranational norms. Corporate social responsibility frameworks should pay attention to their subjective scope. States remain the primary recipients of international public law, but international organizations increasingly recognize the role of private actors. As such, although the ILO tripartite declaration and the OECD guidelines first name governments as recipients, many recommendations are directed to multinational enterprises,[77] but the concept is not defined.[78] On the contrary, the United Nations principles mention that they "*apply to all states and to all*

Penal español," *Revista electrónica de ciencia penal y criminología*, Universidad de Granada, 2019, no. 21, p. 5

[74] J.M. Zugaldía Espinar, M.R. Moreno-Torres Herrera, *Lecciones de derecho penal: parte general*, 2021, p. 391

[75] Also named a criminal compliance system, J.L. Alapont, "Criminal Compliance: análisis de los arts. 31 bis 2 a 5 CP y 31 quater CP," *Revista General de Derecho Penal*, Iustel, 2019, no. 31, p. 1

[76] The OECD framework only considers the transfer of technology to share the benefits of private actors with the local population, their use to share information, to protect the environment, consumers' privacy, or intellectual property rights, OECD, *OECD Guidelines*, *op. cit.* note 64, pp. 14, 30, 43-46, 54-56. The ILO tripartite declaration only considers that technology can contribute to sharing private actors' benefits, in particular to generate employment, ILO, *Tripartite Declaration*, *op. cit.* note 66, ¶¶ 1, 19

[77] ILO, *Tripartite Declaration*, *op. cit.* note 66, ¶ 10; OECD, *OECD Guidelines*, *op. cit.* note 64, pp. 17-18

[78] It includes a wide variety of corporations, ILO, *Tripartite Declaration*, *op. cit.* note 66, ¶ 6; OECD, *OECD Guidelines*, *op. cit.* note 64, p. 17

business enterprises," not only multinational ones.[79] However, the foundational and operational principles of the norms still rest primarily on the duty of states to protect human rights.[80] Similarly, the EU framework is based on directives to be transposed, and the recipients are the member states. Nevertheless, the dispositions on sustainability reporting [81] that specify the recipients of the norm could have a direct effect, as they can be deemed precise, clear, and unconditional.[82] However, their definition questions the usefulness of the framework to develop the transparency of anti-trafficking private actions, since recipients should be "*governed by the law of a Member State and whose transferable securities are admitted to trading on a regulated market of any Member State*," or be credit or insurance entities.[83] Digital actors may not be listed on a European regulated market. Therefore, the 2022 proposal on corporate sustainability due diligence offers a wider definition of recipients,[84] depending on the state law in which they were constituted, their number of employees, and their net worldwide or European turnover.[85] However, the proposal is still limited mainly to large actors, despite the reduction of the thresholds by the European Parliament,[86] with no compliance obligations for small companies.[87] The recipients of

[79] Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, *Guiding Principles on Business and Human Rights*, *op. cit.* note 33, p. 6

[80] *Ibid.* pp. 6-13

[81] Articles 19a and 29a of Directive 2013/34/EU

[82] ECJ, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, February 5, 1963, no. 26-62; ECJ, *Yvonne van Duyn v Home Office*, December 4, 1974, no. 41-74. States can only allow certain specific information to be omitted in exceptional cases, Articles 19a.3 and 29a.3 of Directive 2013/34/EU. However, in the absence of transposition, the states would not be able to oppose the directive against the company, ECJ, *Criminal proceedings against Tullio Ratti*, April 5, 1979, no. 148/78.

[83] Articles 19a.1 and 2.1 of Directive 2013/34/EU. It excludes micro-undertakings, meaning obligated undertakings should at least "*exceed the limits of at least two of the three following criteria: (a) balance sheet total: EUR 350,000; (b) net turnover: EUR 700,000; (c) average number of employees during the financial year: 10*," Article 3.1. It should be assessed positively that not only large undertakings are obligated to report on sustainability matters, since human trafficking can benefit or be facilitated by corporations of any size.

[84] Article 2 of the 2022 proposal on corporate sustainability due diligence

[85] The European Parliament deleted the references to sectors of activities. The original version of the Commission listed sectors of activities that are of particular risk regarding exploitation and exploitative working conditions: the manufacture of textiles, agriculture, and the extraction of mineral resources. However, regarding human trafficking, this did not consider sectors of activities that might be used by traffickers to support the criminal process (such as accommodation and transportation services).

[86] For instance, the original text of the Commission required "*more than 500 employees on average and had a net worldwide turnover of more than EUR 150 million in the last financial year for which annual financial statements have been prepared*." The European Parliament reduces these thresholds to 250 employees and 40 million of net worldwide turnover.

[87] This has been particularly criticized to prevent adequately trafficking for forced labor in the agriculture sector, Special Rapporteur on trafficking in persons, especially women and children, "Report - Trafficking

national norms also tend to be limited. The California law is restricted to manufacturers and retail sellers,[88] which leaves most digital actors outside of its scope, despite most of them being headquartered in California. The United Kingdom Act applies to private actors[89] with "*a global annual turnover of at least £36 million*."[90] In France, the compliance system is applicable to large corporations depending on the number of employees.[91,92]

487. Application to transnational actors. Furthermore, the application of corporate social responsibility frameworks to transnational actors is highly relevant to improving coordination in repressing trafficking.[93] However, international frameworks do not establish territorial limitations,[94] and national frameworks barely define a territorial scope. The California[95] and United Kingdom laws apply as soon as a private

in persons in the agriculture sector: human rights due diligence and sustainable development," General Assembly, UN, April 25, 2022, ¶ 38, A/HRC/50/33

[88] Section 1714.43.a of the California Civil Code, meaning private actors whose main activity is the production of products or the selling of goods, understood as tangible property, Section 6007.a.1 of the California Revenue and Taxation Code. Furthermore, recipients must do business in this US state, and their annual worldwide gross receipts must exceed one hundred million dollars.

[89] A company, group or partnership that supplies goods and services, entirely or partly in the United Kingdom, Section 54.1 and 12 of the United Kingdom Modern Slavery Act

[90] Institute for Human Rights and Business, "Corporate Liability for Forced Labour and Human Trafficking," October 2016, pp. 12-13, https://www.ihrb.org/focus-areas/migrantworkers/ corporate-liability-for-forced-labour-and-human-trafficking. While it is estimated "*around 12 000 companies*," ILO et al., *Ending child labour, forced labour and human trafficking*, *op. cit.* note 19, p. 46

[91] Corporations that, at the end of two financial years, have at least 5 000 employees within the parent company, and direct and indirect subsidiary companies headquartered in France or 10 000 within the parent company and direct and indirect subsidiary companies headquartered in France or abroad, Article L225-102-4.I of the Code de commerce. No official data exists on the number of companies affected. Furthermore, numerous critics have raised concerns about this subjective scope, regarding the definition of the forms of private actors, the counting of employees, etc., P.B. de Lagerie et al., "La mise en œuvre du devoir de vigilance : une managérialisation de la loi ?," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, p. 702; A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, 2019/12/CGE/SG, Conseil Général de l'économie, de l'industrie, de l'énergie et des technologies, January 2020, pp. 17-18

[92] The Spanish Código penal does not set a subjective scope specific to its compliance system. For a comment on the legal persons that can be criminally liable, see *supra* 354 and 355.

[93] As human trafficking is partly linked to globalization and may be transnational, compliance must consider the global network in which a private actor develops its activities. See *supra* 23 to 25 and 80 to 82.

[94] The OECD and ILO frameworks consider multinational enterprises that "*often operate through relationships with other enterprises*," ILO, *Tripartite Declaration*, *op. cit.* note 66, ¶ 6, and which particularly must "*encourage, where practicable, business partners, including suppliers and sub-contractors, to apply principles of responsible business conduct*," OECD, *OECD Guidelines*, *op. cit.* note 64, p. 20. Moreover, the United Nations principles cover "*adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships*," Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, *Guiding Principles on Business and Human Rights*, *op. cit.* note 33, p. 16

[95] It can include a foreign private actor as long as they are engaged in a transaction for profit in California, Section 23101 of the California Revenue and Taxation Code

actor conducts business at least partly in this territory, which can then extend to foreign private actors. On the contrary, the EU Directive creates a tighter territorial link, by being applicable to private actors listed on a member state market[96] or to companies regulated under EU law, such as credit institutions.[97] Nonetheless, parent undertakings of large groups in the scope of the text must publish a consolidated sustainability reporting to assess their impact at the group level, which could include their impact outside the EU.[98] The territorial link is reduced in the 2022 proposal on corporate sustainability due diligence, as it applies to private actors constituted under a member state or third-party law, as long as the other criteria are verified.[99] On the contrary, in France, it applies only to corporations constituted under French law.[100] In Spain, the compliance system for the criminal code depends on the Spanish jurisdiction, underscoring the difficulties of prosecuting foreign legal persons, as already developed.[101]

488. Extraterritoriality of national frameworks. Despite limited subjective scopes, national texts might have an extraterritorial effect that could be positive for coordination in repressing human trafficking. In particular, various norms[102] consider

---

[96] In particular, "*many foreign companies, including banks, have debt listed on EU stock exchanges […] The Commission assumes that such third country companies will prefer to subject themselves to [its norm] rather than lose access to the EU financial markets*," P.-H. Conac, "Sustainable Corporate Governance in the EU," *op. cit.* note 33, p. 115

[97] Article 2.1 of Directive 2013/34/EU

[98] Article 29a of Directive 2013/34/EU

[99] Article 2 of the 2022 proposal on corporate sustainability due diligence. Consequently, "*The threshold proposed is very low and will cover a significant number of foreign companies*," P.-H. Conac, "Sustainable Corporate Governance in the EU," *op. cit.* note 33, p. 116. Thus, the EU means "*to adopt legal instruments that demonstrate that it is possible to promote international trade and the protection of human rights both within and outside the EU*," J.J. Alvarez Rubio, K. Yiannibas, "Conclusion," *in* J.J. Alvarez Rubio, K. Yiannibas (eds.), *Human rights in business: removal of barriers to access to justice in the European Union*, Routledge, 2017, p. 143. Moreover, the 2022 proposal on corporate sustainability due diligence, as amended by the European Parliament, mandates states to oblige parent companies to take actions at the group level, Article 4a, supporting an extraterritorial effect of the text and a comprehensive application to transnational corporations.

[100] Since the regime is to be found in the commerce code and in particular in the chapter on public limited-liability companies. See, in particular, Article L210-3 of the Code de commerce and A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399*, *op. cit.* note 91, pp. 17-18

[101] See *supra* 354.

[102] The verification of supply chains is the main focus of the Californian law, Section 1714.43.c of the Civil Code, and of the United Kingdom Modern Slavery Act, Section 54. Similarly, the main aim of the French duty of vigilance is the control of value chains, through the creation of vigilance measures applicable to the private actor, "*the companies it controls […] directly and indirectly, as well as the activities of subcontractors or suppliers with whom there is an established commercial relationship*," Article L225-102-4 of the Code de commerce. See also L. Moua, "La lutte contre la traite dans les entreprises," *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, p. 251. However, the delimitation of these relations and the possibilities to verify them are still vague and create difficulties in the implementation of the framework, A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399*, *op. cit.* note 91, pp. 17-18. By contrast, the Directive 2013/34/EU only

global supply or value chains.[103] Indeed, "*human trafficking [is] a whole-of-supply-chain problem*"[104] as "*subcontracting and recruitment agencies, in particular, are major risk factors*."[105] Generally, this refers to the phases in which different business contractual relationships arise, from the creation to the selling and functioning of goods and services,[106] including foreign contractual relationships with national private actors. However, due to the absence of any common definition or any definition at all,[107] "*to an important extent, it is left to companies to determine which portions of their global operations*" must comply with corporate social responsibility frameworks.[108] Nevertheless, extraterritorial effects lead to overlapping obligations through the application of various national norms, creating legal insecurities for private actors. Despite criticism, the concept of value chains is of particular importance to target trafficking linked to the different stages before the sale of goods and services, especially as the process leads to forced labor.[109] However, this concept hardly considers the use of services to facilitate a trafficking process, which is at the core of

complementarily considers business relationships and supply chains, in the mapping of risks, Articles 19a.2.f.ii and 29a.2.f.ii. The report should broadly assess the impact of corporations on sustainability matters, not limited to those directly linked to their supply chains. Similarly, the extends due diligence actions to "*broadly scope the impacts of their operations, subsidiaries and business relationships*," thus not limited to an assessment of their value chain, Article 6.1. The Spanish compliance system does not mention value chains and only underlines the need for efficient internal controls within the legal person, Article 31bis.2.2° of the Código penal.

[103] The former is limited to the creation of goods, while the latter is broader to include any creation of value.

[104] ILO et al., *Ending child labour, forced labour and human trafficking*, *op. cit.* note 19, p. 16. See also Committee of Ministers, "Recommendation CM/Rec(2022)21 to member States on preventing and combating trafficking in human beings for the purpose of labour exploitation," Council of Europe, September 27, 2022, p. 30

[105] UNODC, *Compendium on promising practices on Public-Private Partnerships to prevent and counter trafficking in persons*, UN, 2021, p. 60

[106] ILO, *Decent work in global supply chains*, *op. cit.* note 8, ¶ 5

[107] It also depends on the legal discipline in which it is framed, A. Beckers, "L'image juridique évolutive des chaînes de valeur mondiales Introduction au numéro spécial," *Revue internationale de droit économique*, Association internationale de droit économique, 2021, vol. t. XXXV, no. 4, p. 14. The concept seems to be a "*form of economic organization*" that hardly fits with the existing legal categories and liability frameworks, A. Beckers, "Chaînes de valeur mondiales : théorie et dogme des obligations de l'entreprise," *Revue internationale de droit économique*, Association internationale de droit économique, 2021, vol. t. XXXV, no. 4, pp. 126, 130-131. Even an organization such as the ILO managed to obtain a single definition for it, Governance and Tripartism Department, *Achieving decent work in global supply chains*, Report for discussion at the technical meeting on achieving decent work in global supply chains (Geneva, 25–28 February 2020), Geneva, ILO, 2020, p. 7. Its definition is challenged by the multiple structures of value chains, G. LeBaron, A. Rühmkorf, "Steering CSR Through Home State Regulation: A Comparison of the Impact of the UK Bribery Act and Modern Slavery Act on Global Supply Chain Governance," *Global Policy*, 2017, vol. 8, no. S3, pp. 24-25

[108] N. Phillips, G. LeBaron, S. Wallin, *Mapping and Measuring*, *op. cit.* note 38, p. 16

[109] On the contrary, the improvement of working conditions in global value chains reduces the risks of exploitation. In particular, "*'Upgrading' is a term applied to the process through which actors in global supply chains can reap the benefits of their participation in global markets and attain decent work*," ILO, *Decent work in global supply chains*, *op. cit.* note 8, ¶¶ 75-78

the coordination between digital actors and states.

489. Corporate social responsibility frameworks can be used to coordinate anti-trafficking actions by enhancing their transparency. However, their digital evolutions are hardly taken into consideration. Compliance systems throughout Europe and in individual nations are limited mainly to large private actors and face difficulties in being extended to foreign actors and transnational value chains. As is the case for corporate criminal liability, the economic realities of private actors hardly fit into legal categories.[110] Therefore, further limitations are to be highlighted regarding the content of obligations and their enforcement.

§2. Corporate social responsibility: content and control

490. The concept of due diligence. Corporate social responsibility frameworks are based on due diligence.[111] Originally, "*Under Roman law, a person was liable for accidental harm caused to others if the harm resulted from the person's failure to meet the standard of conduct expected of a* diligens *(or* bonus*)* paterfamilias."[112] While the notion has been known since the end of the 19th century in international public law,[113]

[110] K. Amaeshi, O. Osuji, P. Nnodim, "Corporate Social Responsibility in Supply Chains of Global Brands: A Boundaryless Responsibility? Clarifications, Exceptions and Implications," *Journal of Business Ethics*, 2008, vol. 81, no. 1, p. 238

[111] Particularly developed by the UN, Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, *Guiding Principles on Business and Human Rights*, *op. cit.* note 33, pp. 17-20. According to the principles, human rights due diligence is made up of four core elements: "*having a human rights policy, assessing human rights impacts of companies' activities, integrating those values and findings into corporate cultures and management system, and tracking as well as reporting performance*," N. Jägers, C. Rijken, "Prevention of Human Trafficking for Labor Exploitation: The Role of Corporations," *Northwestern Journal of International Human Rights*, 2014, vol. 12, no. 1, p. 54. See also OECD, *OECD Guidelines*, *op. cit.* note 64, p. 20; ILO, *Tripartite Declaration*, *op. cit.* note 66, ¶ 10; Articles 19a.2.f and 29a.2.f of Directive 2013/34/EU, title of the 2022 proposal on corporate sustainability due diligence; Section 54.5.c of the United Kingdom law. The French law mentions "*due vigilance*" (*vigilance raisonnable*) as a similar concept, Article L225-102-4.I¶3 of the Code de commerce. However, Sachs argues that "*The duty of vigilance carries a stronger requirement: In the medium and long term, companies must align their value chains with their capacity to deploy the vigilance they owe*." Indeed, "*While due diligence is a mechanism for minimizing externalities and managing risks within the value chain, the duty of vigilance aims to bring about changes in corporate governance*," T. Sachs, C. Clerc, "Controverse : le devoir de vigilance à la croisée des chemins ?," *Revue de droit du travail*, Dalloz, 2022, p. 357. The Spanish law sets the notion of "*appropriate monitoring and control measures*" (*medidas de vigilancia y control idóneas*), Article 31bis.2.1 of the Código penal. However, the concept is not explicitly mentioned in Californian law.

[112] J. Bonnitcha, R. McCorquodale, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights," *European Journal of International Law*, November 13, 2017, vol. 28, no. 3, pp. 902-903

[113] See, for instance, its mention in Permanent Court of International Justice, *Lotus*, September 7, 1927, no. 9

its use increased in the 1990s as it was adapted to contemporary risks and actors.[114] Although the understandings of this notion is not fully harmonized,[115] due diligence is the positive counterpart of the negative obligations of private actors to refrain from violating human rights. Due diligence requires them to "*prevent and avoid negative impacts of their activities that may constitute human rights violations*."[116] Indeed, the extent of due diligence under international frameworks is limited to an organization standard and not a liability norm.[117] This is logical, as they are only soft norms,[118] with no mandatory authority or monitoring system.[119]

491. Thus, the following study is limited to mandatory compliance systems, which are directed are primarily directed at increasing transparency in private actors' actions. These obligations indeed would "*address the risks of modern slavery [and human trafficking, if they would]: (1) incorporate clear and detailed guidance on disclosure and due diligence requirements; (2) require collaboration with external stakeholders; and (3) provide for compliance mechanisms to couple transparency and due diligence with*

[114] L. d'Ambrosio, "Le devoir de vigilance : une innovation juridique entre continuités et ruptures," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 639-640

[115] For instance, "*Human rights lawyers understand 'due diligence' as a standard of conduct required to discharge an obligation, whereas business people normally understand 'due diligence' as a process to manage business risks*," J. Bonnitcha, R. McCorquodale, "The Concept of 'Due Diligence'," *op. cit.* note 112, p. 900. "*On the one hand, 'due diligence' describes the 'international human rights legal obligation of due diligence in relation to the actions of non-state actors'; on the other hand, it describes the voluntary business practice corporations undertake to assess risks, particularly prior to or during processes such as mergers*," J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation," *op. cit.* note 30, p. 322

[116] K. Martin-Chenut, "Droits de l'homme et RSE : vers un humanisme responsable ?," *in* J. Alix et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, p. 131

[117] L. d'Ambrosio, "Le devoir de vigilance," *op. cit.* note 114, p. 639. It is linked to two understandings of the concept of due diligence in relation to responsibility: "*If due diligence, understood as a standard of conduct, applies, then a business is only responsible for adverse human rights impacts that result from its failure to act with reasonable diligence […] In contrast, if businesses breach their responsibility to respect human rights whenever they infringe human rights - that is, if the responsibility to respect human rights is akin to a strict liability standard and does not entail a fault element - then a business's responsibility to redress situations in which it has infringed human rights is independent of any debate about whether the business has acted with sufficient diligence or care*," J. Bonnitcha, R. McCorquodale, "The Concept of 'Due Diligence'," *op. cit.* note 112, pp. 910-911

[118] The complexity of adopting hard international norms on this topic is due to two reasons: "*International human rights law has developed as a tool to protect individuals from the arbitrary use of power by states, not corporations or other private entities [… And] corporations law traditionally has been almost exclusively a domestic matter*," D. Kinley, J. Tadaki, "From Talk to Walk," *op. cit.* note 6, p. 937

[119] However, the OECD Guidelines include the designation of national contact points that are entitled to resolve issues related to the topics of the text, OECD, *OECD Guidelines*, *op. cit.* note 64, pp. 72-74. Nevertheless, their impact will depend "*on the use that is made of them by the recognized employer and union organizations, as well as by NGOs, governments, and other intergovernmental organizations*," A. Clapham, *Human rights obligations of non-state actors*, *op. cit.* note 8, p. 210

accountability."[120] However, they draft limited obligations (I) and means of enforcement (II).

I. Private sovereigns: transparency as a limited obligation

492. Transparency obligations. First, as the title of the Transparency in Supply Chains Act of California summarizes, this law aims to ensure that the recipients "*provide consumers with information on the efforts undertaken, if any, to eradicate slavery and human trafficking from their supply chains*."[121] Nevertheless, this act "*does not require corporations to adopt such a policy*" but only to disclose their voluntary efforts.[122] Similarly, the EU sees transparency as "*a crucial element of legislation on mandatory due diligence*."[123] The Directive 2013/34/EU, after being first amended by Directive 2014/95/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups, "*stands out by introducing an explicit requirement of [due diligence] disclosure*,"[124] yet standards from the Commission to define its components remain to be published.[125] Again, no positive actions are expected, and "*little attention is paid to the reporting process as a modality to induce organizational change or self-regulation*."[126] Moreover, the United Kingdom law mainly

[120] J. Nolan, "Hardening Soft Law: Are the emerging corporate social disclosure and due diligence laws capable of generating substantive compliance with human rights norms?," *Revista de Direito Internacional*, October 26, 2018, vol. 15, no. 2, p. 74

[121] ILO et al., *Ending child labour, forced labour and human trafficking*, *op. cit.* note 19, p. 46. They must publicly, by posting on their website, disclose: 1) their actions to verify "*product supply chains to evaluate and address risks of human trafficking*," 2) if they audit suppliers, 3) their requirements for materials certification, 4) internal accountability standards and procedures for non-compliant employees or contractors, and 5) their trainings, Section 1714.43.c of California Civil Code

[122] N. Jägers, C. Rijken, "Prevention of Human Trafficking for Labor Exploitation: The Role of Corporations," *op. cit.* note 111, p. 64. There are no positive obligations to prevent human trafficking. For instance, private actors can only be required "*to disclose that they are not implementing*" any action, J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation," *op. cit.* note 30, p. 328

[123] European Parliament, "Resolution with recommendations to the Commission on corporate due diligence and corporate accountability," EU, March 10, 2021, ¶ 24, P9_TA(2021)0073

[124] K. Buhmann, "Neglecting the Proactive Aspect of Human Rights Due Diligence?," *op. cit.* note 33, p. 26

[125] Article 29b of Directive 2013/34/EU. The content mandated for disclosure is quite broad in the main text. It includes a description of "*the due diligence process implemented by the undertaking with regard to sustainability matters, […] the principal actual or potential adverse impacts connected with the undertaking's own operations and with its value chain*," and "*any actions taken by the undertaking to prevent, mitigate, remediate or bring an end to actual or potential adverse impacts, and the result of such actions*," Articles 19a.2.f and 29a.2.f. Before the 2022 amendments of the Directive, "*There [was] little evidence that the non-binding guidelines [… that develop the indicators] have had a significant impact*," European Commission, "Report on the review clauses in Directives 2013/34/EU, 2014/95/EU, and 2013/50/EU," EU, April 21, 2021, p. 20, COM(2021) 199 final

[126] K. Buhmann, "Neglecting the Proactive Aspect of Human Rights Due Diligence?," *op. cit.* note 33, p. 29

mandates private actors to approve and publish a statement on some optionally listed elements,[127] with no provision for mandatory positive actions.[128] Nonetheless, the act has led some corporations to disclose a factory list that could allow civil society and the government to investigate working conditions.[129] Corporations have developed listed activities, such as risk assessments and training for board members and senior executives, and they have increased their collaborations with peers and NGOs.[130] Thus, these texts establish a bare minimum of legal compliance through the mandatory disclosure of a broad list of elements. In particular, these transparency reports are usually made to disclose potential violations within a company's employment structure through value chains and, specifically, to verify working conditions. However, the original meaning of these texts has been broadened, especially by digital actors, who have expanded it to the control of their services to limit their use by perpetrators of offenses, such as traffickers. Thus, these texts can incentivize private actors "*to at least consider the question of whether their company is linked to the issue of*" human trafficking and human rights violations,[131] through the conduct of their activities and in their relationships with the end user or consumer. While the vagueness around transparency has been criticized, it is an example of co-regulation, since "*the state does not disappear […]: Self-regulation is […] ordered [as] heteronomous rules set guidelines for the actors of the corporation*."[132] Going further, it has been argued that self-regulation provides an example of how states transfer to corporations "*the determination of a policy and obligations that they themselves find difficult to express in the form of positive prescriptions, or in any case to impose, even though they are*

[127] The statement may include, similarly to the California text, "*information about (a) the organisation's structure, its business and its supply chains; (b) its policies in relation to slavery and human trafficking; (c) its due diligence processes in relation to slavery and human trafficking in its business and supply chains; (d) the parts of its business and supply chains where there is a risk of slavery and human trafficking taking place, and the steps it has taken to assess and manage that risk; (e) its effectiveness in ensuring that slavery and human trafficking is not taking place in its business or supply chains, measured against such performance indicators as it considers appropriate; (f) the training about slavery and human trafficking available to its staff*," Section 54.5. Thus, this list is a mere guidance, J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation," *op. cit.* note 30, p. 333

[128] As in the Californian framework, private actors can merely disclose that "*they have 'taken no such steps'*," *Ibid.* p. 334

[129] E. Kenway, *The truth about modern slavery*, *op. cit.* note 51, pp. 105-107

[130] Q. Lake et al., *Corporate leadership on modern slavery: How have companies responded to the Modern Slavery Act one year on?*, Hult International Business School & Ethical Trading Initiative, 2016, pp. 14, 19

[131] I. Ras, C. Gregoriou, "The Quest to End Modern Slavery," *op. cit.* note 59, p. 104

[132] T. Sachs, C. Clerc, "Controverse," *op. cit.* note 111, p. 353

bound to do so by international ex ante *commitments*."[133]

493. The limits of transparency. However, as mandatory texts on corporate social responsibility are limited to broad transparency obligations, they are "*hard to measure or evaluate*,"[134] so "*the ambiguity around compliance softens the approach*."[135] Transparency through auditing has been specifically criticized as a way to prevent forced labor.[136] When these obligations are fulfilled minimally, they might be limited to "trafficking washing."[137] Furthermore, the implementation of the texts also highlights their limits. They lead to reports and statements whose "*format and depth […] vary widely [and] the level of granularity reported varies greatly from company to company*."[138] As underlined from the studies on the statements adopted accordingly to the Modern Slavery Act, the documents rely on stereotyped positions, as they "*tend to cast both consumers and commercial organizations as either ignorant (and thus innocent) or as (potential) heroes simply for doing their due diligence*" and still "*encourage continued consumption*."[139] As such, private actors portray themselves as "*protagonists […] who remediate an issue that is presumed to have been, if caused by any party, caused by some other party*," thus "*distracting from those individuals who make the business decisions that end up (both unwittingly and consciously)*

[133] Y. Gaudemet, "De la compliance à la vigilance : les entreprises au secours de l'État ?," *La Semaine Juridique Edition Générale*, LexisNexis, May 29, 2023, no. 21, p. 651
[134] C. Geiger, G. Frosio, E. Izyumenko, "Intermediary Liability and Fundamental Rights," *in* G. Frosio (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, p. 723
[135] J. Nolan, "Hardening Soft Law," *op. cit.* note 120, p. 70
[136] Indeed, "*Some of their most crucial shortcomings include: limited audit duration, resulting in a 'snapshot' of practices rather than long-term observation; weak audit methodologies with ample room for deception and cheating; financial conflicts of interest and commercial relations between audit firms and their clients; failure to encompass practices occurring beyond the factory gates, such as debt bondage to recruiters; a focus on first-tier suppliers' core workforces rather than the many layers of sub-contracting; marginalization of workers, who are most aware of how forced labors manifest on the ground, during the audit process*," G. LeBaron et al., *Confronting root causes: forced labour in global supply chains*, Open Democracy, Beyond Trafficking and Slavery Series, 2018, p. 59
[137] This expression is adapted from the concept of "greenwashing," in which private actors use certain transparency and marketing strategies to deceive the public regarding their real efforts to limit their impact on the environment and climate change. "Trafficking washing" could be a subdivision of "purple washing," for which actors use certain transparency and marketing strategies to deceive the public regarding their real efforts to limit the reproduction of misogynist models. Indeed, anti-trafficking actions have been developed from various feminist perspectives, emphasizing the role of sexist discrimination in supporting trafficking processes.
[138] P. Micek, D.D. Aydin, "Non-financial Disclosures in the Tech Sector: Furthering the Trend," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 253-254; N. Weinberg et al., "AI against Modern Slavery: Digital Insights into Modern Slavery Reporting -Challenges and Opportunities," *Proceedings of the AAAI Fall Symposium on AI for Social Good Virtual Symposium*, November 13, 2020
[139] I. Ras, C. Gregoriou, "The Quest to End Modern Slavery," *op. cit.* note 59, p. 106

encouraging modern slavery."[140] Similarly, non-financial information published on the basis of the Directive 2013/34/EU has not been "*sufficiently comparable or reliable*."[141]

494. Going further than transparency. Nevertheless, the prevention and repression of human trafficking require more than obligations regarding transparency.[142] To achieve this aim, the European, Spanish, and French frameworks appear to extend beyond transparency. Under Spanish law, a due diligence system is mandatory to apply the exemption to criminal liability.[143] Such a system requires prior organization and management models,[144] "*which include surveillance and control measures suitable for preventing offenses […] or for significantly reducing the risk of their commission*."[145] This monitoring should be "*entrusted to an organ of the legal person with autonomous powers of initiative and control*," that should not have omitted or insufficiently exercised these powers.[146] For instance, to prevent transnational human trafficking, corporations should prevent the commission of administrative offenses linked to the recruitment of foreign workers.[147] The case law came to support the idea that the exemption could be applied only when a real culture of legal compliance could be proved within the company or could not be applied when inappropriate compliance leads to a structural flaw.[148] Going further, the 2022 proposal on corporate sustainability due diligence would establish additional positive obligations, required have to integrate "*due diligence into their policies*," identify and assess "*actual or potential adverse impacts*," prevent and mitigate "*potential adverse*

[140] *Ibid.* p. 115
[141] J. Dunin-Wasowicz, A. Bourgin, N. Burnichon, "Entreprises et droits humains à l'aune de l'autonomie stratégique européenne," *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, p. 5
[142] Ezell cites "*three affirmative steps a corporation should take to fulfill its obligations to shareholders to minimize risks of human trafficking violations and the impact violations may have on the corporation: (1) implementing monitoring systems, (2) developing a human trafficking resolution or committee prepared to take enforcement action when aware of violations, and (3) giving adequate disclosure of risks*," L. Ezell, "Human Trafficking in Multinational Supply Chains: A Corporate Director's Fiduciary Duty to Monitor and Eliminate Human Trafficking Violations," *Vanderbilt Law Review*, 2016, vol. 69, no. 2, p. 540
[143] For a detailed explanation, see J.L. Alapont, "Criminal Compliance," *op. cit.* note 75, p. 1
[144] The models should include, in particular, a risk assessment, decision-making processes, the attribution of suitable financial means to implement the model, the obligation to inform of potential or actual violations, disciplinary processes, and periodical monitoring and updating of the model, Article 31bis.5 of the Código penal
[145] Article 31bis.2.1 of the Código penal
[146] Article 31bis.2.2 and 4 of the Código penal
[147] Articles 52 to 54 of the Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social. See J.G. Fernández Teruelo, "Responsabilidad penal de las personas jurídicas," *op. cit.* note 73, p. 9
[148] Tribunal Supremo. Sala Segunda, de lo Penal, February 29, 2016, no. 154/2016; Tribunal Supremo. Sala Segunda, de lo Penal, March 16, 2016, no. 221/2016

impacts," bring "*actual adverse impacts to an end*" and minimize their extent, establish and maintain "*publicly available and effective notification and non-judicial grievance mechanisms*," and "*continuously verify the implementation and monitor the adequacy and effectiveness of their actions*."[149] Similarly, in France, by establishing a duty of vigilance instead of diligence, the law seeks to mandate the adoption of measures with concrete results in favor of human rights.[150] Thus, the law focuses "*on the substantive actions [that] business entities must take to understand and address human rights risks*,."[151] and it mandates recipients to adopt a vigilance plan in coordination with all stakeholders.[152] However, the law requires only "*reasonable measures*," and the components of the plan are not detailed,[153] allowing corporations to soften their obligations.[154] The later evaluations of the law highlight a still-in-process integration of the duty of vigilance,[155] due to an "*unclear and unevenly shared understanding of [it], its insufficient readability and visibility in already dense management reports, [and] the relevant level of detail*."[156] The plans are still "*very much focused on the risks for the companies*" rather than on human rights.[157] If no further efforts are made to specify the duty of vigilance, such a process might evolve into "*tick-the-box compliance, not a real*

[149] Articles 5 to 10 of the 2022 proposal on corporate sustainability due diligence
[150] L. d'Ambrosio, "Le devoir de vigilance," *op. cit.* note 114, p. 643
[151] J. Nolan, "Hardening Soft Law," *op. cit.* note 120, p. 73
[152] The plan must include a risk mapping and assessment, regular monitoring processes, mitigation and prevention-adapted measures, an alert procedure, and an evaluation procedure of the measures, Article L225-102-4.I of the Code de commerce. The law lacks a provision on remedies and reparation, S. Olarte Encabo, "El desafío del trabajo decente en las cadenas mundiales de suministros," *op. cit.* note 64, p. 121
[153] T. Sachs, J. Tricot, "La loi sur le devoir de vigilance : un modèle pour (re)penser la responsabilité des entreprises," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, p. 690
[154] L. Moua, "La lutte contre la traite dans les entreprises," *op. cit.* note 102, p. 252
[155] "*In 2019, in half of the cases, […] the plans announce future mapping work, or are limited to a few lines to affirm that a mapping has been carried out, but without delivering any information on the method or content of the mapping […] Secondly, some plans focus on the risk mapping process […] without mentioning the content or nature of the risks. Conversely, a quarter of the plans designate the major risks that the mapping method leads to identify, but often remain silent on the method as such: the mapping is then presented as a list, more or less detailed and precise, of the main risks or major issues that it highlights. Finally, a minority of plans distinguish themselves by seeking to present the risk map in the form of graphic objects*," P.B. de Lagerie et al., "La mise en œuvre du devoir de vigilance," *op. cit.* note 91, pp. 706-707.
[156] A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399*, *op. cit.* note 91, pp. 8, 34-38
[157] J. Renaud et al., *Loi sur le devoir de vigilance des sociétés mères et entreprises donneuses d'ordre - Année 1 : les entreprises doivent mieux faire*, Forum Citoyen pour la RSE, February 2019, pp. 10-11. "*Companies often mentioned the risks that potential human rights abuses pose to the company and its performance, when it is the risks that the company poses to human rights and the environment that should be the focus of these plans*," *Ibid.* p. 15. This report highlights the lack of explanation of the methodology regarding the risk assessment and the lack of detail in its results. Nor do the plans make "*a clear distinction between vigilance policies for their subsidiaries and those for their suppliers and subcontractors*," *Ibid.* p. 16, or mention an evaluation of the measures, *Ibid.* p. 19.

day-to-day risk reduction policy."[158]

495. National and European norms are softened by their limitations on transparency obligations and by their vagueness. Thus, instead of setting adequate standards to coordinate the repression of human trafficking with private actors, the main question is still "*whether the business community has the will to self-regulate to prevent illegal behavior*."[159] This is an example of "*mandated self-regulation, in which a collective group […] is required or designated by the government to formulate and enforce norms within a framework defined by the government, usually in broad terms*."[160] The state appears here as an intermediary by establishing legal guidance on digital actors' potential coercion and control to repress human trafficking. Thus, current transparency and organizational compliance are not "*silver bullet[s]*" as they are "*supposed to be a means, not an end*."[161] Therefore, mechanisms of enforcement by states should be studied.

II. Public sovereigns: limited control

496. Transparency enforcement. Unfortunately, "*mechanisms for exacting compliance are weak*,"[162] even at the national level.[163] The norms mostly consider private actors liable for the lack of implementation of transparency obligations or compliance systems instead of holding them "*legally accountable for any actual adverse human rights impacts connected to their operations*."[164] California law and the Modern Slavery Act have been criticized for their lack of liability and sanctions for non-disclosure,[165] since enforcement is possible only through the production of an

[158] A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399*, *op. cit.* note 91, p. 38
[159] M. Delmas-Marty, *Le flou du droit: du code pénal aux droits de l'homme*, Presses universitaires de France, Les Voies du droit, 1st ed., 1986, p. 209
[160] J. Black, "Constitutionalising Self-Regulation," *op. cit.* note 7, pp. 27-29
[161] E. Kenway, *The truth about modern slavery*, *op. cit.* note 51, p. 107
[162] J.E. Cohen, *Between truth and power: the legal constructions of informational capitalism*, Oxford University Press, 2019, p. 246
[163] Under the EU norm, sanctions "*are limited to the disclosure requirement and not the extent and quality of the information disclosed*" and audit requirements are limited to "*a check that the non-financial statement has been provided, not that the information disclosed is correct*", K. Buhmann, "Neglecting the Proactive Aspect of Human Rights Due Diligence?," *op. cit.* note 33, pp. 42-43 and Article 51 of the Directive 2013/34/EU. On the contrary, the 2022 proposal on corporate sustainability due diligence details the sanctions that must be adopted by member states, Article 20.
[164] J. Nolan, G. Bott, "Global supply chains and human rights," *op. cit.* note 16, p. 53
[165] G. LeBaron, A. Rühmkorf, "Steering CSR Through Home State Regulation," *op. cit.* note 107, p. 17

injunction.[166] Nevertheless, the United Kingdom Home Office encourages collaboration: It provides a registry of statements, and it "*wrote directly to 16, 000 organizations […] to invite them to submit their statements to the registry*."[167] Many private actors complied voluntarily, highlighting a commitment to transparency despite the lack of strong enforcement mechanisms. Nonetheless, scholars underline that the act "*does not appear to have yielded substantive change in multinational enterprises' policy and practices regarding labor standards in their global supply chains*."[168] Similarly, French law allows requests for the creation of a vigilance plan through a letter of notice[169] and, then, a judicial injunction.[170] However, the civil fine of up to €10 million euros in cases of transparency non-compliance was declared unconstitutional.[171]

497. Other means of enforcement. Even so, scholars underline the need to draft, from a social responsibility perspective, a legal liability[172] by making private actors responsible for human rights violations, including human trafficking committed within their scope of control, due to the lack of implementation of effective compliance systems. The Spanish framework triggers the criminal liability of corporations for a lack effective implementation of due diligence systems.[173] This verification, for which

[166] The California text only considers a possible action for injunctive relief by the Attorney General, Section 1714.43.d of the California Civil Code. This never took place up until 2016, J. Planitzer, "Trafficking in human beings for the purpose of labour exploitation," *op. cit.* note 30, p. 329. See also Section 54.11 of the Modern Slavery Act, whose use has been limited, G. LeBaron et al., *Confronting root causes*, *op. cit.* note 136, p. 58. For instance, in the first two years after the passing of the act, "*The [United Kingdom] Department of Justice has brought a total of sixty-three cases. Thus, while the act was on the books, it was not sufficiently enforced*," C. Martell, "Customer Transparency Can Dampen the Growing Human Trafficking Problem," *Journal of Business, Entrepreneurship and the Law*, 2021, vol. 14, no. 1, p. 70

[167] HM Government et al., *2021 UK Annual Report on Modern Slavery*, United Kingdom, October 2021, p. 27

[168] G. LeBaron, A. Rühmkorf, "Steering CSR Through Home State Regulation," *op. cit.* note 107, p. 17

[169] Judges saw this letter of notice as a way to open dialogue between parties to the creation of the plan, and highly closed the way to judicial litigation by requiring further letters of notice once the dialogue failed, M. Hautereau-Boutonnet, B. Parance, "Prudence dans l'analyse du premier jugement sur le devoir de vigilance des entreprises ! - À propos du projet pétrolier en Ouganda et Tanzanie des filiales de TotalEnergies," *La Semaine Juridique Edition Générale*, LexisNexis, March 27, 2023, no. 12, p. 373

[170] Article L225-102-4.II of the Code de commerce. However, it is not clear if those demands should be registered in a civil or commercial court, A. Beckers, "Chaînes de valeur mondiales," *op. cit.* note 107, p. 146. Moreover, no mechanism has been planned specifically for the evaluation and following of the law to obtain updated information, A. Duthilleul, M. de Jouvenel, *Evaluation de la mise en oeuvre de la loi n° 2017-399*, *op. cit.* note 91, p. 19

[171] Conseil constitutionnel, *Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, March 23, 2017, 2017-750 DC, ¶ 14

[172] L. d'Ambrosio, P.B. de Lagerie, "La responsabilité des entreprises reformulée par la loi : un regard pluridisciplinaire," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, p. 626

[173] When the effectiveness of the compliance system cannot be fully proven but it exists, the sanction might be reduced, Article 31bis.2 and 4 of the Código penal

evidence is to be brought by the accusing parties,[174] is divided into two parts: First, the compliance program is assessed generally; second, the effectiveness of the program is assessed depending on the specific offense committed,[175] for instance, if it was appropriate to prevent human trafficking. However, criminal liability faces the difficulties presented earlier.[176] The French framework triggers civil liability for damages that might have been avoided by a correct implementation of the duty of vigilance.[177] Still, this provision does not modify the civil norms: It "*does not seek to impute damage or to establish the cause of the damage*."[178] It does not create an objective liability; plaintiffs still must prove the damage and causality.[179] The EU 2022 proposal on corporate sustainability due diligence requires member states to create a liability for private actors for damages deriving from their failure to comply with the positive obligations of the text,[180] but it remains to be seen how states will implement this liability framework.[181] This provision is seen as bold and might not remain in such terms in the final text.[182]

498. Conclusion of the section. Corporate social responsibility fosters collaboration between private actors, including digital actors, and states to improve the repression of human trafficking. However, when compliance systems are examined closely, it is apparent that "*legal efforts […] have been limited*"[183] and are not adapted to the fight against trafficking. Their scope barely mentions human trafficking; it is limited to very large private actors, while creating similar frameworks applicable to the same actors; and it is challenged by legal borders, since value chains hardly consider the multiplicity of transnational issues linked to cyber human trafficking. Moreover, the

[174] M.C. Rayón Ballesteros, "Cuestiones clave de las once primeras sentencias del Tribunal Supremo sobre la responsabilidad penal de la persona jurídica," *Revista Aranzadi de Derecho y Proceso Penal*, June 2018, vol. 50; Tribunal Supremo. Sala Segunda, de lo Penal, March 16, 2016, *op. cit.* note 148
[175] E. Gutiérrez Pérez, "Los *compliance programs* o la vuelta al *no body to kick, no soul to damn*. Una aproximación a la luz de la reforma del Código Penal por la Ley Orgánica 1/2015," *in* L.M. Díaz Cortés et al. (eds.), *Propuestas penales: nuevos retos y modernas tecnologías*, Ediciones Universidad de Salamanca, 2016, p. 391
[176] See *supra* Part 2. Title 1. Chapter 1. .
[177] Article L225-102-5 of the Code de commerce
[178] A. Hatchuel, B. Segrestin, "Devoir de vigilance : la norme de gestion comme source de droit ?," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, p. 670
[179] On the contrary, under an objective liability, the parent company would have been liable by default unless it had proven the effective implementation of an adequate vigilance plan, L. d'Ambrosio, "Le devoir de vigilance," *op. cit.* note 114, p. 646
[180] Article 22 of the 2022 proposal on corporate sustainability due diligence
[181] B. Lecourt, "Vers une directive sur le devoir de vigilance des sociétés," *op. cit.* note 64, p. 6
[182] *Ibid.* p. 8. However, the European Parliament particularly broadened the version of the Commission.
[183] J. Nolan, G. Bott, "Global supply chains and human rights," *op. cit.* note 16, p. 45

texts are close to soft law,[184] due to broad obligations limited mainly to transparency and a lack of enforcement means. While this situation might be seen as a beginning for co-regulation and a collaboration between sovereigns to set the guidelines and concrete implementation of corporate social responsibility, the balance remains in favor of private actors.[185] Current compliance systems support the independence of sovereign powers, but they limit the exportation of values to protect European sovereignties.[186] Therefore, the EU developed new forms of compliance systems dedicated to digital actors to protect European values, potentially applying them to order collaboration for repressing cyber human trafficking.

Section 2. Digital social responsibility: complementary cooperation against cyber human trafficking

499. Digital social responsibility and human trafficking. Corporate social responsibility is a useful discipline to coordinate the actions of states' and private actors to repress human trafficking by building systems of compliance to protect human rights in general. However, these systems are not appropriate for the specific fight against cyber human trafficking. In response to the weight of the United States in regulating and influencing digital actors, the EU has developed stricter frameworks to externalize core European values, "*such as privacy, security, accuracy, and transparency*";[187] their protection is increasingly transformed into obligations for digital actors.[188] This specific digital social responsibility,[189] at the crossroads of "*the obligation of states to protect individuals from violations of their rights by private actors, and the moral or ethical duties of corporations*,"[190] could be useful to improve collaboration in the fight against

[184] R. Steurer, "The role of governments in corporate social responsibility: characterising public policies on CSR in Europe," *Policy Sciences*, March 2010, vol. 43, no. 1, p. 51
[185] G. Teubner, "L'auto-constitutionnalisation des ETN," *op. cit.* note 7, p. 16
[186] The current European texts might not support a Brussels Effect, P.-H. Conac, "Sustainable Corporate Governance in the EU," *op. cit.* note 33, p. 118. For a definition of the concept, see *infra* 500.
[187] J. van Dijck, "Guarding Public Values in a Connective World: Challenges for Europe," *in* O. Boyd-Barrett, T. Mirrlees (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, p. 178
[188] In general, Internet governance was mainly developed through compliance systems, M.-A. Frison-Roche, "Gouvernance d'internet: 'Nous sommes face à un enjeu de civilisation,'" *Petites affiches*, Lextenso, July 18, 2019, no. 143, p. 4
[189] Or "*corporate social responsibility on the Internet*," R. Cohen-Almagor, "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications," *Journal of Business Ethics*, March 2012, vol. 106, no. 3, p. 356
[190] M.K. Land, "Toward an International Law of the Internet," *Harvard International Law Journal*, 2013, vol. 54, no. 2, p. 445

human trafficking.[191] These texts support the construction of processes conforming to the rule of law and the protection of human rights, resulting in the improvement of the fight against trafficking.

500. The Brussels Effect. The study of European digital social responsibility and its suitability to coordinate the actions of sovereign states and digital actors to repress cyber human trafficking focuses on two texts: the Digital Services Act[192] and the Proposal for an Artificial Intelligence Act.[193] To assess how they could protect European values and broadly support the autonomy of European approaches to combat human trafficking against the various US imperialisms, the theory of the Brussels Effect is used. This theory "*refers to the EU's unilateral power to regulate global markets [and] to promulgate regulations that shape the global business environment*" without needing to rely primarily on sanctions and coercion.[194] This theory "*explains how global corporations respond to EU regulations by adjusting their global conduct to EU rules [leading to] a broader set of mechanisms that transmit EU rules to foreign jurisdictions*."[195]

501. To determine how digital social responsibility is useful to coordinate the actions of digital actors to repress human trafficking with European values, two

[191] In particular, the Digital Services Act, European Commission, "Fourth report on the progress made in the fight against trafficking in human beings," EU, December 19, 2022, pp. 12-13, COM(2022) 736 final

[192] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). This Act will particularly be studied in relation to the German Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Network Enforcement Act), NetzDG, which influenced widely the European Act. Advocating in favor of the Brussels effect of the Digital Services Act, see A. Turillazzi et al., "The digital services act: an analysis of its ethical, legal, and social implications," *Law, Innovation and Technology*, Routledge, March 10, 2023, vol. 0, no. 0, p. 22. Advocating against the Brussels Effect of the Proposal for an Artificial Intelligence Act, see T. Christakis, *"European Digital Sovereignty": Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, p. 34. In particular, the adoption of slightly different national legislations on similar topics could challenge the Brussels Effect and creates legal insecurity for digtal actors. For instance, in France, the loi n° 2021-1109 confortant le respect des principes de la République was adopted before the adoption of the Digital Services Act, while creating similar but slightly different obligations (see for instance, Article 6.4 of the loi n° 2004-575 pour la confiance dans l'économie numérique).

[193] European Commission, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, April 21, 2021, COM/2021/206 final; European Parliament, Amendments on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, June 14, 2023, P9_TA(2023)0236. This study includes the amendments of the European Parliament.

[194] A. Bradford, *The Brussels effect: how the European Union rules the world*, Oxford University Press, 2020, p. xvi

[195] *Ibid.* p. 2

characteristics of the texts should be evaluated. Both their scope (§1) and measures (§2) should be adapted to anti-trafficking initiatives from digital actors.

§1. Digital social responsibility's scope: adaptation to human trafficking

502. Legal disciplines regulating online activities barely consider the repression of human trafficking, while anti-trafficking frameworks hardly contemplate the use of norms applied to digital activities and actors. Thus, at first sight, both the Digital Services Act and the Proposal for an Artificial Intelligence Act are not related to the repression of human trafficking. However, their material (I) and subjective (II) scopes can be interpreted in such a way to apply to anti-trafficking actions by digital actors.

I. Material scope: extension to anti-trafficking actions

503. Common aims. Both the Digital Services Act and the Proposal for an Artificial Intelligence Act create new obligations for internal market actors to ensure that "*fundamental rights enshrined in the Charter [of Fundamental Rights …] are effectively protected*"[196] as well as the "*EU's ultimate values*," in general.[197] Although the repression of human trafficking is not mentioned, it is implicitly included, as it is prohibited by the Charter.[198] However, this approach has been highly criticized regarding the Proposal for an Artificial Intelligence Act, since the main obligations applicable to high-risk systems depend on a pre-assessed level of risk by the Commission[199] and a further case-by-case assessment to verify whether "*they pose a significant risk of harm to the health, safety, or fundamental rights of natural*

[196] Article 1.1 of the Digital Services Act; many references to the Charter in the preamble (paragraphs 2b, 2f, 3, 4a, 9a, 10, 13, 16a, 28a, 38, 40a, 41, 41a, 72) and Article 4a.1 of the Proposal for an Artificial Intelligence Act

[197] F. Bueno de Mata, "Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2021, no. 150, pp. 7-8; C. Castets-Renard, "Quelle politique européenne de l'intelligence artificielle ?," *Revue trimestrielle de droit européen*, 2021, p. 298

[198] Article 5.3 of the Charter of Fundamental Rights of the EU

[199] Y. Meneceur, *Analyse des principaux cadres supranationaux de régulation de l'intelligence artificielle : de l'éthique à la conformité*, Projet d'étude, May 27, 2021, p. 22, online https://lestempselectriques.net/index.php/2021/05/27/analyse-des-principaux-cadres-supranationaux-de-regulation-de-lintelligence-artificielle-de-lethique-a-la-conformite/ (retrieved on May 28, 2021). In the original version, no mandatory rules regarded the prohibition of discrimination and the protection of gender equality, F. Lütz, "Gender equality and artificial intelligence in Europe. Addressing direct and indirect impacts of algorithms on gender-based discrimination," *ERA Forum*, May 1, 2022, vol. 23, no. 1, p. 42. Such a provision was included by the European Parliament, Article 4a.1.e of the Proposal for an Artificial Intelligence Act

persons."[200] Thus, providers of high-risk systems according to the Commission can declare that they are not required to comply with obligations linked to these systems if their own system "*does not pose a significant risk*," based on their internal assessment.[201] Additionally, both texts establish harmonized rules, particularly based on due diligence obligations,[202] to frame self-regulation by digital actors.[203] Thus, they are digital corporate social responsibility frameworks designed to develop coordination with digital actors while ensuring European sovereignties.

504. Moderating illegal content. In particular, the Digital Services Act regulates content moderation,[204] which It is defined as "*the activities, whether automated or not […] that are aimed, in particular, at detecting, identifying, and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility , and accessibility of that illegal content or that information […] or that affect the ability of the recipients of the service to provide that information*."[205] This definition avoids a limitation on "*binary remove-or-not decision[s]*" due to illegal content under national laws.[206] The latter concept is defined as "*any information that, in itself or in relation to an activity […] is not in compliance with Union law or the law of any Member State*."[207] Due to the broadness of this definition,[208] scholars underline that what is protected by

[200] Article 6.2 of the Proposal for an Artificial Intelligence Act
[201] Article 6.2a of the Proposal for an Artificial Intelligence Act
[202] Article 1.2.b and c of the Digital Services Act, Article 1.1 of the Proposal for an Artificial Intelligence Act. Although the second text does not mention the concept of due diligence, the obligations laid down, especially regarding transparency, are to be framed within this concept.
[203] A. Joux, "DMA, DSA : l'Europe va réguler les plateformes," *La revue européenne des médias numériques*, March 18, 2021, online https://la-rem.eu/2021/03/dma-dsa-leurope-va-reguler-les-plateformes/ (retrieved on April 29, 2021)
[204] P. Auriel, "La liberté d'expression et la modération des réseaux sociaux dans la proposition de Digital Services Act," *Revue de l'Union européenne*, 2021, p. 416. This incentive to regulate content moderation can be linked to the decrease in trust in the self-regulation of digital actors to deal with illegal content moderation, and to the introduction of national laws to target online hate speech, A. Bradford, *The Brussels effect*, *op. cit.* note 194, p. 143
[205] Article 3.t of the Digital Services Act
[206] C. Busch, "Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation Special Issue: Governing the Digital Space," *UCLA Journal of Law and Technology*, 2022, vol. 27, no. 2, p. 39
[207] Article 3.h of the Digital Services Act
[208] For instance, the definition is not limited to illegal content under criminal laws but includes harmful content prohibited under other frameworks or whose dissemination requires specific conditions (such as pornography). For an approach to the difference between strictly illegal and harmful content, see European Commission, "Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Illegal and Harmful Content on the Internet," EU, October 16, 1996, COM(96)487 final. However, this "one-size-fits-all" approach is criticized, M.D. Cole, C. Etteldorf, C. Ullrich, *Updating the Rules for Online Content Dissemination - Legislative Options of the European Union and the Digital Services Act Proposal*, Nomos Verlagsgesellschaft mbH & Co. KG, 2021, pp. 125-127. On the contrary, this broad definition avoids limiting illegal content to "hate speech"

freedom of expression or criminalized—for instance, sex work[209]—still differs significantly depending on member states.[210] This concept has been criticized as "*extremely open and vague*,"[211] leading digital actors to implement their own prohibitions.[212] Even so, digital actors can rely on the EU's harmonized definition of human trafficking as illegal content.

505. Artificial intelligence. Content moderation might be realized through artificial intelligence systems. These can be used for other purposes and by other actors outside the scope of the Digital Services Act, particularly to improve the repression of human trafficking.[213] Therefore, the Proposal for an Artificial Intelligence Act establishes transversal rules on this topic.[214] First, the text defines an "artificial intelligence system" as "*a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments*."[215] Scholars criticized the prior version of the definition for merely referring to a list of types of algorithms.[216] However, this newer version is also

---

or "fake news," as in Section 1.3 of the German NetzDG, whose material scope was restricted to a list of offenses from the criminal code, A. Rochefort, "Regulating Social Media Platforms: A Comparative Policy Analysis," *Communication Law and Policy*, Routledge, April 2, 2020, vol. 25, no. 2, p. 245. This list does not include human trafficking, although other offenses could be linked to this offense, in particular: Section 111 (public incitement to commit crimes), Sections 129bis and 129b (formation of criminal organizations), Section 131 (depiction of violence), Section 184b (distribution, acquisition, and possession of child pornography content), and Section 201a (violation of the highly personal area of life and personal rights through image recordings) of the Strafgesetzbuch

[209] See *supra* Part 2. Title 1. Chapter 2. .

[210] For instance, "*Hungarian law prohibits certain "communist" or LGBTQI (lesbian, gay, bi, trans, queer, intersex) words and symbols that are not a problem in the rest of the Union*," C. Perarnaud, "Pour automatiser la censure, cliquez ici," *Le Monde diplomatique*, July 1, 2022, online https://www.monde-diplomatique.fr/2022/07/PERARNAUD/64826 (retrieved on July 11, 2022)

[211] J. Barata, "Obligations, Liabilities and Safeguards in Content Moderation," *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, March 2, 2021, online https://intr2dok.vifa-recht.de/receive/mir_mods_00010155 (retrieved on November 27, 2021)

[212] Indeed, it questions "*how a hosting service provider is capable of interpreting all sections of criminal law, intellectual property rights, privacy and personal data regulation, compensation or tort law, consumer law and such special fields*," P. Korpisaari, "From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act," *Journal of Media Law*, Routledge, November 24, 2022, vol. 0, no. 0, p. 23

[213] See *supra* Part 2. Title 1. Chapter 2. Section 2. .

[214] C. Castets-Renard, "Quelle politique européenne de l'intelligence artificielle ?," *op. cit.* note 197, p. 299

[215] Article 3.1 of the Proposal for an Artificial Intelligence Act. This definition comes from the OECD framework, leading to a beginning of harmonization, Y. Meneceur, *Analyse des principaux cadres supranationaux de régulation de l'IA*, *op. cit.* note 199, p. 14

[216] J. Mökander et al., "Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation," *Minds & Machines*, June 1, 2022, vol. 32, no. 2, p. 258

denounced, as the listing is moved to Recital 6 of the text, thereby limiting its technology-neutral approach of the text.[217] Second, artificial intelligence systems are classified according to four levels of risks,[218] which are referred to as a "*risks pyramid.*"[219] In particular, two levels of risk are of special interest for anti-trafficking actions. First, under banned systems, the European Parliament added systems dedicated to predictive policing,[220] questioning the mere legality of algorithms to detect trafficked victims online.[221] Second, high-risk systems include, in general, those posing "*a significant risk of harm*" to fundamental rights,[222] and, in particular, those used in the fields of employment[223] or migration[224] and used by law enforcement authorities.[225] The difference between banned systems and high-risk systems seems vague, especially for the application of the text to artificial intelligence systems that are

[217] J. Sénéchal, "Vote des parlementaires européens sur l'AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s'inspirant du DSA, du Data Act et du RGPD ?," *Dalloz actualité*, Dalloz, June 22, 2023

[218] The four levels are the following: "*(i) extreme risk applications, which are prohibited; (ii) high risk applications, dealt with by a conformity assessment […]; (iii) a limited number of applications that have a significant potential to manipulate persons, which must comply with certain transparency obligations; (iv) no high-risk uses, dealt with by codes of conduct*," A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, T.M.C. Asser Press; Springer, Information Technology and Law Series, 2022, vol. 36, pp. 167-168. For a critic on the criterion of risk to assess artificial intelligence systems, see J. Chamberlain, "The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective," *European Journal of Risk Regulation*, Cambridge University Press, December 5, 2022, pp. 1-13; C. Novelli et al., "Taking AI risks seriously: a new assessment model for the AI Act," *AI & SOCIETY*, July 12, 2023. Other scholars criticized the vagueness of this approach and, in particular, the lack of a precise definition of high-risk artificial intelligence systems, J.M. Muñoz Vela, *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas: de lo dispositivo a lo imperativo*, Thomson Reuters Aranzadi, 1st ed., 2021, chap. 5

[219] A. Bensamoun, "Artificial Intelligence Act : l'Union européenne invente la pyramide des risques de l'intelligence artificielle," *Le Club des Juristes*, May 21, 2021, online https://blog.leclubdesjuristes.com/artificial-intelligence-act-lunion-europeenne-invente-la-pyramide-des-risques-de-lintelligence-artificielle/ (retrieved on June 17, 2021)

[220] Article 5.1.d a of the Artificial Intelligence Act Proposal

[221] See *supra* 468.

[222] Article 6.2 of the Proposal for an Artificial Intelligence Act, M. Martín-Casals, "An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems," *Ius et Praxis*, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, August 2022, vol. 28, no. 2, p. 5

[223] Annex III.1.4 of the Proposal for an Artificial Intelligence Act

[224] Annex III.1.7 of the Proposal for an Artificial Intelligence Act

[225] In particular, used as "*polygraphs and similar tools, insofar as their use is permitted under relevant Union and national law […] to evaluate the reliability of evidence […] for profiling of natural persons*," and "*for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data*," which is particularly relevant for the artificial intelligence systems developed and used in the United States. Moreover, this list has been criticized as it does not "*address more in detail the vast field of law enforcement activities*," S. Roksandić, N. Protrka, M. Engelhart, "Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?," *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022, pp. 1229-1230

designed to detect patterns of trafficking online.[226] On the contrary, the last version by the European Parliament of the listing excludes artificial intelligence systems that focus on content moderation,[227] which are among the systems that "*are nevertheless usually identified as harmful*" to fundamental rights.[228]

506. Brussels Effect: market size. Thus, the Digital Services Act and the Proposal for an Artificial Intelligence Act regulate content moderation and artificial intelligence systems through a lens of fundamental rights. The first criterion of the Brussels Effect is market size: The EU's market power to influence digital actors and to protect its values and sovereignty "*depends on the attractiveness of its consumer market compared to the alternative markets available*."[229] Digital actors broadly rely on the EU consumer market to develop their activities. On the contrary, Bradford considers that the EU "*has little leverage over targets of regulation that are not subject to market access*,"[230] leading to the absence of the Brussels Effect in the field of human rights. Nonetheless, market size and fundamental rights are linked in these texts, as the EU aims to oblige digital actors to incorporate rule-of-law values.

507. Furthermore, these texts offer standards for international legal competitiveness,[231] thanks to their broad subjective scope, which making it appropriate to include digital actors who are involved in the repression of cyber human trafficking.

II. Subjective scope: inclusion of digital actors repressing trafficking

508. Subjective scope: pyramid of actors. The Digital Services Act broadly applies to "*intermediary services*,"[232] mainly the categories already established by the

---

[226] Moreover, those modifications to the list of high-risk artificial intelligence systems create confusion as they do not "*substantially differentiate between levels of high risk systems*." This is also due to the almost complete lack of "*any rules to follow [by] systems that can have an 'indirect midlevel' effect on citizens*," *Ibid.*

[227] Although it has been discussed A. Bogucki et al., *The AI Act and emerging EU digital acquis. Overlaps, gaps and inconsistencies*, CEPS In-Depth Analysis, Centre for European Policy Studies, September 14, 2022, p. 3. However, the European Parliament added as high-risk recommender systems of social media designed as very large online platforms according to the Digital Services Act, Annex III.1.8 ab of the Proposal for an Artificial Intelligence Act

[228] J. De Cooman, "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act," *Market and Competition Law Review*, March 23, 2022, vol. 6, no. 1, p. 67

[229] A. Bradford, *The Brussels effect*, *op. cit.* note 194, p. 26

[230] *Ibid.* p. 30. Yet she later recognized the power of the EU due to its market size on the topic of online hate speech and content moderation, *Ibid.* pp. 140, 145

[231] A. Bensamoun, *Artificial Intelligence Act*, *op. cit.* note 219

[232] Article 2.1 of the Digital Services Act. Within this general category appears the specific group of "*online search engines*," Article 3.j. This latter category has been criticized as it does not have specific obligations, leading to questions about its necessity, S. Merabet, "Le Digital Services Act : permanence

E-Commerce Directive:[233] "mere conduit" services such as Internet service providers, "caching" services such as content delivery networks, and "hosting" services such as social media or marketplaces.[234] Hosting services includes "*online platform*," which, "*at the request of a recipient of the service, stores and disseminates information to the public*," meaning "*to a potentially unlimited number of third parties*."[235] The criterion of "dissemination to the public" has been criticized, since it supposes to exclude the "*dissemination of information within closed groups composed of a finite number of predetermined individuals*," such as the service of WhatsApp or email services.[236] This excludes digital actors used for trafficking in direct communications from the additional obligations set by the text. Within this category are "*very large online platforms*," designated by the European Commission[237] as those that "*which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million*."[238] The Digital Services Act establishes a period to verify these data but

---

des acteurs, renouvellement des qualifications," *La Semaine Juridique Edition Générale*, LexisNexis, October 17, 2022, no. 41, ¶ 9

[233] Thus, the text will face the same difficulties of interpretation as the e-commerce directive, S.F. Schwemer, T. Mahler, H. Styri, "Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?," *Oslo Law Review*, Universitetsforlaget, 2021, vol. 8, no. 01, pp. 28-29. See *supra* Part 2. Title 1. Chapter 1. Section 1. §2. . Slightly differently, the NetzDG applies to telemedia service providers, "*classified as the following: 1) access providers who "connect the user to the internet via a telecommunication line or link," 2) host providers who host customer websites on "technical facilities" for connection to the internet, or 3) content providers who offer "services such as databases, entertainment or information offers, or online shopping"*," L.E. Moon, "A New Role for Social Network Providers: NetzDG and the Communications Decency Act," *Transnational Law & Contemporary Problems*, 2019, vol. 29, no. 1, p. 612

[234] Article 3.g of the Digital Services Act

[235] Article 3.i and k of the Digital Services Act

[236] J. Cruz Ángeles, "Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso," *Cuadernos de derecho transnacional*, September 29, 2022, vol. 14, no. 2, ¶ 19. The NetzDG also excluded from its scope "*platforms which are designed to enable individual communication or the dissemination of specific content*," Section 1.1 *in fine*. This definition was deemed to also exclude online games and sales platforms, P. Zurth, "The German NetzDG as Role Model or Cautionary Tale? – Implications for the Debate on Social Media Liability," *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2021, vol. 31, no. 4, pp. 1103-1104. Moreover, the concepts that regulate digital actors multiply, leading to a lack of clarity in the whole legal order, S. Merabet, "Le Digital Service Act (1)," *op. cit.* note 232, ¶ 8

[237] This designation procedure is needed to provide legal certainty on the starting date of their supplementary obligations, S. Merabet, "Le Digital Service Act (1)," *op. cit.* note 232, ¶ 11

[238] Article 33 of the Digital Services Act. It also includes very large online search engines. For the first round of designation, the European Commission listed: as very large online platforms, Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, and Zalando; as very large online search engines, Bing and Google Search, European Commission, "DSA: Very Large Online Platforms and Search Engines," *European Commission*, April 25, 2023, online https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 (retrieved on May 12, 2023). The NetzDG sets a similar criterion, as its scope is limited to services that have more "*than two million registered users in the Federal Republic of Germany*," Section 1.2

does not consider the possibilities of a disguised location.[239] Additionally, this single criterion has been denounced for failing to reach a sufficient number of actors.[240] As traffickers look for new online services to hide their activities, this limitation might indeed reduce the effectiveness of the text to apply to the repression of cyber human trafficking. However, this pyramid allows for the adaptation of standards to the numerous categories of digital actors.[241]

509. Subjective scope: providers and deployers. The Proposal for an Artificial Intelligence Act applies to all operators[242] in the life cycle of an artificial intelligence system.[243]. Providers[244] of artificial intelligence systems are the core actors of the text, along with their deployers, who are "users" in the text of the Commission,[245] and subcategories of providers are developed: importers, distributors, and authorized

[239] The NetzDG was criticized as it does not take into account either of these two challenges, aside from being vague regarding "*which users exactly fall under that definition*," P. Zurth, "The German NetzDG as Role Model or Cautionary Tale?," *op. cit.* note 236, p. 1104. Scholars argued that the number of registered users was dependent on the "*IP address that was used when the user registered*," H. Lutz, S. Schwiddessen, "The New German Hate Speech Law – Introduction and Frequently Asked Questions," *Computer Law Review International*, Verlag Dr. Otto Schmidt, July 26, 2017, vol. 18, no. 4, p. 107

[240] Differently, the concept of "structuring platform" is based on various indicators such as "*the access to the data from which the platform benefits, the degree of portability of this data, its unavoidable character, its possible dominant position on a market, its possible integration on neighboring markets, its possibilities of conglomerate expansion, its financial power, the network effects and economies of scale from which it benefits, its capacity to define the rules of the market, its ability to put a regulator in a situation of asymmetry of information, the possibilities of differentiation between the players, or the importance of the costs of migration for users*," A.-S. Choné-Grimaldi, "Digital Services Act - Vers un nouveau droit de la concurrence et de la régulation applicable au secteur numérique ?," *La Semaine Juridique Edition Générale*, November 30, 2020, no. 49, p. 2182. However, other authors have argued that it "*covers more platforms than the "usual suspects" […so] the [Digital Services Act] is [not] targeted at Big Tech only*," B. Wagner, "A first impression of regulatory powers in the Digital Services Act," *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, January 4, 2021, online https://intr2dok.vifa-recht.de/receive/mir_mods_00009734 (retrieved on November 27, 2021). The NetzDG threshold was only deemed too low, limiting its effectiveness. For instance, in 2021, only "*eight platforms meet the user threshold […]: Change.org, Facebook, Instagram, Jodel, Reddit, SoundCloud, TikTok, Twitter and YouTube*," R. Griffin, *New School Speech Regulation and Online Hate Speech: A Case Study of Germany's NetzDG*, SSRN Scholarly Paper, ID 3920386, Social Science Research Network, September 9, 2021, pp. 17, 21

[241] M. Cornils, *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries*, Algorithm Watch, May 26, 2020, p. 74

[242] Article 3.8 of the Proposal for an Artificial Intelligence Act

[243] Article 2.1 of the Proposal for an Artificial Intelligence Act

[244] Defined as "*a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name*," Article 3.2 of the Proposal for an Artificial Intelligence Act

[245] Defined as "*any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity*," Article 3.4 of the Proposal for an Artificial Intelligence Act. "*The distinction between provider and user is especially important because these two roles carry nearly all of the regulatory responsibility*," A. Engler, A. Renda, *Reconciling the AI Value Chain with the EU's Artificial Intelligence Act*, CEPS In-Depth Analysis, Centre for European Policy Studies, September 30, 2022, p. 4

representatives.[246] The various actors in the artificial intelligence life cycle rely on pre-existing concepts, facilitating its coherency within the EU legal structure.[247] Thus, this text would apply to both European law enforcement authorities who use artificial intelligence systems to support their anti-trafficking actions and to digital actors who developing these systems for content moderation.

510. Territorial scope. Both the territorial scopes of the Digital Services Act and the Proposal for an Artificial Intelligence Act are defined mainly depending on the establishment of users or deployers[248] instead on the establishment of digital actors. This definition allows for the application of the norms to foreign actors according to the "*market location principle*," a solution that was already chosen in the GDPR.[249] In particular, the Digital Services Act settles for the requirement of a "*substantial connection*" to the EU territory, through the presence of an establishment; or "*a significant number of recipients of the service in one or more Member States in relation to its or their population; or the targeting of activities towards one or more Member States*,"[250] through, for instance, its language, "*a currency generally used in [a] Member State, or the possibility of ordering products or services*."[251] The Proposal for an Artificial Intelligence Act similarly extends its territorial scope to providers of artificial intelligence systems on the market or in service in the Union, deployers established or located in the Union, and providers and deployers when "*either Member State law applies by virtue of a public international law or*" the output of the system is intended to be used in the Union.[252] These broad criteria allow, "*on the one hand, to ensure*

[246] Article 3.5 to 7 of the Proposal for an Artificial Intelligence Act. All other operators can become providers under Article 28. However, those rules have been criticized by considering the realities of the evolution of the roles of the different actors linked to an artificial intelligence system's lifecycle, A. Engler, A. Renda, *Reconciling the AI Value Chain with the EU's Artificial Intelligence Act*, *op. cit.* note 245

[247] C. Crichton, "Projet de règlement sur l'IA (I) : des concepts larges retenus par la Commission," *Dalloz Actualité*, Dalloz, May 3, 2021. However, they are not fully aligned "*with internationally agreed definitions and existing terminology in the EU digital policy acquis*," A. Bogucki et al., *The AI Act and emerging EU digital acquis*, *op. cit.* note 227, p. 25

[248] Positively, the texts do not differentiate between consumers and professionals, S. Merabet, "Le Digital Service Act (1)," *op. cit.* note 232, ¶ 3

[249] M.D. Cole, C. Etteldorf, C. Ullrich, *Updating the Rules for Online Content Dissemination*, *op. cit.* note 208, pp. 155-156. A similar approach was adopted by the NetzDG, section 1.

[250] Article 3.d and e of the Digital Services Act

[251] Preamble ¶8 of the Digital Services Act

[252] Article 2.1 of the Proposal for an Artificial Intelligence Act. Article 2.4 nonetheless excludes its application "*to public authorities in a third country […] where those authorities […] use [artificial intelligence] systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States and are subject of a decision of the Commission adopted in accordance with Article 36 of Directive (EU)2016/680*." As there is no adequacy decision with the United States, the regulation could apply to the use of American algorithms to detect human trafficking online in the framework of an international cooperation.

compliance and security of systems developed, deployed, or used in the EU, whatever their origin, and, on the other hand, to ensure fair and ethical competition from third-country developers and manufacturers, who will be subject to this framework to deploy or use their technology in the EU."[253] The text, thus, would apply to digital actors providing artificial intelligence systems to European actors or when using them to lead to an outcome within the EU, such as when moderating content originated by EU recipients.

511. The Brussels Effect: inelastic targets and non-divisibility. Both texts could support a Brussels Effect through their extraterritorial and voluntary application, leading to the protection of European values and sovereignties in coordination with digital actors' activity. By establishing a territorial scope based on the market location principle, recipients of the norms are inelastic (immobile) targets: "*They cannot 'shop' for favorable regulations without losing access to the regulated market*."[254] Additionally, the establishment of such a territorial scope creates "*legal non-divisibility*:" The broad territorial and subjective scopes create "*drivers of uniform standards*," as they might lead to "*a spillover effect that follows from the corporation's compliance with the laws of the most stringent jurisdiction*." This effect is supported by a "*technical non-divisibility,*" which results from "*the difficulty of separating the firm's production or services across multiple markets for technological reasons*," and an "*economic non-divisibility,*" which happens when the production of different products or services for multiple markets is not economically tenable due to scale economies.[255] Thus, "*as code writing becomes commercial—as it becomes the product of a smaller number of large companies—the government's ability to regulate it increases*."[256] However, by its extraterritorial application, the Brussels Effect is criticized as a means for the EU's regulatory protectionism.[257] Even so, Bradford highlights that "*European companies*

[253] J.M. Muñoz Vela, *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas*, *op. cit.* note 218, chap. 5
[254] A. Bradford, *The Brussels effect*, *op. cit.* note 194, pp. 48-53
[255] The "*simplification in manufacturing or service provision [leads] to additional cost savings and safer products* [and] *a single standard also facilitates the preservation of a global brand and reputation*," *Ibid.* pp. 53-63. However, the obligations of the Digital Services Act might only impact recipients in the EU, similar to obligations derived from the NetzDG which are usually only visible from a German connection. However, the transparency obligations will be available globally. The technical non-divisibility effect is more stringent regarding the development and use of artificial intelligence systems, as they might not be modified depending on the region in which they are supposed to function.
[256] L. Lessig, *Code*, Basic Books, 2nd ed., 2006, p. 71
[257] According to various authors, the late logic of the regulation of digital actors highlights a "*logic of protecting the national society [that] takes precedence over the logic of an international society structured by the principle of the free exercise of digital activities*," C. Castets-Renard, V. Ndior, L. Rass-

are hardly the main beneficiaries" of these regulations: Instead of developing protectionism, the EU means to develop stronger regulations to enhance coordination and to protect values.[258] Therefore, these regulations might be seen as "*regulatory imperialism*," which would face the imperialistic policies of the United States. However, Bradford answers that "*The EU is simply asking others to play by its rules when operating in its home market, and enforcing the norms of the single market equally on domestic and foreign players. If the self-interest of multinational corporations leads them to voluntarily adopt the EU regulation across their global operations, the EU can hardly be accused of 'imperialism*'."[259]

512. The Digital Services Act offers a broad scope, which is appropriate to include activities linked to or applied to the repression of cyber human trafficking, such as content moderation. The current version of the Proposal for an Artificial Intelligence Act also has a broad subjective and territorial scope. Still, the multiple debates around the limits of banned and high-risk systems could lead to the prohibition of systems designed to detect patterns of trafficking online and to apply them only at the margin to content moderation systems. Nevertheless, while they do not include the repression of trafficking and exploitation in their goals, these frameworks could support this aim, as they are indirectly meant to protect human rights. It remains to be seen whether useful coordination obligations are applicable to the various recipients.

§2. Digital social responsibility: content and control

513. Digital social responsibility extends further than corporate social responsibility. Strengthened obligations to digital actors (I) and enhanced mechanisms of enforcement (II) support the coordination between digital actors and states to repress cyber human trafficking.

I. Private sovereigns' obligations: improving cooperation

514. Transparency obligations. As with corporate social responsibility, digital corporate social responsibility provides for transparency obligations that are more

Masson, "Introduction," *in* C. Castets-Renard, V. Ndior, L. Rass-Masson (eds.), *Enjeux internationaux des activités économiques: entre logique territoriale des États et puissance des acteurs privés*, Larcier, Création, information, communication, 2020, p. 13

[258] A. Bradford, *The Brussels effect*, *op. cit.* note 194, pp. 241-246

[259] *Ibid.* pp. 247-253

detailed. The Digital Services Act establishes different obligations for various categories of digital actors.[260] All providers of intermediary services[261] are required to publish, at least once a year, a report on content moderation.[262] This report must include specific information, such as the number of orders from member states to act against illegal content and to provide information, as well as meaningful data on proactive moderation, both categorized by type of illegal content[263], which, thus, should include information on moderation regarding content linked to human trafficking or related offenses. Additionally, hosting services must submit information regarding users' notices for alleged illegal content,[264] which could lead to even more data on moderation linked to human trafficking. Further information is required from online platforms,[265] particularly very large ones.[266] The latter should include details about the training of content moderators,[267] which could include training on the evolution of human trafficking online.[268] It remains to be seen what the quality of the reports will

[260] C. Busch, "Regulating the Expanding Content Moderation Universe," *op. cit.* note 206, p. 55

[261] Except for micro and small enterprises that are not designated as very large online platforms, Article 15.2 of the Digital Services Act. For a definition, see Article 2.2 and 3 of the Annex of the European Commission, "Recommendation concerning the definition of micro, small and medium-sized enterprises," May 6, 2003

[262] Article 15 of the Digital Services Act. "*The measure is particularly welcome as it is difficult to establish the faults of an operator because of the informational asymmetry that benefits hosting companies and other intermediary services*," S. Merabet, "Le Digital Services Act : guide d'utilisation de lutte contre les contenus illicites," *La Semaine Juridique Edition Générale*, October 24, 2022, no. 42, ¶ 12. This information must be "*publicly available, in a machine-readable format and in an easily accessible manner [, …] clear, [and] easily comprehensible*," Article 15.1. This "*sets a golden standard*" close to the requirements of Article 12.1 of the GPDR on the right to information. However, conforming to these standards will be challenging. "*First, easily accessible is already problematic given the amount of information that has to be provided […] Second, conciseness is another problem [: …] several topics discussed in this paper are complex and they cannot be explained concise and clear at the same time. Third, most consumers are not interested at all in all this information*," A.R. Lodder, J. Morais Carvalho, *Online Platforms: Towards An Information Tsunami with New Requirements on Moderation, Ranking, and Traceability*, SSRN Scholarly Paper, ID 4050115, Social Science Research Network, March 4, 2022, p. 14. The NetzDG was partly already considering the publication of this kind of information, and it adds more specific information to their own transparency reports, for instance the "*time between complaints being received by the social network and the unlawful content being deleted or blocked*," Section 2.2.8, or "*which groups are particularly likely to post or be affected by illegal content*," R. Griffin, *New School Speech Regulation and Online Hate Speech*, *op. cit.* note 240, p. 18. For a study of these transparency obligations, see J. Park, *The public-private partnerships' impact on transparency and effectiveness in the EU internet content regulation : the case of "Network Enforcement Act (NetzDG)" in Germany*, Thesis, Universitätsverlag Potsdam, 2020, pp. 43-48. The harmonization between European and national rules will then be one of the main challenges for digital actors.

[263] Article 15.1.a and c of the Digital Services Act

[264] Article 15.1.b of the Digital Services Act

[265] Article 24 of the Digital Services Act

[266] Article 42 of the Digital Services Act

[267] This element was already included in the NetzDG. After passing the law, "*80 moderators at Facebook and seventy-three at YouTube have been specifically trained to evaluate content prohibited by the NetzDG*," which, however, does not include human trafficking, R. Badouard, "Ce que peut l'État face aux plateformes," *Pouvoirs*, April 27, 2021, vol. N° 177, no. 2, p. 54

[268] Article 42.2.b of the Digital Services Act

be.[269]

515. Vigilance obligations. Going further, very large online platforms have obligations regarding vigilance. They must publish audit reports, risk assessment reports, information about mitigation measures, and audit implementation reports.[270] Thus, they are required to conduct diligent risk assessments related to the design, functioning, or use of their services, particularly through "*the dissemination of illegal content*,"[271] which would then include the potential for traffickers to use online services. Linked to these risks, very large online platforms must implement "*reasonable, proportionate, and effective mitigation measures*," including by adapting their terms of service and their enforcement or their moderation processes.[272] Mitigation measures regarding illegal content might include "*the expeditious removal of, or the disabling of access to, the content notified*"[273] or "*taking awareness-raising measures*"[274] that might be useful for the repression of cyber human trafficking.

516. Cooperation obligations. Finally, the Digital Services Act develops measures to ensure cooperation between law enforcement authorities and digital actors.[275] These provisions will be especially useful in coordinating the repression of cyber human trafficking. First, law enforcement and administrative authorities can issue orders to providers of intermediary services to act against illegal content or to

[269] The reports published under the NetzDG have been criticized for the "*lack of substantial information*," despite the criteria set by the law, A. Heldt, "Reading between the lines and the numbers: an analysis of the first NetzDG reports," *Internet Policy Review*, June 12, 2019, vol. 8, no. 2, p. 2; J. Park, *The public-private partnerships' impact on transparency*, *op. cit.* note 262, pp. 22, 53; R. Griffin, *New School Speech Regulation and Online Hate Speech*, *op. cit.* note 240, pp. 20, 24. In particular, these reports "*do not all provide reliable numbers*," A. Heldt, "Let's Meet Halfway: Sharing New Responsibilities in a Digital Age," *Journal of Information Policy*, Penn State University Press, 2019, vol. 9, p. 342. However, the Digital Services Act plans the development of common guidelines for these reports, Article 15.3, which do not exist under the NetzDG, T. Kasakowskij et al., "Network enforcement as denunciation endorsement? A critical study on legal enforcement in social media," *Telematics and Informatics*, March 2020, vol. 46, p. 101335

[270] Article 42.4 of the Digital Services Act

[271] Article 34.1.a of the Digital Services Act

[272] Article 35.1 of the Digital Services Act

[273] Article 35.1.c of the Digital Services Act

[274] Article 35.1.i of the Digital Services Act

[275] Those measures are particularly interesting as they were not included in the original NetzDG, which only considered transparency obligations: by only having to take down notified content and without formal obligations of cooperation, the NetzDG did "*not really help finding the culprit*" of offenses, W. Schulz, *Regulating Intermediaries to Protect Privacy Online – The Case of the German NetzDG*, SSRN Scholarly Paper, ID 3216572, Social Science Research Network, July 19, 2018, p. 10. However, the law was later modified to include obligations "*to send removed illegal content to the [Federal Criminal Police Office - Bundeskriminalamt], with the poster's IP address [… and] Complainants must also be informed of the possibility of filing criminal complaints*," D. He, "Governing Hate Content Online: How the Rechtsstaat Shaped the Policy Discourse on the NetzDG in Germany," *International Journal of Communication*, June 29, 2020, vol. 14, no. 0, p. 34. See new Section 3 of the NetzDG.

provide information on users.[276] Unfortunately, neither article establishes a specific deadline for an answer, although this is a major challenge.[277] Additionally, these orders must be specific regarding the content. In contrast, the CJEU case law considered that "*an injunction which is intended to bring an end to an illegal act […] must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal*."[278] This was criticized as extending injunctions to a gray zone,[279] but these texts are "*without prejudice to national civil and criminal procedural law*."[280] This has led to the multiplication of possible ways for cooperation between states and digital actors while limiting the harmonization of procedures. Second, the Digital Services Act creates a new obligation for providers of hosting services to notify law enforcement authorities[281] of their suspicions[282] regarding the past, future, or likely future commission of a criminal offense "*involving a threat to the life or safety of a person or persons*,"[283] which will concern only "*the most blatant illegalities*."[284] This notification should include the offense of human trafficking, as it involves a threat to both the life and safety of victims. However, content linked to human trafficking might not be explicit regarding these threats; therefore, it could have been useful to create a list of harmonized offenses under EU law for which notification is mandatory. Setting aside these limits, cooperation is thus bidirectional and facilitated. Cooperative measures are reinforced by the obligation to designate a point of contact and a legal representative

[276] Article 9 of the Digital Services Act. The article details, in particular, the content of those orders, their territorial scope, and the notification to the affected user. The article only concerns information already collected by the digital actor.
[277] S. Merabet, "Le Digital Services Act (2)," *op. cit.* note 262, ¶ 5. As the author underlines, other texts already set specific delays, such as the Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, Article 3 (1 hour). However, those are orders of removal, while the Digital Services Act leaves a margin of appreciation on the effect to give to the orders. The NetzDG only sets delays to take action upon a user's notice, Section 3.
[278] CJEU, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, October 3, 2019, C-18/18, ¶ 41
[279] P. Auriel, "La liberté d'expression et la modération des réseaux sociaux," *op. cit.* note 204, p. 419
[280] Article 9.6 and 10.6 of the Digital Services Act
[281] The law enforcement authorities are those of the concerned state, which is where the offense is supposed to have been committed or is supposed to be committed, or where the offender or victim is residing or is located. If not determinable, the digital actors will inform the state of its establishment or location of a legal representative and/or Europol, Article 18.2 of the Digital Services Act.
[282] Due to their own initiatives of moderation or following a user's notice of potential illegal content.
[283] Article 18.1 of the Digital Services Act
[284] S. Merabet, "Le Digital Services Act (2)," *op. cit.* note 262, ¶ 5

when digital actors are not established in the EU.[285]

517. Algorithms transparency. Finally, the Digital Services Act provides specific transparency obligations regarding the use of automated means of moderation.[286] Even so, these obligations are limited to specific digital actors and particular automated systems. Therefore, by adopting a "*transversal approach*,"[287] the Proposal for an Artificial Intelligence Act adds obligations for providers of artificial intelligence systems,[288] including for some related to the repression of human trafficking.[289] These obligations focus on providers of high-risk artificial intelligence systems.[290] In particular, vigilance obligations are expected *ex ante*, through the establishment of a risk-management system, including assessing risks, especially to vulnerable groups of people, which could include trafficked victims;[291] ensuring their elimination or mitigation;[292] ensuring a quality management system;[293] and *ex post*, through the creation of a post-market monitoring system.[294] This vigilance must apply to "*training,*

[285] Articles 11 and 13 of the Digital Services Act. Those obligations were already considered by the NetzDG, Section 5. It allows for direct litigation against a European entity.

[286] They all must include data regarding "*any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied*," Article 15.1.e of the Digital Services Act. Additionally, hosting services must publish "*the number of notices processed by using automated means*," Article 15.1. Very large online platforms must detail "*the indicators of accuracy and related information [on the use of automated means] broken down by each official language of the Member States*," Article 42.2.c. The latter category also must assess risks linked to their algorithmic systems, in particular with regard to the right to non-discrimination, Article 34.1.b. However, the text does not explicitly provide that digital actors' automated means should "*not produce discriminatory or unjustified results*," despite the recommendation of the European Data Protection Supervisor, "Opinion 1/2021 on the Proposal for a Digital Services Act," EU, February 10, 2021, ¶ 56.

[287] C. Castets-Renard, "Quelle politique européenne de l'intelligence artificielle ?," *op. cit.* note 197, p. 299

[288] However, obligations are criticized for not being harmonized with those derived from the GDPR and the Digital Services Act, A. Bogucki et al., *The AI Act and emerging EU digital acquis*, *op. cit.* note 227, pp. 6-11

[289] However, it does not go as far as the Digital Services Act as it lacks a "*participatory dimension*," A. Mantelero, *Beyond Data*, *op. cit.* note 218, p. 173

[290] This has been criticized: first, as it creates a "*critical barrier between high risk and lower risk*," *Ibid.* p. 170; and second, as "*a more nuanced approach is required, given the part played by providers and users in the development, deployment and use of AI applications, and the potential impacts of each stage on human rights and freedoms*," *Ibid.* p. 175

[291] Article 9.8 of the Proposal for an Artificial Intelligence Act

[292] Article 9 of the Proposal for an Artificial Intelligence Act. However, "*The Proposal fails to explain how and on the basis of which parameters, and method of evaluation, these risks should be assessed in relation to specific AI applications*," and it fails to define the notion of acceptable risk that may remain. In particular, this concept does not seem adapted as it "*comes from product safety regulation, while in the field of fundamental rights the main risk factor is proportionality*," A. Mantelero, *Beyond Data*, *op. cit.* note 218, pp. 171-172; J.M. Muñoz Vela, *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas*, *op. cit.* note 218, chap. 5

[293] Article 17 of the Proposal for an Artificial Intelligence Act

[294] Article 61 of the Proposal for an Artificial Intelligence Act

validation, and testing data sets,"[295] and it is supported by traceability obligations through record-keeping[296] and by human oversight obligations "*as proportionate to the risks associated with those systems*."[297] The proposal also adds basic provisions for transparency, including technical documentation[298] and the provision of detailed information "*to enable providers and users to reasonably understand the system's functioning*."[299] However, it should be underlined that the Council of the EU attempts to soften some due diligence obligations for artificial intelligence systems developed for and used by law enforcement authorities: Human oversight obligations have been reduced and they are exempt from registration on the EU database.[300]

518. The Brussels Effect: stringent regulations. The third criterion for the Brussels Effect is to adopt stringent regulations.[301] Bradford especially highlights a "*pro-regulation ideology*," built on a "*faith in government as opposed to markets to generate fair and efficient outcomes (ideology); and the relative importance of public regulation over private litigation and lower threshold for intervention by regulators in cases of uncertainty (process)*."[302] While corporate social responsibility is still becoming a stringent regulation in the EU, digital social responsibility obligations are even stronger. Provisions not only include stricter transparency reporting but also *ex ante* risk assessment and mitigation. However, stringent regulations might increase

[295] Article 10.1 of the Proposal for an Artificial Intelligence Act
[296] Article 12 of the Proposal for an Artificial Intelligence Act
[297] Article 14.1 of the Proposal for an Artificial Intelligence Act. However, the text "*should add 'relevant' or 'significant' [human oversight,] with greater detail as to what scope such supervision should have*," J.M. Muñoz Vela, *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas*, *op. cit.* note 218, chap. 5. The author also criticizes the fact that human oversight obligations are limited to high-risk artificial intelligence systems, as their absence in any of these might lead to high risks to fundamental rights.
[298] Article 11 of the Proposal for an Artificial Intelligence Act
[299] Article 13.1 of the Proposal for an Artificial Intelligence Act. However, it will be difficult to implement those norms on "*transparency and full explainability, especially in view of the complexity of some intelligent systems, and particularly those with self-learning capabilities, since it is possible that not even their designer or manufacturer may be able to explain them*," J.M. Muñoz Vela, *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas*, *op. cit.* note 218, chap. 5
[300] L. Bertuzzi, "EU Council nears common position on AI Act in semi-final text," *Euractiv*, October 19, 2022, online https://www.euractiv.com/section/digital/news/eu-council-nears-common-position-on-ai-act-in-semi-final-text/ (retrieved on October 25, 2022). See Council of the EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, December 6, 2022, 2021/0106(COD), Articles 14.5 and 51.1
[301] Indeed, "*changes in citizens' risk perception and decision makers' increased willingness to respond to mounting demands for more regulation […] caused the EU to eclipse the United States as the predominant global regulator*," A. Bradford, *The Brussels effect*, *op. cit.* note 194, p. 37
[302] *Ibid.* p. 38

costs[303] and deter innovation.[304] Still, these costs should not be new, as major private actors are already obligated under other social responsibility norms. The European digital social responsibility framework increases harmonization and avoids the multiplication of national frameworks. Furthermore, the risk approach and the pyramid of digital actors, setting aside the criticism they receive, allow for the avoidance of "one-size-fits-all" legislation and the adaptation of obligations.[305] Legal security and adaptability aim to facilitate innovation.[306]

519. Thanks to stringent obligations, digital social responsibility seems to be well adapted to improving coordination between European states and digital actors to globally repress cyber human trafficking. However, the study of the enforcement of these obligations is required.

II. Public sovereigns' control: ensuring cooperation

520. Self-enforcement. The first means of enforcement under the digital social responsibility framework is self-enforcement, meaning control procedures mandated by law but implemented by digital actors themselves. Under the Digital Services Act, very large online platforms must rely on independent (external) audits to control vigilance obligations at least once a year,[307] and they are required create an internal compliance officer function.[308] Similarly, the Proposal for an Artificial Intelligence Act mandates audits, through conformity assessments, for high-risk artificial intelligence systems.[309]. Nevertheless, external audits are usually limited to formal verifications

[303] Regarding costs linked to the NetzDG, some scholars argued that it would be an "*affordable burden*," especially since obligations are limited to the biggest digital actors, A. Rochefort, "Regulating Social Media Platforms," *op. cit.* note 208, p. 238; while other scholars considered "*that it puts considerable economic and administrative burdens on them*," F. Stjernfelt, A.M. Lauritzen, *Your post has been removed: tech giants and freedom of speech*, SpringerOpen, 2020, p. 179

[304] A. Bradford, *The Brussels effect*, *op. cit.* note 194, pp. 236-240

[305] Under the Digital Services Act, exceptions are provided for micro and small enterprises, for instance, Articles 19 and 29. Under the Proposal for an Artificial Intelligence Act, for instance, Article 55.

[306] Article 1.1 of the Digital Services Act. The Proposal for an Artificial Intelligence Act includes specific measures for innovation, Articles 53 and following.

[307] Article 37.1 of the Digital Services Act. However, it has been criticized for relying on private actors to audit digital actors, M.D. Cole, C. Etteldorf, C. Ullrich, *Updating the Rules for Online Content Dissemination*, *op. cit.* note 208, p. 201

[308] Article 41 of the Digital Services Act

[309] Article 43 of the Proposal for an Artificial Intelligence Act. This article has been criticized for lacking the ability to adapt the process to the different sectors of high-risk artificial intelligence systems and to define precisely its scope, J. Mökander et al., "Conformity Assessments and Post-market Monitoring," *op. cit.* note 216, p. 251

and have limited impact, while internal audits increase the risk of collusion.[310] Even with a rigorous monitoring system, an audit may not "*be the most appropriate method of collecting, let alone communicating, up-to-date information about factory [or transparency or moderation] conditions*."[311] While self-enforcement processes might be a first step, they rely on business relationships between private actors and do not support coordination with public sovereigns. New ways of enforcement should complement self-enforcement, to ensure coordination in anti-trafficking actions.

521. Enforcing responsibility. The enforcement of the Digital Services Act will be implemented by the national Digital Services Coordinators[312] and the Commission for very large online platforms.[313] In general, the text provides for specific powers of investigation to enforce the act[314] and raises the potential fines to 6% of the total worldwide annual turnover in the preceding financial year[315] of the digital actors,[316] which is seen as appropriate to incentivize digital actors to voluntarily comply with the text.[317] Similarly, the Proposal for an Artificial Intelligence Act provides for market

[310] *Ibid.* p. 250. In particular, the effectiveness of the conformity assessment (and declaration of conformity, Article 48) in the Proposal for an Artificial Intelligence Act is questioned as it will be implemented by the provider of the system. One solution would be, as in the Digital Services Act, to require independent audits, *Ibid.* p. 262

[311] R.M. Locke, *The Promise and limits of private power*, *op. cit.* note 8, p. 60

[312] Article 49 of the Digital Services Act. This national distribution of the procedures might nevertheless lead to "*fragment[ing] the national regulatory landscape*," B. Wagner, "A first impression of regulatory powers in the Digital Services Act," *op. cit.* note 240, especially since the illegality of the content depends on national laws, A. Joux, *DMA, DSA*, *op. cit.* note 203. Despite the harmonization of the definition of human trafficking, national transpositions produced similar but still different offenses that are interpreted differently. This fragmentation of the procedures could also derive from the participation of sectorial authorities that might also be designated as competent, S. Merabet, "Le Digital Service Act (1)," *op. cit.* note 232, ¶ 14. However, the designation of an authority to supervise the enforcement of the text could be seen as an improvement compared to the NetzDG, which only considered administrative offenses for systematic failures, M. Cornils, *Designing platform governance*, *op. cit.* note 241, p. 51. Nevertheless, the 2021 reform increased "*proactive compliance monitoring*" procedures, R. Griffin, *New School Speech Regulation and Online Hate Speech*, *op. cit.* note 240, p. 18. Moreover, those penalties are to be implemented by the Federal Office of Justice, which reports directly to the Ministry of Justice, "*making it by no means politically independent*," W. Schulz, *Regulating Intermediaries to Protect Privacy Online*, *op. cit.* note 275, p. 10. On the contrary, the Digital Services Act sets specific requirements for the Coordinators' independence, Article 50.

[313] Article 65 of the Digital Services Act. This centralization of enforcement derives from the experience of the enforcement of the GDPR, which resulted in the multiplication of procedures among very few member states coordinators, B. Wagner, "A first impression of regulatory powers in the Digital Services Act," *op. cit.* note 240

[314] Articles 51 and 66 to 69 of the Digital Services Act

[315] Compared to a maximum of four percent under the GPDR, Article 83.

[316] Articles 52 and 65 of the Digital Services Act. Other measures, such as the restriction of the service, only apply in restrictive circumstances, Article 51.3.b. However, this measure might be used if the provider of an intermediary service does not comply with the actions needed to avoid the infringement and the latter "*entails a criminal offense involving a threat to the life or safety of persons*," which would be the case with human trafficking.

[317] However, expensive fines have been criticized under the NetzDG as an incentive to overblock content, K. Kaesling, "Privatising Law Enforcement in Social Networks: A Comparative Model Analysis,"

surveillance by national supervisory authorities[318] and sanctions, including fines for up to 2%, 4%, or 7% percent of the total worldwide annual turnover in the preceding financial year of the digital actor, depending on the violated obligation.[319]. The application of these sanctions remains to be seen.[320] These fines sanction nonconformity with the transparency and vigilance frameworks, but there is still no liability for human rights violations or the facilitation of criminal processes, such as human trafficking.

522. Setting liability frameworks. The Digital Services Act only slightly modifies the liability framework for digital actors, as established originally in the E-Commerce Directive.[321] Hosting service providers still will not be liable for illegal content that they did not know they hosted or, when they knew it, if they acted "*expeditiously to remove or to disable access to the illegal content*."[322] The text complements this provision by creating a "*Good Samaritan rule, whereby providers who carry out self-initiated investigations in order to detect and remove illegal content will not lose their liability exemption for this reason alone*."[323] This action seeks "*to eliminate existing disincentives towards voluntary own investigations undertaken by*" digital actors,[324] for instance, to moderate content that might be linked to human trafficking. Nevertheless,

---

Erasmus Law Review, March 20, 2019, vol. 11, no. 3, p. 161; M. Bassini, "Fundamental rights and private enforcement in the digital age," *European Law Journal*, March 2019, vol. 25, no. 2, p. 194; D. Leisegang, "No country for free speech?: An old libel law and a new one aimed at social media are two threats to free expression in Germany," *Index on Censorship*, SAGE Publications Ltd, July 1, 2017, vol. 46, no. 2, pp. 76-77

[318] Articles 63 to 68 of the Proposal for an Artificial Intelligence Act. However, the European Parliament added the requirement that those authorities should be independent, as for the Digital Services Coordinators, see Article 59.4a of the Proposal. Further, it also requested the European Artificial Intelligence Office to be independent, Articles 56.1. This lack of independence in the Commission version was criticized by the doctrine, J. Mökander et al., "Conformity Assessments and Post-market Monitoring," *op. cit.* note 216, p. 253. Its tasks have been widely extended by the European Parliament, Article 56 b, to reduce the risk of "*significant divergences*" due to "*the lack of a unified ecosystem of enforcement*," A. Bogucki et al., *The AI Act and emerging EU digital acquis*, *op. cit.* note 227, p. 27

[319] Article 71.3 to 5 of the Proposal for an Artificial Intelligence Act. However, national regulations still obtain a wide margin of appreciation for the implementation of penalties, Article 71.7.

[320] For instance, under the NetzDG, no fine had been issued until April 2018, W. Schulz, *Regulating Intermediaries to Protect Privacy Online*, *op. cit.* note 275, p. 7. Though, in 2019, the Office fined Facebook €2 million for "*the underreported number of complaints*" in its transparency report, J. Park, *The public-private partnerships' impact on transparency*, *op. cit.* note 262, p. 44

[321] The liability framework of the E-Commerce Directive has been deleted in favor of the version adopted under the Digital Services Act, Article 89 of the latter.

[322] Article 6 of the Digital Services Act

[323] C. Busch, "Regulating the Expanding Content Moderation Universe," *op. cit.* note 206, p. 54, Article 7 of the Digital Services Act. However, this article is not to be included within the e-commerce directive, Article 89, which questions its scope of application.

[324] A. Kuczerawy, "The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act," *Verfassungsblog: On Matters Constitutional*, January 12, 2021, online https://verfassungsblog.de/good-samaritan-dsa/ (retrieved on May 27, 2021)

the applicability of this article does not fundamentally change the liability framework;[325] warnings were issued that it might lead only to "*incentivize the over-removal of hosted content*."[326] Similarly, the Proposal for an Artificial Intelligence Act "*does not deal with liability arising from damage caused by the infringement of its provisions*,"[327] such as a violation of human rights—non-discrimination, or freedom of expression—linked to the use of artificial intelligence systems to repress combat cyber human trafficking.[328] Thus, these harms "*will be governed by national law, something which will lead to fragmentation*."[329]

523. The Brussels Effect: regulatory capacity. Finally, the Brussels Effect requires the entity regulating digital social responsibility to "*commit to building institutions and vesting them with regulatory capacity to translate its market power into tangible regulatory influence*."[330] While both the Digital Services Act and the Proposal for an Artificial Intelligence Act establish stringent penalties for non-compliance, monitoring is primarily limited to auditing procedures. Furthermore, the power of the European regulations seems to be questioned by their application by national

[325] Scholars even considered that its introduction was in contradiction with the original European framework, leading "to increase legal uncertainty regarding the liability exemption for hosting service providers," M. Peguera, "The Platform Neutrality Conundrum and the Digital Services Act," *International Review of Intellectual Property and Competition Law*, May 1, 2022, vol. 53, no. 5, p. 683

[326] J. Barata, "Obligations, Liabilities and Safeguards in Content Moderation," *op. cit.* note 211. In particular, since "*any errors or omissions made by the platforms in the performance of this task do not imply their liability*," J. Barata i Mir, "Libertad de expresión, regulación y moderación privada de contenidos," *Teoría y derecho: revista de pensamiento jurídico*, Tirant lo Blanch, 2022, no. 32, pp. 98-99. Moreover, since it allows voluntary investigations without *per se* creating knowledge, it might support the online "*endemic monitoring of individuals' behaviour*," European Data Protection Supervisor, *Opinion 1/2021*, *op. cit.* note 286, ¶ 53

[327] M. Martín-Casals, "An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems," *op. cit.* note 222, p. 6

[328] Here should be underlined the European Parliament, "Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence," EU, October 20, 2020, P9_TA(2020)0276. This text is based on a strict liability for operators of high-risk artificial intelligence systems and a fault-based liability for operators of other artificial intelligence systems. However, this text was not included in the Proposal for an Artificial Intelligence Act. Liability for harm due to defective products is harmonized by Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products and applies to artificial intelligence systems. But the text is inadapted since it is limited to specific cases (a product not providing "*the safety which a person is entitled to expect limited harms*," Article 6) and harms ("*damage caused by death or by personal injuries; […] or destruction of any item of property*," Article 9), M. Martín-Casals, "An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems," *op. cit.* note 222, pp. 11-21. On this topic, see also European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), September 28, 2022, COM(2022) 496 final, that aims at facilitating the disclosure of evidence and setting presumption of non-compliance.

[329] M. Martín-Casals, "An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems," *op. cit.* note 222, p. 21

[330] A. Bradford, *The Brussels effect*, *op. cit.* note 194, p. 30

supervisory authorities. On the contrary, Bradford highlights the "*extensive sanctioning authority*" of the Commission as "*an effective deterrent*,"[331] which might be developed under the Digital Services Act.

524. Conclusion of the section. Digital social responsibility, as developed by the EU, offers new tools to strengthen coordination between digital actors and states, which is applicable to the repression of cyber human trafficking, although it is not dedicated to this topic. While regular compliance frameworks continue to face challenges in their comprehensive implementation, digital social responsibility produces more stringent obligations, including requirements for cooperation. Their potential Brussels Effect contributes to protecting the independence of EU sovereignties by reasserting a model of control that is not based on criminal liability. This effect is particularly relevant, as the Digital Services Act and the Proposal for an Artificial Intelligence Act rely on market criteria to be applicable, instead of the artificial legal requirement of establishment, which is blind to economic realities. However, the protection of European sovereignties through harmonization is still restricted by through reliance on national definitions of "illegal content." Human trafficking, although harmonized, does not benefit from an equal definition in all member states. Moreover, the major deficiency of these texts is the lack of liability for harms deriving from nonconformity, such as the facilitation of human trafficking or the violation of human rights in the use of artificial intelligence systems to repress trafficking. Even so, liability traditionally seeks to reassert coercion rather than to facilitate coordination and the protection of values derived from the rule of law. Compliance systems develop other legal obligations and relationships between digital actors and states to improve their coordination in the repression of cyber human trafficking.

525. Conclusion of the chapter. The repression of cyber human trafficking exemplifies the new powers of coercion of digital actors that, from a pragmatic perspective, develop both internal and external sovereignty. New ways of ordering control between sovereigns arise. Traditional control through criminal liability and newer extralegal means of control through extended criminal policies tend to reduce the independence of all sovereigns while reasserting the imperialistic powers of the United States. Therefore, other legal tools can order control between sovereigns. In

[331] *Ibid.* p. 34

particular, corporate social responsibility is relevant to coordinate the actions of digital actors with values protected by states and the EU, including the repression of human trafficking and the violations of human rights linked to the process and pre-existing it. These systems are designed to leverage private actors "*for public purposes*,"[332] especially to prevent human trafficking in some countries. However, corporate social responsibility frameworks continue to lack stringent obligations and have hardly adapted to the realities of cyber human trafficking. Nonetheless, they establish general standards for private actors to contribute to the protection of fundamental rights. Digital social responsibility, developed in the EU, manages to create stronger obligations, going further than reporting obligations that are designed to enhance the transparency of the actions of digital actors. While not drafted for the repression of human trafficking, they offer legal tools that are useful for better coordination between digital actors and member states, particularly by explicitly framing new ways of cooperation. Still, corporate social responsibility, including digital social responsibility, aims for coordination between states and private actors. Its main principles rely on transparency and monitoring processes, with few consequences for people. Protecting European values and states' independence does not rest only on improving coordination with digital actors. To effectively develop policies against cyber human trafficking that is respectful of fundamental rights, the direct relationships between digital actors and people, including trafficked victims, must be considered.

[332] F.W. Mayer, "Leveraging private governance for public purpose: business, civil society and the state in labour regulation," *in* A. Payne, N. Phillips (eds.), *Handbook of the International Political Economy of Governance*, Edward Elgar Publishing, 2014, pp. 354-355. However, corporate social responsibility is still developed within the framework of "*the neoliberal form of global economy*" and does not "*challenge the fundamental structures and beliefs of our politics and economy*," E. Kenway, *The truth about modern slavery*, *op. cit.* note 51, pp. 109-110. Similarly, policies to prevent climate change focus on sustainable development and are still framed in the neoliberal capitalistic economy, while other theories have come to question the paradigm of economic growth.

Chapter 2. Connecting sovereignties through legitimacy

526. Strengthening the state's hard sovereignty over digital actors questioned their independence. Subsequently, it questioned the legitimacy of sovereigns' actions in repressing human trafficking. Outside of criminal law, soft sovereignty offers other tools to coordinate the efforts of states and digital actors in the fight against cyber trafficking. The application of other legal disciplines highlights new grounds to legitimize these coordinated actions. In particular, European regulations improve the quality of the connection between digital actors and individuals, supporting a comprehensive legitimacy in repressing cyber trafficking (Section 1). This multifaceted fight recognizes the need to support multi-leveled connections for legitimacy. As a result, one element of sovereignty becomes prominent: independence. As the owners of coercion multiply, so do the sources of legitimacy. When the repression of cyber human trafficking underlines the need for a coordinated network, a new source of legitimacy appears: interdependence (Section 2).

Section 1. Legitimizing sovereignty: connecting digital actors to individuals

527. Digital actors' legitimacy to repress cyber trafficking. The coercion of digital actors' coercion relied on an empirical acknowledgment of their power, and this pragmatic sovereignty is useful to recognize their role in repressing cyber trafficking. However, the coercion of digital actors is explicitly backed by legitimacy only narrowly. Coming back to Weber's theory,[1] the coercion of digital actors could rely on their users believing in the validity of the contract accepted to use the service or other "*practical "'competence"*" derived from rules.[2] Under the legal theory, legitimacy was equated to the state's legal order.[3] Thus, it is limited to internal legitimacy, deriving from processes

[1] The coercion of digital actors could also rest in traditional legitimacy, although not legitimized by their spread through time but by their spread worldwide and their strong inclusion in daily individual habits, M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, tran. R. Livingstone, p. 34. It could further rest in charismatic legitimacy, due to the trust in certain "*leadership qualities*" of the company or its individual representation, *Ibid.*

[2] M. Weber, *The vocation lectures*, *op. cit.* note 1, p. 34, Weber gives the examples of "*the modern 'servant of the state' and all those agents of power who resemble him*." This could be connected to the concept of "*legitimacy by experience*" or "*legitimacy-utility*," developed by P. Rosanvallon, *La contre-démocratie: la politique à l'âge de la défiance*, Seuil, Les livres du nouveau monde, 2006, pp. 109-110

[3] See *supra* 103. On the difference between normative and sociological legitimacy, see also A.E. Buchanan, *The heart of human rights*, Oxford University Press, 2013, pp. 112-113

to adopt norms based on an understanding of democracy as the election of representatives to the people.[4] However, these processes are not equivalent between digital actors and their users.[5] Then, a new basis for their legitimacy, external to the state, should be identified. External sources of legitimacy are variable, but the repression of crimes is of public interest and legitimizes coercion; in particular, human trafficking receives an international consensus for its repression. Nonetheless, for a long time, repression was focused on a security approach, a criminal justice issue based on the prosecution of traffickers, and the control of borders. The current role of digital actors rests mainly on this approach:[6] The repression of human trafficking as a corporate policy has "*technologies of surveillance, carceral control, and market-based exploitation as their actual illicit underside*."[7] Even so, the global approach to trafficking evolved to include other external values: the protection of fundamental rights, particularly those of victims, and preventive actions to reduce the risks of trafficking. Fundamental rights are a counterweight to legitimizing sovereign actions.[8] However, "*a very small number of technology tools within partnerships focus on the empowerment of the victims of trafficking*."[9] Additionally, human rights are still based

[4] However, democracy as "*mere majoritarianism*" is criticized as too restrictive and leads to a vague definition such as "*democracy means that the people rule*," M.C. Nussbaum, *Creating Capabilities – The Human Development Approach*, Harvard University Press, 2013, p. 179

[5] "*Google dominates the World Wide Web. There was never an election to determine the Web's rulers*," S. Vaidhyanathan, *The googlization of everything: and why we should worry*, University of California Press, Updated edition, 2012, p. 13. As such, Thieulin argues that digital actors "*erode the traditional political leverage of our democratic societies*," B. Thieulin, "Gouverner à l'heure de la révolution des pouvoirs," *Pouvoirs*, January 11, 2018, vol. N° 164, no. 1, p. 24

[6] Their action aims to obtain evidence to secure convictions and to control their spaces to exclude content that might be linked to human trafficking. This approach is slightly different when digital actors are considered as companies that must prevent human trafficking processes in their value chains, but then the connection to cyber trafficking is less clear. Thus, their action "*supports and sometimes expands carceral agendas*." J. Musto, "The Limits and Possibilities of Data-Driven Anti-trafficking Efforts," *Georgia State University Law Review*, May 1, 2020, vol. 36, no. 4, p. 1166

[7] E. Bernstein, "Brokered Subjects and Sexual Investability," *in* P. Kotiswaran (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, p. 346

[8] S. Rodota, "Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives," *Mouvements*, La Découverte, June 8, 2010, vol. 62, no. 2, p. 57. Although, Guarnieri advocates that the balance between fundamental rights and technological opportunities might need to partly sacrifice the former, C. Guarnieri, "Agency for All, Privacy for None," *in* B. Herlo (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, p. 125

[9] UNODC, *Compendium on promising practices on Public-Private Partnerships to prevent and counter trafficking in persons*, UN, 2021, p. 104. When specific groups are protected, this assistance refers more to militarized humanitarianism, than a real implementation of human rights, E. Bernstein, "Militarized Humanitarianism Meets Carceral Feminism: The Politics of Sex, Rights, and Freedom in Contemporary Antitrafficking Campaigns," *Signs: Journal of Women in Culture and Society*, The University of Chicago Press, September 1, 2010, vol. 36, no. 1, pp. 45-71. It could similarly be criticized that state' protection is also limited. They are usually part of a strategy to secure a criminal procedure (conditions for protection) or aimed at supporting border control measures (measures of repatriation).

mainly on states' obligations, and they can be seen by digital actors as too vague for their implementation. New conceptual grounds for external legitimacy could be sought.

528. From human rights to capabilities to affordances. The theories on capabilities[10] appear as an alternative and complementary concept to human rights.[11] Indeed, capabilities "*specify a minimum threshold […] below which people cannot as a practical matter enjoy [their] civil and political rights*."[12] It requires the promotion of "*a set of opportunities or substantial freedoms which people then may or may not exercise in action: the choice is theirs*."[13] Despite the state—in particular, the judge—being at the core of the implementation of this theory,[14] this approach offers a new perspective for how digital actors could perform a comprehensive role in repressing human trafficking. The capabilities approach primarily emphasizes the role of combined capabilities: Opportunities are created "*by a combination of personal abilities and the political, social, and economic environment*."[15] External actors can nurture internal capabilities.[16] While Nussbaum's capabilities[17] are not linked to cyberspace, they might be realized in this context: Opportunities might be offered to users, including trafficked victims, to develop their online capabilities. This idea has been developed under the concept of affordances,[18] and state law is deficient if it does not affect the affordances

[10] These theories were developed as an alternative to indicators (such as the Gross Domestic Product) to measure well-being and development. For the various interpretations of the concept, see J.E. Cohen, "Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt," *Georgetown Law Faculty Publications and Other Works*, March 13, 2017, vol. 4, no. 1, p. 6

[11] In particular, since the concept of human rights has received many debates and interpretations, M.C. Nussbaum, *Women and human development: the capabilities approach*, Cambridge University Press, 2000, p. 97. From a pragmatic perspective, "*Fundamental rights are only words unless and until they are made real by government action*," M.C. Nussbaum, *Creating Capabilities*, *op. cit.* note 4, p. 65. Criticizing the usefulness of the concept of human rights for an online implementation, see R. Griffin, "Rethinking rights in social media governance: human rights, ideology and inequality," *European Law Open*, Cambridge University Press, March 2023, vol. 2, no. 1, pp. 30-56

[12] J.E. Cohen, "Affording Fundamental Rights," *op. cit.* note 10, p. 9

[13] M.C. Nussbaum, *Creating Capabilities*, *op. cit.* note 4, pp. 18-19

[14] *Ibid.* pp. 174-176. Both capabilities and human rights place "*great emphasis on the importance and the basic role of [the] spheres of ability*" of states to guarantee them, M.C. Nussbaum, *Women and human development*, *op. cit.* note 11, p. 100. On the contrary, Nussbaum criticizes the role of "*private philanthropy*" in securing capabilities, M.C. Nussbaum, *Creating Capabilities*, *op. cit.* note 4, pp. 119-121. She argues in favor of a decentralized institutional solution. However, she might seem to recognize various spheres of ability as she says that "*in the context of a nation, it then becomes the job of government to secure them if that government is to be even minimally just*," *Ibid.* p. 169

[15] M.C. Nussbaum, *Creating Capabilities*, *op. cit.* note 4, pp. 20-21

[16] *Ibid.* p. 23

[17] For the list, see M.C. Nussbaum, *Women and human development*, *op. cit.* note 11, pp. 78-80

[18] J.E. Cohen, "Affording Fundamental Rights," *op. cit.* note 10, p. 8. Also known as "*technological embeddedness*" of the professional community of digital actors, B. Wagner, *Global Free Expression - Governing the Boundaries of Internet Content*, Springer International Publishing, Law, Governance and Technology Series no. 28, 1st ed., 2016, p. 14

provided by digital actors.[19] By shaping online affordances, digital actors can create opportunities and protect trafficked victims.[20] These opportunities are "*what possibilities the users perceive the platform to have for various actions*."[21] Recognizing the role of affordances, it highlights "*technology as a range of techniques that structure and are structured by power and expertise*," since the material and technical parts are "*indelibly tied to discourses, institutions, and arrangements of power that authorize its development and use*."[22] However, it should be highlighted that, as with the law, "*users may also need to find creative ways to negotiate, or work around*"[23] these affordances, particularly to leverage opportunities or the lack thereof for the protection of potential or actual trafficked victims or the lack thereof, although they were not meant for this goal.

529. To look for a comprehensive legitimacy of digital actors' anti-trafficking actions, their role should be reinforced in the prevention of the phenomenon and the protection of its victims instead of focusing primarily on supporting the prosecution of traffickers and controlling the borders of cyberspace. The evolution of affordances, in connection with the evolution of state norms, can broaden the role of digital actors and

---

[19] B. Wagner, *Global Free Expression*, *op. cit.* note 18, p. 39; R. Badouard, "Ce que peut l'État face aux plateformes," *Pouvoirs*, April 27, 2021, vol. N° 177, no. 2, p. 51. On the necessity to change practices as a complement to legal amendments, see D. Salas, "« Et la nuit noire de l'esclavage tomba sur moi… » Réflexions conclusives," *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, p. 293

[20] Adapted from the statement "*by shaping our computing experience, Microsoft can shape much more*" of A.L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Century Foundation, May 15, 2000, p. 88

[21] K. Tiidenberg, E. van der Nagel, *Sex and social media*, 2020, p. 52. Various layers of code-based changes exist: "*at the root server level of the domain name system, at the application layer of [Transmission Control Protocol/Internet Protocol], on individual users' hard drives, or in the design of digital products*," S. Biegel, *Beyond our control? Confronting the limits of our legal system in the age of cyberspace*, MIT Press, 2001, p. 193. The affordances studied here particularly focus on modifications in the application layer providing for interfaces through certain functionalities and in the design of digital products or services. boyd theorized in particular four high-level affordances in online public sociality: persistence ("*Digital expressions are automatically recorded and archived*"); replicability ("*Digital content is easily duplicated*"); scalability ("*The potential visibility of digital content is great*"); and searchability ("*Digital content is often accessible through search engines*"), d. boyd, A. Marwick, "Social Steganography: Privacy in Networked Publics," *International Communication Association*, Boston, MA, May 28, 2011, pp. 9-10; d. boyd, "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life," *in* D. Buckingham (ed.), *Youth, Identity, and Digital Media*, MIT Press, The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, January 4, 2008, p. 126. High-level affordances are "*the kinds of dynamics and conditions enabled by technical devices, platforms and media*," and they are complemented by low-level affordances, "*typically located in the materiality of the medium, in specific features, buttons, screens and platforms*," T. Bucher, A. Helmond, "The Affordances of Social Media Platforms," *in* J. Burgess, A. Marwick (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, pp. 239-240

[22] J. Musto, M. Thakor, B. Gerasimov, "Editorial: Between Hope and Hype: Critical evaluations of technology's role in anti-trafficking," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 5

[23] K. Albury, "Sexual Expression in Social Media," *in* J. Burgess, A. Marwick (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 448

their legitimacy in repressing cyber trafficking.[24] The following study focuses on specific rights necessary for the protection of trafficked victims or for the prevention of trafficking and evaluates the role of digital actors in their implementation. However, victims' rights leave a very thin margin of action for digital actors (§1). These rights must be complemented by other frameworks not meant for trafficked victims but that could be useful for their protection and the prevention of further harm (§2).

§1. A limited connection to victims' human rights

530. Traditionally, trafficked persons' rights are linked to their victim status, in general, within a criminal procedure. Digital actors' role is limited due to a lack of consideration of the cyber components of the protection of victims (I). However, framing people as victims might not properly encompass the diversity of realities associated with trafficking processes and could result in limited comprehensive assistance (II).

I. Applying victims' rights to cyber trafficking contexts

531. Trafficked victims' rights. A victim of human trafficking is "*any natural person who is subject to trafficking*."[25] General measures of protection are slightly developed in anti-trafficking texts and barely recognize the role of new technologies to provide assistance.[26] The Council of Europe Convention on Action against Trafficking in Human Beings (the Warsaw Convention) highlights the protection of victims' private lives and personal data, which is not a specific right, as it derives from other frameworks.[27] Additionally, material assistance to victims is merely cited:[28] Thus, the texts do not mandate states to provide for accommodation, food, or means to connect

[24] It should be noted that part of strengthening the legitimacy of digital actors lies in the improvement of their transparency and on the process of adoption and modification of its contractual terms, Article 14 of the Digital Services Act; Article 3 of the Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, regarding this specific category of users; Article 6 of the Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, for distance contracts, in case of trader-consumer relationships (complemented by Articles 7 and 8 of the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services). However, these standards are not meant for the creation and implementation of specific rights and affordances for users.
[25] Article 4.e of the Warsaw Convention
[26] See, for instance, Articles 11 and 12 of Directive 2011/36/EU. Article 11.4.b only mentions the "*use of appropriate communication technologies*" to avoid "*visual contact between victims and defendants*."
[27] Article 11.1 of the Warsaw Convention, see *infra* 539 to 542.
[28] Article 12.1.a of the Warsaw Convention and Article 11.5 of the Directive 2011/36/EU

with their social network, to find a job, et cetera.[29] The latter could be sponsored by digital actors. Furthermore, trafficked victims benefit from specific rights: a reflection period and a right to a residence permit,[30] the latter of which is issued by the state. The start of the reflection period depends on the official identification as a trafficked victim, which mainly rests in the hands of the state's institutions. If this identification is extended to non-state actors, it is mainly to NGOs who are charged with the victim's protection.[31] Thus, digital actors' role is highly limited in implementing trafficked victims' special rights.

532. Victims' rights. The international framework defines a victim as a person "*who, individually or collectively, ha[s] suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws*."[32] The EU has adopted norms to harmonize victims' rights and compensation. However, the roles of digital actors, and of the private sector in general are limited as a result of framing these rights in relation to criminal procedure, which is at the apex of states' sovereignty. Regarding technologies, the texts focus mainly on videoconferencing[33] and on technology as a tool for raising awareness.[34] Thus, technology appears primarily as an optional service contracted by the state instead of a collaboration with actors developing these technologies.[35] Nonetheless, it should be mentioned that

---

[29] It could be mentioned that a study highlighted that access "*to a smartphone and data package helped survivors develop skills to assist them in their move toward independent living and an understanding of the systems and services in their environment*," A. Malpass et al., "Overcoming Digital Exclusion during the COVID-19 Pandemic: Impact of Mobile Technology for Survivors of Modern Slavery and Human Trafficking – A Mixed Method Study of Survivors and Support Service Provider Views," *Journal of Human Trafficking*, Routledge, March 29, 2022, vol. 0, no. 0, pp. 1-20

[30] Articles 13 and 14 of the Warsaw Convention and Articles 6 to 8 of the Council Directive 2004/81/EC of 29 April 2004 on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration who cooperate with the competent authorities.

[31] On identification of trafficked victims and national referral mechanisms, see *supra* 257 to 259.

[32] General Assembly, "Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power," UN, November 29, 1985, ¶ A, Annex, A/RES/40/34

[33] Articles 7.2, 17.1.b, 23.3.a and b and 26.2 of the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime; Article 9.a of the Council Directive 2004/80/EC of 29 April 2004 relating to compensation to crime victims

[34] Article 26.2 of Directive 2012/29/EU, European Commission, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on victims' rights (2020-2025)," EU, June 24, 2020, pp. 5-7, COM(2020) 258 final

[35] Article 8.4 of Directive 2012/29/EU highlights the possibility to set up and collaborate with the public and NGOs to support and assist victims. The role of the business sector is not mentioned. See also *Ibid.* pp. 19-20

protection orders "*include, among others, measures aimed at limiting personal or remote contacts between the protected person and the person causing danger, for example, by imposing certain conditions on such contacts or imposing restrictions on the contents of communications*."[36] Developing this possibility, the Spanish criminal code allows prohibitions to contact the victim "*by any means of communication or computerized or telematics means*."[37] The decision is directed at the offender, and the state is required to guarantee its application. Even so, the technical affordances to implement the decision in cyberspace rest in the hands of digital actors.

533. In the current order of coercion and sovereign competencies, the protection of trafficked victims is still linked primarily to the state as part of its criminal sovereignty. Consequently, digital actors barely receive attention as potential partners in supporting trafficked victims, but, their role should overcome the victim approach.

II. Overcoming the victim approach

534. Criticisms of the victim approach. The victim approach is necessary to offer specific protection to victims as part of a criminal procedure. However, this approach is not comprehensive and has been the focus of much criticism. From a legal perspective, victims' protection relies on various texts in Europe that lack adequate harmonization.[38] Additionally, protection through criminal law does not consider underlying human rights violations and vulnerabilities,[39] thus limiting a full human rights perspective.[40] This can lead to harmful results from protective measures.[41] From a

---

[36] ¶ 21 of the Preamble of the Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order

[37] Article 48.3 in relation to Article 57.1 of the Código penal. The case law applied it, for instance, to contact through Twitter, A. Rodríguez Álvarez, "Cinco preguntas y algunas respuestas sobre los tweets en el proceso penal," *in* F. Bueno de Mata, I. González Pulido (eds.), *Fodertics 7.0: estudios sobre derecho digital*, Comares, 2019, pp. 275-276. No similar precision is to be found in France, Article 132-45.13° of the Code pénal.

[38] K. Plouffe-Malette, *La protection des victimes de traite des êtres humains: approches internationales et européennes*, Bruylant, Mondialisation et droit international no. 25, 2013, p. 153

[39] P. Lloria García, *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*, Iustel, 1st ed., 2020, p. 29. In particular, the choice of trafficked victims to cooperate with law enforcement authorities to receive protection does not consider "*the desire to migrate, the dependence between the migrant and those who help them to come, the great vulnerability of migrants due to the irregularity of their situation […] and the implementation of control strategies in the destination country*," B. Lavaud-Legendre, "Introduction," *in* B. Lavaud-Legendre (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 9

[40] J.K. Lobasz, "Beyond Border Security: Feminist Approaches to Human Trafficking," *Security Studies*, Routledge, June 12, 2009, vol. 18, no. 2, p. 332

[41] This harm might be directed at presumed victims and also to criminal procedure principles. In particular, "*The gender perspective cannot be used as an excuse to justify the implementation of authoritarian systems that relax such guarantees to the point of undermining the principle of presumption*

sociological perspective, "*The term victim is often associated with weakness, passivity, and helpless persons who are in need of being rescued, and therefore many trafficking victims do not recognize themselves as victims*."[42] In the context of trafficking, the vulnerable victim is often pictured as a woman. Nonetheless, this is "*based on gender essentialism; that is, overgeneralized claims about women*," which then "*reinforces the depiction of women in the Third World as perpetually marginalized and underprivileged*," leading to support for "*remedies and responses from states that have little to do with promoting women's rights [through] protectionist, and even conservative, responses*."[43]

535. From trafficked victims to deserving victims. This restrictive perspective on the assistance of trafficked victims leads to practical limits in protecting them. The victim approach is framed by criminal procedure, which requires their identification by designated institutions that interpret the notion of trafficked victims. However, the variety of victims' situations is hardly recognized. Their specific protections, framed by migration law, are directed mainly to third-state nationals, particularly for a residence permit, excluding many EU citizens who are victims of trafficking "*from the special programs for trafficking victims*"[44] or from their formal regularization.[45] Moreover,

---

of innocence," P. Lloria García, "Algunas reflexiones sobre la perspectiva de género y el poder de castigar del Estado," *Estudios Penales y Criminológicos*, June 15, 2020, vol. 40, p. 351. A thin balance must be drawn between the requirements for a fair trial and the protection of victims, R. Serra Cristóbal, "Intimidad de la víctima en el proceso. Un ejemplo en la mujer víctima de la trata," *in* J. Boix Reig, Á. Jareño Leal (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, p. 354. This harm can also derive from the perspective of the anti-trafficking framework, which sees women and children as specifically vulnerable although "*they do not share the same needs*." This creates risks of "*infantilizing women and failing to afford children the recognition they need*," J. Turner, "Root Causes, Transnational Mobility and Formations of Patriarchy in the Sex Trafficking of Women," *in* M. Malloch, P. Rigby (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, p. 195. On the infantilizing of women victims, see in particular E. Durisin, E. van Der Meulen, "The Perfect Victim: 'Young girls', domestic trafficking, and anti-prostitution politics in Canada," *Anti-Trafficking Review*, April 29, 2021, no. 16, pp. 145-149

[42] C. Rijken, "Trafficking in persons A victim's perspective," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 240

[43] R. Kapur, "The Tragedy of Victimization Rhetoric: Resurrecting the 'Native' Subject in International/Post-Colonial Feminist Legal Politics," *Harvard Human Rights Journal*, 2002, vol. 15, no. 1, pp. 7-8. This is particularly relevant in the absence of "*distinction between forced and voluntary sex work, [where women are pictured] as helpless victims needing masculine/state supervision*," D. Otto, "Lost in translation: re-scripting the sexed subjects of international human rights law," *in* A. Orford (ed.), *International Law and its Others*, Cambridge University Press, 2006, p. 325. However, "*To view women as victims or sex workers […] does not offer a more nuanced discussion about how norms and discourses are inhabited, or answer the question as to what makes individuals both identify and resist certain subject positions*," R. Andrijasevic, *Migration, agency, and citizenship in sex trafficking*, Palgrave Macmillan, Migration, minorities and citizenship, 2010, p. 122

[44] C. Rijken, "Trafficking in persons A victim's perspective," *op. cit.* note 42, p. 239

[45] B. Lavaud-Legendre, "L'émergence d'un statut de traite des êtres humains en droit français," *in* B. Lavaud-Legendre (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*,

states' institutions, by identifying trafficked victims, are drawing the line between "eligible" and "non-eligible"[46] or "deserving" and "undeserving"[47] victims for protection. From a legal perspective, "*The use of a means relating to the use of force or a fraudulent element […] reduces the protection in the sense that a separation is made between the victims who deserve to be rescued—such as 'good' victims—and the 'bad' victims*."[48] From a practical perspective, in many cases, "*To stand any chance of being identified and assisted as a [trafficked victim] by the authorities, a migrant woman or girl working in the sex trade needs to demonstrate, first, that she did not choose or consent to work in prostitution, and, second, that she has undergone great physical suffering*."[49] This division is also highlighted in the application of the non-prosecution principle.[50] "Genuine" and "deserving" victims are still distinguished from "fraudulent" and "undeserving" ones to imprison some and grant protective status to others.[51]

536. From deserving victims to ideal victims. This victim approach based on a "deserving" criteria, which is derived from a "*managerial logic*" of justice to ensure the

---

ÉdKarthala, Hommes et sociétés, 2013, p. 116; Á. Lara Aguado, "Capítulo IV. Violencia contra la mujer extranjera y trata desde la perspectiva de género," *in* J.M. Gil Ruiz (ed.), *El convenio de Estambul: como marco de derecho antisubordiscriminatorio*, Dykinson, 2018, p. 115

[46] S. Copić, M. Simeunović-Patić, "Victims of Human Trafficking Meeting Victims' Needs?," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 281

[47] M. Jakšić, "Le mérite et le besoin," *Terrains travaux*, September 17, 2013, vol. 22, no. 1, p. 209

[48] K. Plouffe-Malette, *La protection des victimes de traite des êtres humains*, *op. cit.* note 38, p. 3

[49] J. O'Connell Davidson, "Will the Real Sex Slave Please Stand Up?," *Feminist Review*, SAGE Publications, August 1, 2006, vol. 83, no. 1, p. 14. For instance, in France, to receive refugee status, "*the figure of the victim can only appear 'true' if it can be shown to be forced from start to finish*," P. de Montvalon, "Sous condition « d'émancipation active » : le droit d'asile des prostituées nigérianes victimes de traite des êtres humains," *Droit et société*, August 27, 2018, vol. 99, no. 2, p. 386 ; or to receive the status of trafficked victim, M. Darley, "Le proxénétisme en procès, réaffirmation d'un ordre sexuel national," *Sexualité, savoirs et pouvoirs*, Les Presses de l'Université de Montréal, Universanté, 2019, p. 166. Thus, "*The status of victim does not exist per se, but is earned through a series of ordeals: possible arrest by the police, police custody, filing of a complaint or testimony, support from associations*," M. Jakšić, "« Tu peux être prostituée et victime de la traite »," *Plein droit*, March 18, 2013, vol. 96, no. 1, pp. 19-22. Some institutions request additional requirements that are not in the law, for instance, stopping sex work activity. See also B. Lavaud-Legendre, "L'émergence d'un statut de traite," *op. cit.* note 45, pp. 105-109. This division is also applied when requesting compensation through the state fund, M. Jakšić, N. Ragaru, "Réparer l'exploitation sexuelle. Le dispositif d'indemnisation des victimes de traite en France," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, p. 139

[50] This principle first requires the identification of the victim and the use of the human trafficking offense, R. Piotrowicz, L. Sorrentino, "The non-punishment provision with regard to victims of trafficking A human rights approach," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, pp. 177-178

[51] M. Malloch, "Criminalising Victims of Human Trafficking: State Responses and Punitive Practices," *in* M. Malloch, P. Rigby (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 184-185; M. Jakšić, "Figures de la victime de la traite des êtres humains : de la victime idéale à la victime coupable," *Cahiers internationaux de sociologie*, July 4, 2008, vol. n° 124, no. 1, p. 137; Á. Lara Aguado, "Capítulo IV," *op. cit.* note 45, p. 122

conviction of traffickers,[52] is complemented by the notion of the ideal victim. This term refers "*to the image of an individual affected by [trafficking] who is readily afforded victimhood status because of perceived adherence to certain socially constructed criteria. […] The ideal victim is often viewed as being female, vulnerable, and weak, while the ideal offender is often viewed as being male, big, and bad*."[53] However, this stereotypical approach to trafficked victims challenges the repression of trafficking[54] and reduces the self-identification of victims.[55] It guides the work of law enforcement authorities, leading to the identification of victims corresponding to this description, while failing to identify[56] or to not prosecute other victims.[57] This could partly explain the lack of priority to detect trafficked victims for forced labor,[58] along with, for instance, economic benefits deriving from cheap labor, particularly men.[59] It supports questioning the credibility of victims[60] and a relationship with law enforcement

---

[52] B. Lavaud-Legendre, "L'émergence d'un statut de traite," *op. cit.* note 45, p. 121

[53] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, *Applying gender-sensitive approaches in combating trafficking in human beings*, Occasional paper, no. 10, OSCE, 2021, p. 11, adapted from the concept of N. Christie, "The Ideal Victim," *in* E.A. Fattah (ed.), *From Crime Policy to Victim Policy: Reorienting the Justice System*, Palgrave Macmillan UK, 1986, pp. 17-30

[54] K. Kempadoo, "The Modern-Day White (Wo)Man's Burden: Trends in Anti-Trafficking and Anti-Slavery Campaigns," *Journal of Human Trafficking*, Routledge, January 2, 2015, vol. 1, no. 1, p. 12

[55] In particular due to a lack of consideration of the will to migration, N. Ragaru, "Du bon usage de la traite des êtres humains. Controverses autour d'un problème social et d'une qualification juridique," *Genèses*, Belin, 2007, vol. 2007/1, no. 66, p. 85; for instance, regarding transgender victims, A.E. Fehrenbacher et al., "Transgender People and Human Trafficking: Intersectional Exclusion of Transgender Migrants and People of Color from Anti-trafficking Protection in the United States," *Journal of Human Trafficking*, Routledge, March 14, 2020, vol. 6, no. 2, p. 188

[56] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, *Applying gender-sensitive approaches in combating trafficking*, *op. cit.* note 53, p. 33; J. Leser, *Feeling Blue: Affective Rationalities in Vice Squad Policing*, doctoral thesis, Universität Leipzig, 2019, pp. 48, 72; S. Machura et al., "Recognizing Modern Slavery," *Journal of Human Trafficking*, Routledge, July 3, 2019, vol. 5, no. 3, p. 211. For instance, in the United States, see J. Srikantiah, "Perfect victims and real survivors: the iconic victim in domestic human trafficking law," *Boston University Law Review*, 2007, vol. 87, no. 1, p. 188

[57] Accordingly, "*Many less-ideal victims find themselves blamed for their own victimization, stigmatized, and even ostracized*," C. Gregoriou, I.A. Ras, "Representations of Transnational Human Trafficking: A Critical Review," *in* C. Gregoriou (ed.), *Representations of Transnational Human Trafficking*, Springer International Publishing, 2018, p. 11. For instance, transgender victims are more prone to be detained, A.E. Fehrenbacher et al., "Transgender People and Human Trafficking," *op. cit.* note 55, p. 189

[58] J. Srikantiah, "Perfect victims and real survivors," *op. cit.* note 56, p. 161

[59] J. Trounson, J. Pfeifer, "The Human Trafficking of Men: The Forgotten Few," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 547-548; I.M. Barron, C. Frost, "Men, Boys, and LGBTQ: Invisible Victims of Human Trafficking," *in* L. Walker, G. Gaviria, K. Gopal (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 73-84; K. Kaye et al., "Neoliberal Vulnerability and the Vulnerability of Neoliberalism," *in* J. Jakobsen, E. Bernstein (eds.), *Paradoxes of Neoliberalism*, Routledge, 1st ed., December 7, 2021, p. 94

[60] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, *Applying gender-sensitive approaches in combating trafficking*, *op. cit.* note 53, p. 45

authorities and NGOs "*characterized by mutual distrust and hostility*."[61] These stereotypes are highly shared in communication campaigns and news reports,[62] underlying the role of digital actors in fostering awareness while avoiding the reliance on such a limited understanding of human trafficking.

537. Cyber trafficking requires protection for victims offline and online, but victim status is still linked to state criminal sovereignty. Thus, state law barely considers victims' capabilities in cyberspace or a collaboration with digital actors. However, repressing cyber trafficking requires new ways of providing assistance to trafficked victims and vulnerable people. Therefore, to strengthen the legitimacy of digital actors, new means of protection can be sought outside the criminal discipline.

§2. Connecting users' rights to the repression of cyber trafficking

538. When considering cyber human trafficking, victims are primarily users of digital actors' services. As such, they benefit from other rights that could be useful to protect them as victims or as vulnerable people. The role of digital actors in implementing these rights and contributing to the assistance provided to victims could offer a more comprehensive legitimacy for exercising coercion to repress human trafficking in

---

[61] M. Darley, "Le statut de la victime dans la lutte contre la traite des femmes," *Critique internationale*, 2006, vol. 30, no. 1, p. 116

[62] C. Gregoriou, I.A. Ras, "'Call for Purge on the People Traffickers': An Investigation into British Newspapers' Representation of Transnational Human Trafficking, 2000–2016," *in* C. Gregoriou (ed.), *Representations of Transnational Human Trafficking*, Springer International Publishing, 2018, pp. 25-59; S. Rodríguez-López, "(De)Constructing Stereotypes: Media Representations, Social Perceptions, and Legal Responses to Human Trafficking," *Journal of Human Trafficking*, Routledge, January 2, 2018, vol. 4, no. 1, pp. 61-72; A.L. Ruiz Herrera, S.M. Ruiz Guevara, E.J. López Cantero, "El papel de los medios de comunicación masiva en la comprensión del fenómeno de la trata de personas," *Revista Criminalidad*, August 30, 2018, vol. 60, no. 2, p. 31; V. Saiz-Echezarreta, M.-C. Alvarado, P. Gómez-Lorenzini, "Advocacy of trafficking campaigns: A controversy story," *Comunicar: Revista Científica de Comunicación y Educación*, April 1, 2018, vol. 26, no. 55, pp. 29-38; K. Sharapov, J. Mendel, "Trafficking in Human Beings: Made and Cut to Measure? Anti-trafficking Docufictions and the Production of Anti-trafficking Truths," *Cultural Sociology*, SAGE Publications, December 1, 2018, vol. 12, no. 4, p. 540; E. Acién González, "Mujeres migrantes nigerianas. La realidad frente al relato trafiquista," *in* N. Cordero Ramos, P. Zúñiga Cruz (eds.), *Trata de personas, género y migraciones en Andalucía (España), Costa Rica y Marruecos: retos y propuestas para la defensa y garantía de los derechos humanos*, Dykinson, 2019, p. 71; A.B. Puñal Rama, *La prostitución en el espejo de los medios: una análisis de ABC y El País entre 1977 y 2012*, Universidad de Málaga, Atenea : estudios de género no. 101, 2019; E. Krsmanović, "Mediated Representation of Human Trafficking: Issues, Context, and Consequence," *in* J. Winterdyk, J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, p. 869; E. Krsmanović, "Child Trafficking vs. Child Sexual Exploitation: Critical reflection on the UK media reports," *Anti-Trafficking Review*, April 29, 2021, no. 16, pp. 69-85; A. Forringer-Beal, "Why the 'Ideal Victim' Persists: Queering representations of victimhood in human trafficking discourse," *Anti-Trafficking Review*, September 27, 2022, no. 19, pp. 87-102; A. Sierra-Rodríguez, W. Arroyo-Machado, D. Barroso-Hurtado, "La trata de personas en Twitter: Finalidades, actores y temas en la escena hispanohablante," *Comunicar: Revista Científica de Comunicación y Educación*, 2022, vol. 30, no. 71, p. 89

general. These rights derive largely from EU regulations, first linked to data protection (A) and later developed further regarding content moderation (B).

I. Implementing the GDPR's rights to repress cyber trafficking

539. Affordances for trafficked victims: control over personal data. Data regulation is a core topic of digital sovereignty. From a capitalist perspective, data are assets that could be owned, although legal scholars question this qualification.[63] From a surveillance perspective, data are information to which access can be granted and that can be used for coercion.[64] This approach was particularly relevant to studying the division of coercion between states and digital actors in obtaining data for the prosecution of traffickers. Going a step further, the regulation of data can be understood from a human rights perspective, to rule the relationship between trafficked victims as users of cyberspace and digital actors. Access to and control over data can be useful to target traffickers, but this process could also offer new opportunities for protection and prevention. Personal data protection is usually framed through the right to privacy. However, as an affordance available to trafficked victims, it can contribute to the protection of various other fundamental rights, such as the right to health, particularly mental health; to non-discrimination; liberty and security; et cetera.[65] Within the EU, the GDPR establishes the rights linked to personal data protection. The regulation obviously was not meant for the protection of actual or potential trafficked victims. However, digital actors can support this aim through the implementation of these rights via online specific affordances.

540. The GDPR for trafficked victims. In general, the GDPR offers rights to users

---

[63] R.H. Weber, "Data Ownership in Platform Markets," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 147; C. Zolynski, "What Legal Framework for Data Ownership and Access? The French Digital Council's Opinion," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 163; G. Zarkadakis, "The Internet Is Dead: Long Live the Internet," *in* H. Werthner et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, p. 49. On the contrary, for an approach to data as a common good, see A. Garapon, J. Lassègue, *Justice digitale: révolution graphique et rupture anthropologique*, Presses universitaires de France, 1re édition, 2018, p. 86; or as part of the public domain, see J.E. Cohen, *Between truth and power: the legal constructions of informational capitalism*, Oxford University Press, 2019, pp. 51-52

[64] K. Irion, "Government Cloud Computing and National Data Sovereignty," *Policy & Internet*, 2012, vol. 4, no. 3-4, p. 62

[65] See *supra* 67 to 73.

ahead of those granted to the controller of their personal data,[66] meaning the digital actors. These rights might be limited to protect trafficked victims, first, due to the lack of digital literacy[67] and, second, due to the lack of impact on their relationship with the trafficker. Nonetheless, some rights might be of interest. First, the GDPR provides for a right to information[68] that requires the controller to identify themselves.[69] If a website is developed to support a trafficking process or a company involved in such a process—an employment agency or a mail-order bride company, for example—a user registering or providing data to this website should be informed about the entity processing their data. When that information is available, it would provide a starting point for a judicial action. Second, the right to access[70] could be used to obtain data retained and processed by the digital actor, even when these data are not accessible directly by the victim (for instance, an account created by the trafficker or if their phone is confiscated), as evidence against the trafficker, or to request websites to determine whether the trafficker published data linked to the victim. Furthermore, the right to access might be understood more broadly as a right to control who has access to one's data, including additional affordances such as the blocking of other users, for instance, a potential victim blocking a trafficker's account. Third, the right to data portability[71] allows one to request the transmission of data from one controller, such as a digital actor, to another, such as an NGO or law enforcement authorities. However, the right that offers the strongest control over data is the right to be forgotten.

541. The right to be forgotten for trafficked victims. The right to be forgotten, or the right to erasure,[72] might offer a revolutionary change for the online world and the real-life protection of actual or potential trafficked victims. Victims might want to erase data accessible to the trafficker, published by the trafficker or themselves for their

[66] Meaning the person that "*determines the purposes and means of the processing of personal data*," Article 4.7 of the GDPR
[67] Questioning the role of consent of trafficked victims in the transmission of their data highlighting its limits due to the lack of knowledge on the implementation of their rights, see M.J. Castaño Reyero et al., *Cultura de datos en la trata de seres humanos: informe técnico de investigación*, Universidad Pontificia Comillas, 1st edition, February 17, 2022, pp. 53-54
[68] Article 13 of the GDPR
[69] Similarly, for a distance contract, including a digital service, the trader must identify themselves, Article 6.1.b of the Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights. The Digital Services Act also requires the identification and traceability of traders, Article 30.
[70] Article 15 of the GDPR
[71] Article 20 of the GDPR
[72] Article 17 of the GDPR

exploitation, or published or owned by traffickers as a means of control,[73] et cetera. This right refers to the "*de-indexing of information on Internet search engines (virtual environment) or the request for deletion of information from the original sources (physical environment)*."[74] The former is a right to delist,[75] and the latter constitutes the strict right to be forgotten, including "*the right to oblivion (grounded in the right to privacy […], a right based on the individual's desire to hide certain information from the public eye) and the right to erasure (a more "mechanical" right, focused […] on the removal of passively disclosed data)*."[76] In the context of human trafficking, the right to erasure offers a positive understanding of oblivion, "*the capacity to forget that the individual develops because it is necessary. In this dimension, forgetting has a constructive, even restorative function*."[77] It can also be seen as a form of individual sovereignty by providing powers of coercion to an individual over digital actors.[78] Indeed, the erasure is mandatory when the processing was unlawful, as when the trafficker used the victim's data without their consent or when the victim withdraws their consent, for instance, once they leave the trafficking process or the exploitation.[79]

---

[73] For instance, the sharing of intimate pictures on a public website or to other specific people, also known as revenge porn, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, OSCE, May 2020, p. 20. This is meant as a means of public shaming, in particular by sharing the sexual characteristics of the exploitation, especially to threaten the rehabilitation of the victim, d. boyd et al., *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the US*, Microsoft Research Connections, December 2011, p. 9; or as a means to dehumanize and objectify the victim to prepare them for later exploitation, M. Graw Leary, "Fighting Fire with Fire: Technology in Child Sex Trafficking," *Duke Journal of Gender Law & Policy*, 2014, vol. 21, p. 313. For an example of a case including this means of control in Romania, see D.M. Hughes, "Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies," *SAGE Open*, December 18, 2014, vol. 4, no. 4, p. 4. However, the prevalence of this means of control is highly challenged by M. Ioannou, M. Oostinga, "An empirical framework of control methods of victims of human trafficking for sexual exploitation," *Global Crime*, January 2015, vol. 16, no. 1, p. 39, finding revenge porn in only 8% of cases of human trafficking for sexual exploitation.

[74] O.A. Mendoza Enríquez, "Derecho al olvido en la economía digital," *in* F. Bueno de Mata (ed.), *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*, Editorial Comares, 2017, p. 370

[75] Since the activity of a search engine was considered processing data by the CJEU, *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*, May 13, 2014, C-131/12, ¶ 41

[76] K. Garstka, D. Erdos, "Hiding in Plain Sight: Right to be Forgotten and Search Engines in the Context of International Data Protection Frameworks," *in* L. Belli, N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 130

[77] M. Boizard et al., *Le droit à l'oubli [Rapport de recherche]*, report, no. 11-25, Mission de recherche Droit et Justice, February 2015, p. 8, online https://halshs.archives-ouvertes.fr/halshs-01223778 (retrieved on May 17, 2021). The right to be forgotten can be seen as a "*method of repairing a harmful situation*," E. Cruysmans, "Oubli, anonymisation, déréférencement. Cachez-moi ces informations que je ne veux plus voir en ligne !," *Bulletin social et juridique*, 2018, vol. 617, no. 1, p. 7

[78] M. Boizard, "La tentation de nouveaux droits fondamentaux face à Internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique," *in* A. Blandin-Obernesser (ed.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, pp. 31-55

[79] Article 17.1.b and d of the GDPR

While the right to erasure already existed in the first text on personal data protection,[80] the Court of Justice, in *Google Spain*, established that the controller of the data must guarantee the "*full effect and that effective and complete protection of data subjects […] may actually be achieved*."[81] This decision has a practical impact:[82] Digital actors must offer new affordances to users, including trafficked victims, to erase or request the erasure of their data.

542. The right to be forgotten: scope. Nevertheless, the current framing of the right to be forgotten can raise questions about its adaptation to the protection of trafficked victims. First, its territorial application is of particular importance. Regarding illegal content, the European Commission has advocated for global erasure.[83] Various approaches are possible for the erasure: over all versions of a website, over all European national versions of a website, or based on the place from which the search is operated or the website is seen.[84] In 2019, the CJEU ruled in favor of a mandatory erasure on all European national versions of a website and an obligation to prevent the data's availability on other versions accessible from the EU territory.[85] However, national laws and jurisdictions can request worldwide erasure.[86] While such an erasure might affect foreign persons' rights (such as their freedom of expression)[87] or states' sovereignty,[88] trafficked victim's protection should be prioritized.[89] Second, the scope

[80] Article 12.b of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[81] CJEU, *Google Spain*, *op. cit.* note 75, ¶ 38

[82] J. Le Clainche, "CJUE : le droit à l'oubli n'est pas inconditionnel," *Revue Le Lamy Droit de l'immatériel*, August 1, 2014, no. 107, p. 112

[83] European Commission, "Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Illegal and Harmful Content on the Internet," EU, October 16, 1996, p. 14, COM(96)487 final

[84] B. Hardy, "Application dans l'espace de la directive 95/46/CE : la géographie du droit à l'oubli Commentaire de l'arrêt de la Cour de justice dans l'affaire Google Spain et Google (C-131/12)," *Revue trimestrielle de droit européen*, 2014, pp. 883-885

[85] F. Donnat, "Droit à l'oubli," *La semaine juridique édition générale*, LexisNexis, October 7, 2019, no. 41, p. 1818; CJEU, *Google LLC v. CNIL*, September 24, 2019, C-507/17

[86] H. Muir Watt, "La portée territoriale du droit au déréférencement : un exercice de proportionnalité dans l'espace," *Revue critique de droit international privé*, Dalloz, 2020, vol. 2020/2, no. 2, p. 340. However, this worldwide erasure that was requested by the French authority on data protection was later censored by the Conseil d'Etat due to the absence of an explicit balance between the right to privacy and the freedom of information, Conseil d'État, 10ème - 9ème chambres réunies, March 27, 2020, no. 399922, ¶ 10

[87] Conseil d'État (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 2, p. 176

[88] B.A.D. Chaffaut, "Droit au déréférencement : mise en œuvre et zones d'ombre," *Legipresse*, 2019, vol. N° 61, no. HS1, p. 19. This interference into foreign states' sovereignty raises particular attention for requests for erasure from non-democratic and authoritarian countries.

[89] Various criteria were set by the CJEU for this balance, such as "*the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having*

of this right questions its applicability to the automatic erasure of the republished same content. While states cannot order a general online monitoring to digital actors,[90] the CJEU validated orders to erase and prevent the publication of similar content as long as the order "*contains specific elements […] such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined, and equivalent content to that which was declared to be illegal*."[91] This might allow jurisdictions to order that trafficked victims' data must not be republished. Third, other questions are specific to the situation of trafficked victims. While the right to erasure might support their protection, it leads to the disappearance of potential proof. Accordingly, erasure should be balanced with a right to retention, leading to a right to temporarily limit access to data before their erasure and after they are provided as proof to law enforcement authorities. Additionally, the right to erasure is understood only as a remedy; it arises after the publication of the data. Even so, from a preventive perspective and supposing that traffickers might have offline data that cannot be erased, a right for victims to block in advance the publication of data could be considered. Aside from data protection, digital actors could then support the online protection of victims' lives.

543. Personal data protection rights can assist in the protection of trafficked victims through the affordances established by digital actors. However, these rights are hardly dynamic and refer to the person as a set of data instead of considering their digital life and relationships. A second regulation, the Digital Services Act, attempted to create further rights for users, which should be studied from a trafficked victim's perspective.

---

that information, an interest which may vary, in particular, according to the role played by the data subject in public life," CJEU, *Google Spain*, *op. cit.* note 75, ¶ 81; CJEU, *GC, AF, BH and ED v. CNIL*, September 24, 2019, C-136/17, ¶ 66, the accuracy of data, and "*a distinction must be drawn between factual assertions and value judgements*," CJEU, *TU and RE v. Google LLC*, December 8, 2022, C-460/20, ¶¶ 64, 66. The ECHR similarly sets criteria for the right to erasure when balanced with freedom of expression and information: contribution to a debate of public interest, whether the person concerned was known to the public, the subject of the article, the conduct of the person concerned with regard to the media, how the information was obtained and its veracity, the content, form, and consequences of the publication, and the severity of the measure imposed on the applicant, ECHR, *Hurbain v. Belgium*, June 22, 2021, no. 57292/16; É. Cruysmans, "Le droit à l'oubli devant la Cour européenne des droits de l'homme : l'intégration d'une composante temporelle dans un litige vie privée/liberté d'expression," *Revue trimestrielle des droits de l'Homme*, Anthemis, 2022, vol. 129, no. 1, p. 174

[90] Article 15.1 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, substituted by Article 8 of the Digital Services Act (see Article 89)

[91] CJEU, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, October 3, 2019, C-18/18, ¶ 45

II. Implementing the Digital Services Act's rights to repress cyber trafficking

544. The Digital Services Act for trafficked victims. The aim of the Digital Services Act is to establish "*harmonized rules for a safe, predictable, and trusted online environment […] in which fundamental rights […] are effectively protected*."[92] To achieve this aim, the Act is not directed to consumers only but to any recipient of an intermediary service, broadening the meaning of "*users*."[93] The Digital Services Act provides for increased regulation of the relationships between digital actors and their users,[94] and it requires the implementation of specific affordances for the application of certain rights. Although the Act considers only the online protection of minors,[95] other rights could be leveraged for the protection of trafficked victims. For instance, the Act regulates online interface design. While it prohibits only the manipulation or distortion of the users' ability to make a free and informed decision,[96] the Act could have gone further to protect victims by empowering their online affordances, such as through the obligation to limit discrimination derived from interface design or via the facilitation of the right to disconnect from specific online spaces. Furthermore, the Act provides for the possibility of deactivating recommender systems based on profiling;[97] these mechanisms usually lead to filter bubbles,[98] thereby limiting the experience of an online service to one that is similar to a previous experience. As such, a victim could be enclosed in a re-victimization bubble[99], by revealing content linked to their previous exploitation or by closely connecting them to actors in their trafficking process. Therefore, it is then of particular importance that a victim, even when blocking a

---

[92] Article 1.1 of the Digital Services Act

[93] Article 3.b and c of the Digital Services Act

[94] In general, communication is facilitated through the designation of a signal point of contact, Article 12 of the Digital Services Act; compliance is strengthened by the potential liability of the provider but also of their legal representative, whose designation is mandatory for providers without establishment in the Union, Article 13.

[95] Article 28 of the Digital Services Act

[96] Article 25 of the Digital Services Act

[97] Article 38 of the Digital Services Act. However, this obligation is only directed at very large online platforms and search engines.

[98] "*A filter bubble occurs when selective exposure is produced by the social network's own algorithms, which choose which users' content we will see first. This personal filtering is opaque and even the users aware of its existence cannot easily recalibrate*," P. Petricca, "Commercial Content Moderation: An opaque maze for freedom of expression and customers' opinions," *Rivista internazionale di Filosofia e Psicologia*, December 30, 2020, vol. 11, no. 3, p. 321. The concept was first coined and developed by the activist E. Pariser, *The filter bubble: how the new personalized web is changing what we read and how we think*, Penguin Books, 2014

[99] C. Chen, N. Dell, F. Roesner, "Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors," *Proceedings of the 28th USENIX Security Symposium*, Santa Clara, CA, USA, August 16, 2016, p. 94

trafficker's account, could request their extraction from this harmful online bubble. Digital actors could offer this option, in particular, after reporting content linked to a trafficking process.

545. Reporting illegal content. According to the Digital Services Act, providers of hosting services "*shall put mechanisms in place to allow any individual […] to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content*."[100] Through this mechanism, a trafficked victim could exercise their right to be forgotten, and any person could notify digital actors of content purportedly related to trafficking. This mechanism provides recipients with a substantial advantage: "*Compared to court proceedings, Internet service providers can operate quickly and flexibly, and the procedure is usually cost-effective or free*."[101] Nonetheless, these notices are not anonymous,[102] a circumstance that could restrain the will of people to flag this type of content, especially victims or "clients," who might not want to face a criminal procedure. The article provides the possibility of anonymous notification only in cases of sexual abuse and sexual exploitation of children and child pornography, thus allowing the notice of content potentially linked only to the trafficking of children for sexual exploitation. The text could have also referred to the anti-trafficking directive for anonymous notice. Despite this drawback, the text details the procedure for such a mechanism, strengthening communication and transparency during the process. Thus, it reinforces, by applying due process values, the legitimacy of digital actors in protecting victims and preventing trafficking. Furthermore, these values are also applied to online sanctions adopted against potential traffickers.

546. The Digital Services Act against traffickers. The notice of illegal or harmful content by the victims, by any person, or by a state's entity could lead a digital actor to act upon the accessibility of the presumed trafficker to their service, such as the suspension of their account. Instead of focusing on the control of victims for their protection, which could lead to collateral damage and re-victimization, a different focus

---

[100] Article 16.1 of the Digital Services Act

[101] P. Korpisaari, "From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act," *Journal of Media Law*, Routledge, November 24, 2022, vol. 0, no. 0, p. 22. Criticism arises as digital actors are seen as deciding on the legality of content, which should be the work of judges, see, for instance, J.J. Castelló Pastor, "El alertador fiable como notificador de contenido ¿ilícito? en la red," *in* A. Martínez Nadal, M.B. Aige Mut, J. Martí Miravalls (eds.), *Plataformas digitales: aspectos jurídicos*, Aranzadi, Estudios, 1st ed., 2021, p. 62; European Data Protection Supervisor, "Opinion 1/2021 on the Proposal for a Digital Services Act," EU, February 10, 2021, ¶ 14

[102] Article 16.2.c of the Digital Services Act

turns to the control of the potential perpetrator. Even so, this control should not be executed without consideration of the rule of law. In the implementation of these sanctions, the Digital Services Act requires digital actors to embed due process values[103] through notification, a statement of reasons[104] for the sanction, and the possibilities of redress, including "*internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress.*"[105] This means regulating and legitimizing the "*almost hegemonic powers*" of digital actors.[106] Going further, providers of online platforms have the obligation to sanction users who "*frequently provide manifestly illegal content*,"[107] which could be the case for the account of the trafficker constantly reported for grooming, sharing recruitment services linked to exploitation, or promoting trafficked victims' services. Here again, the procedure should follow the basic values of due process.

547. Conclusion of the section. Digital actors exercise coercion to contribute to the repression of human trafficking. Nevertheless, this interest rests mainly on a security approach based on support for prosecutions and control over content. However, comprehensively repressing trafficking requires adopting a human rights perspective. The online implementation of rights through affordances can lead to tools for both control and protection.[108] This dual approach is needed to legitimize the

---

[103] Although it should be noted that there are no strict deadlines for the decision on the complaint, criticized by the European Data Protection Supervisor, *Opinion 1/2021*, *op. cit.* note 101, ¶ 48

[104] While, on the contrary, up until now, "*Most platforms reserve great powers in their terms of service to remove content posted by users, stating that they may do it at their 'sole discretion' or 'belief' that it violates their policies*," T. Dias Oliva, "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression," *Human Rights Law Review*, December 9, 2020, vol. 20, no. 4, p. 612

[105] Article 17 of the Digital Services Act. The internal complaint-handling system is mandatory for providers of online platforms, and includes further requirements regarding delays and quality, in particular, to be handled "*in a timely, non-discriminatory, diligent and non-arbitrary manner*," Article 20. Meta had already created, for Facebook, an Oversight Board, before the adoption of the Digital Services Act. For an analysis of this new entity, see V. Ndior, "Le Conseil de surveillance de Facebook, « service après-vente » de la liberté d'expression ?," *Recueil Dalloz*, Dalloz, 2020, no. 26, p. 1474

[106] S. Merabet, "Le Digital Services Act : guide d'utilisation de lutte contre les contenus illicites," *La Semaine Juridique Edition Générale*, October 24, 2022, no. 42, ¶ 8. These mechanisms avoid fees, speed processes, and develop trust, R. Van Loo, "The Corporation as Courthouse," *Yale Journal on Regulation*, January 1, 2016, vol. 33, pp. 560-564. While these mechanisms also receive criticism, due to a lack of transparency and representation, or procedural inequality and discrimination, *Ibid.* pp. 578-582, the Digital Services Act is a first step towards better private dispute resolution. For a comprehensive list of characteristics to improve these mechanisms, see F. Martín Diz, "Planteamiento y estructura de soluciones extrajudiciales online de controversias y conflictos generados in Internet," *in* F. Bueno de Mata (ed.), *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*, Editorial Comares, 2017, pp. 666-668

[107] Article 23 of the Digital Services Act

[108] S. Howell, "Systemic Vulnerabilities on the Internet and the Exploitation of Women and Girls: Challenges and Prospects for Global Regulation," *in* H. Kury, S. Redo, E. Shea (eds.), *Women and*

actions of digital actors and should lie, in particular, on relationships with trafficked victims. However, criminal law barely recognizes a role for actors other than the state to protect victims. Stepping outside criminal law, digital actors offer new means of protection to victims as users. Through personal data protection, based on the GDPR, and rights linked to their online environment, based on the Digital Services Act, digital law establishes the foundation for a new layer of relationships between digital actors and potential or actual victims that are built on human rights and the rule of law. Thus, the capabilities of trafficked victims are founded on three levels. First, human rights provide general guidance; second, the law establishes specific rights meant for the protection of their personal data or for their control over cyberspace architecture; and third, the code implements the accessibility and applicability of these rights. The pragmatic legitimacy of a state's sovereignty now depends on their relationship with digital actors to obtain or apply means of coercion. The pragmatic legitimacy of digital actors' sovereignty similarly depends on the intermediation by state law of rights and goals of general interest to later transcribe them into online affordances. The interlinks of legitimization processes then question independence as a component of sovereignty.

Section 2. Rethinking sovereignty: interdependence as a component of legitimacy

548. In practice, digital actors exercise coercion like sovereigns do. However, this pragmatic sovereignty still lacks solid grounds to be fully legitimate. Increasing the digital actors' role in repressing cyber human trafficking highlights the interlinks in the implementation of rights and the rule of law between their powers and those of states. Therefore, one particular element of sovereignty is independence. From the theory to the daily practice of comprehensively repressing cyber human trafficking, the independence of sovereign entities arises as a limit to the implementation of human rights and the rule of law (§1). As a consequence, the legitimacy of sovereign actors seems to rely on a new standard relevant to strengthening the repression of cyber human trafficking: interdependence (§2).

Children as Victims and Offenders: Background, Prevention, Reintegration, Springer International Publishing, 2016, p. 592

§1. The limits of independent sovereignties to repress cyber trafficking

549. Independent sovereignty refers to the characteristic of traditional sovereigns, states, to exclude competing entities exercising powers of coercion.[109] From this perspective, "*Interdependence is the exact opposite of the principle of sovereignty*."[110] However, the origin of independence, particularly the public/private division, is highly criticized, leading to questions about its adequacy to legitimate sovereignty (I). Furthermore, independent sovereignties challenge the repression of cyber trafficking (II).

I. Delegitimizing independence: criticism of the public/private division

550. Legal public/private divisions. The independence theory of states relies mainly on the distinction between "the public" and "the private." This distinction establishes the scope of the powers of the sovereign, understood as a state, by excluding the public from the private or by justifying the interference of the public in the private. The public/private division has many applications. From the perspective of the legal discipline, its main application is the division between the public and private orders, "*often viewed as being fundamentally opposed poles of governance*."[111] This divides fields of law that purportedly do not involve the state and rely on private law[112] from those that purportedly involve the state and rely on public law.[113] Even so, non-state actors are also producing general norms that frame individual relationships. Legal scholars are then divided between soft law, supposedly designed as a means for

---

[109] J.L. Cohen, *Globalization and sovereignty: rethinking legality, legitimacy and constitutionalism*, Cambridge University Press, 2012, p. 27. However, some authors link independence to external sovereignty only, P. Mortier, *Les métamorphoses de la souveraineté*, Thesis, Université d'Angers, January 1, 2011, ¶ 212; O. Beaud, *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994, pp. 15-16. This perspective is logical in the traditional definition of sovereignty: states' relationships are always considered external.

[110] B. Badie, "D'une souveraineté fictive à une post-souveraineté incertaine," *Studia Diplomatica*, Egmont Institute, 2000, vol. 53, no. 5, p. 10

[111] L.A. Bygrave, *Internet governance by contract*, Oxford University Press, 1st ed., 2015, pp. 22-23

[112] Such as family law and labor law, fields that were, historically, not even regulated by the state. They are nowadays usually regulated and framed by the state, but it still relies on private norms, in particular the contract, for its daily implementation. Another distinction is made between individual private norms and general public law, M. Alcaraz Ramos, "Preguntas de la explosión tecnológica del conocimiento a la política democrática y al derecho," *in* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, p. 79

[113] Such as constitutional law, administrative law, and taxation law, fields that rely on a specific presupposition: the existence of states, H.F. Nissenbaum, *Privacy in context: technology, policy, and the integrity of social life*, Standford University Press, 2010, p. 90

private actors, and hard law, which is the traditional tool of the public state.[114] These divisions do or do not allow actors to perform in specific spheres, whether public or private.[115]

551. Pitfalls of the public/private spheres. According to Habermas, the public sphere is "*open to all*" and is the main space for the development of politics and the state.[116] Thus, any public space should, from this perspective, be politicized to be legitimate.[117] On the contrary, the private sphere is "*split into the sphere of private ownership in the economy and intimacy in the family*."[118] Supposedly, the private sphere is where "*the individual is most in control of [their] activities and communications*."[119] It is then closely linked to the implementation of privacy as a control over information to manage the private sphere and to exclude public interference.[120] Still, private, or closed, spaces, can also defend or implement public values[121] and justify the interference of the public sphere.[122] Exploitation in a private sphere, within an intimate relationship or in a workplace setting, leads to human rights violations and justifies the interference of public institutions. Similarly, public spaces

---

[114] G. Shaffer, M. Pollack, "Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance," *Boston College Law Review*, September 1, 2011, vol. 52, no. 4, p. 790. This dichotomist division has long been criticized, in particular with the evolution of legal ordering, O. Afori, "Online Rulers as Hybrid Bodies: The Case of Infringing Content Monitoring," *University of Pennsylvania Journal of Constitutional Law*, April 2021, vol. 23, no. 2, p. 378. It barely survives nowadays, as, for instance, private actors "*are increasingly involved in activities that since the emergence of the Westphalian international system gradually became the more or less exclusive domain of the nation state*," J.H. van Oosterhout, "The Role of Corporations in Shaping the Global Rules of the Game: In Search of New Foundations," *Business Ethics Quarterly*, April 2010, vol. 20, no. 2, p. 253. For instance, regarding defense and surveillance, C. Fuchs, "Social Media and the Public Sphere," *TripleC: Communication, Capitalism & Critique*, February 19, 2014, vol. 12, no. 1, pp. 83-84

[115] By contrast, Nissembaum distinguishes between private and public actors, so attention focuses on the barrier between private citizens and governments; between private and public realms, to guide the limits of the normative scope; and between private and public information, to divide private and public facts to guide legal and policy practice, H.F. Nissenbaum, *Privacy in context*, *op. cit.* note 113, pp. 91-96

[116] J. Habermas, *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*, MIT Press, Studies in contemporary German social thought, 1989, p. 1

[117] *Ibid.* p. 177

[118] C. Fuchs, "Social Media and the Public Sphere," *op. cit.* note 114, p. 60. Differently said, "*The term private signals the realms of the familial, the personal, or intimate relations, while the term public signals civic actions […] beyond the home and the personal*," H.F. Nissenbaum, *Privacy in context*, *op. cit.* note 113, p. 90

[119] C. Fuchs, "Towards an alternative concept of privacy," *Journal of Information, Communication and Ethics in Society*, Emerald Group Publishing Limited, January 1, 2011, vol. 9, no. 4, p. 221

[120] S. Rodota, "Nouvelles technologies et droits de l'homme," *op. cit.* note 8, pp. 65-66. Originally understood as the right to be let alone, S.D. Warren, L.D. Brandeis, "The Right to Privacy," *Harvard Law Review*, The Harvard Law Review Association, 1890, vol. 4, no. 5, pp. 193-220

[121] Thus, "*Labor and economic production, formerly part of private households, would have become public by being integrated into capitalist production*," C. Fuchs, "Towards an alternative concept of privacy," *op. cit.* note 119, p. 229

[122] A.M. Battesti, "La coopération des plateformes," *Legipresse*, 2019, vol. N° 61, no. HS1, p. 45

serve purposes other than politics, such as the development of social identities.[123] For instance, the criminal procedure and the identification of trafficked victims can contribute to the expansion or limitation of these victims' individual identities. Criticism of the public and private spheres has been fueled particularly fueled by feminist theories.[124] The existence of one public sphere and one political sphere will "*support structural relationships of power*" while traditionally refusing to regulate various private spheres in which oppression is exercised,[125] and the equality principle between independent public spheres "*overlooks the unequal power structures among states*."[126] Feminist theories questioned the meaning of the private sphere,[127] the distribution between spheres,[128] and the mere idea of their division, from which arose the famous saying:[129] "The personal is political." Private spheres can be a public, politicized sphere, in which coercion can be exercised and in which public values can be implemented.[130] These questionings led to the understanding that "*the public and private spheres, when they can be identified as such, exist not so much in opposition*

---

[123] N. Fraser, "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy," *in* C.J. Calhoun (ed.), *Habermas and the public sphere*, MIT Press, Studies in contemporary German social thought, Nachdr., 1993, pp. 109-142

[124] This approach had its own set of criticisms, in particular when questioning the public/private division "*when it is used in an essentialist manner and when it is conceptualized as a static concept*," D.E. Buss, "14. Going Global: Feminist Theory, International Law, and the Public/Private Divide," *in* S.B. Boyd (ed.), *Challenging the Public/Private Divide*, University of Toronto Press, January 31, 1997, p. 365

[125] *Ibid.* pp. 373-374. Traditionally, this divide led to a "*dichotomy between the public sphere of independence, considered the territory of men, and the private sphere of dependency management, considered the territory of nature and the natural domain of women*," B. Rodríguez Ruiz, "Hacia un Estado post-patriarcal. Feminismo y ciudadanía," *Revista de estudios políticos*, Centro de Estudios Políticos y Constitucionales (España), 2010, no. 149, p. 96

[126] D.E. Buss, "14. Going Global," *op. cit.* note 124, p. 375

[127] E. Beltrán, "Justicia, democracia y ciudadanía: las vías hacia la igualdad," *in* E. Beltrán, V. Maquieira (eds.), *Feminismos, debates teóricos contemporáneos*, Alianza Editorial, El Libro universitario no. 069, 2001, p. 205

[128] The public/private division can rest on various interpretations: "*First, a distinction is often drawn between state regulation (government activity) and private economic activity (the market) […] A second aspect of the public/private divide is a distinction drawn between the market and the family […] A third aspect of the public/private divide is the distinction between state regulation and family relations […] Finally, international law constructs a public world of interstate activity that is said to be separate from the 'private' world of domestic state affairs, a distinction analogous to that between state and family. At the international level, only relations between states, or issues that states have agreed to submit to regulation through international treaty or contract, are legitimate subjects for 'public' international legal regulation*," S.B. Boyd, "1. Challenging the Public/Private Divide: An Overview," *in* S.B. Boyd (ed.), *Challenging the Public/Private Divide*, University of Toronto Press, January 31, 1997, pp. 8-11

[129] V. Maquieira, "Genero, diferencia y desigualdad," *in* E. Beltrán, V. Maquieira (eds.), *Feminismos, debates teóricos contemporáneos*, Alianza Editorial, El Libro universitario no. 069, 2001, p. 154. This divide is even considered a "*myth*," since "*The state has traditionally interfered in women's decisions about their sexuality and reproductive health, but refrained from intervening in the family context*," S. De Vido, *Violence against women's health in international law*, *Violence against women's health in international law*, Manchester University Press, June 12, 2020, pp. 166-167

[130] C. Amorós Puente, "Conceptualizar es politizar," *Género, violencia y derecho*, Tirant lo Blanch, Alternativa, 2008, pp. 21-22

to one another, but rather in reciprocal connection with one another."[131]

552. The flagrant inadequacy of independence in cyberspace. Similarly to states, cyberspace, at its beginnings, was declared "*independent*," excluding the sovereignty of states.[132] Thus, a state-based criterion was translated into spaces managed by digital actors. However, facing the practical realities of cyberspace and the digitalization of society, the independence criteria, particularly in their interpretation of the divide between sovereign states and private actors such as digital actors, seem highly compromised. States rely on digital actors for the implementation of coercion.[133] In particular, the EU relies on a "*structural dependence of key corporate players on the clouds, software, and platform infrastructures in the hands of Big Tech*."[134] Nevertheless, private actors are not independent either;[135] they are framed by multiple states' regulations: Cyberspace "*is no legal* terra nullius."[136] Legitimacy based on values such as human rights and the rule of law are intermediated by EU norms, and states establish liability and accountability rules.[137] However, the public/private divide is still applied to regulate digital actors and cyberspace.[138] First seen as tools to

---

[131] S.B. Boyd, "1. Challenging the Public/Private Divide," *op. cit.* note 128, p. 13

[132] M. Mossé, "Le numérique et le retour de la souveraineté," *in* P. Türk, C. Vallar (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 55; J. Perry Barlow, "Déclaration d'indépendance du cyberespace," *in* O. Blondeau, F. Latrive (eds.), *Libres enfants du savoir numérique*, éd. de l'éclat, 2000, pp. 47-54

[133] J. Adams, M. Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies*, September 29, 2016, vol. 4, no. 6, p. 262; J. Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors," *University of Cincinnati Law Review*, January 1, 1997, vol. 66, p. 187

[134] D. Bassens, R. Hendrikse, "Asserting Europe's technological sovereignty amid American platform finance: Countering financial sector dependence on Big Tech?," *Political Geography*, August 1, 2022, vol. 97, p. 9; R. Avila Pinto, "Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies," *Sur - International Journal on Human Rights*, July 16, 2018, vol. 15, no. 27, p. 19; F. G'Sell, "Remarques sur les aspects juridiques de la « souveraineté numérique »," *La revue des juristes de Sciences Po*, 2020, no. 19, p. 52. That led the European Commission to emphasize independence as an aim of their strategy on digital sovereignty, A. Calderaro, S. Blumfelde, "Artificial intelligence and EU security: the false promise of digital sovereignty," *European Security*, Routledge, July 3, 2022, vol. 31, no. 3, p. 417

[135] Additionally, they are not independent from each other. There are many interlinks between digital actors and other sectors, such as Big Tech companies with the media or the financial sector, D. Bassens, R. Hendrikse, "Asserting Europe's technological sovereignty amid American platform finance," *op. cit.* note 134, p. 2, and "*a growing number of economic sectors […] increasingly and quickly dependent on dominant platforms*," B. Thieulin, *Towards a European digital sovereignty policy*, Opinion of the Economic, Social and Environmental Council, France, March 13, 2019, p. 10. These interlinks can then be regulated by state law, for instance, through competition law.

[136] M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020, pp. 4, 47

[137] H. Ruiz Fabri, "Droits de l'homme et souveraineté de l'État : les frontières ont-elles été substantiellement redéfinies ?," *in* Collectif (ed.), *Les droits individuels et le juge en Europe: mélanges en l'honneur de Michel Fromont*, Presses universitaires de Strasbourg, 2001, p. 398

[138] A.L. Shapiro, *The Control Revolution*, *op. cit.* note 20, pp. 153-157. Scholars multiply criteria to set the distinction: private spaces as closed spaces with limited access or visibility due to geographical of

privatize spaces, new technologies created an extension or new places for the private sphere, such as intimate connection. Still, the many uses of new technologies, their instrumentality, including to exercise coercion, quickly made them tools linked to the public sphere:[139] As they facilitate offenses, including human trafficking, the situation justifies public interference. Thus, cyberspace is a useful example of the fluidity of the public/private divide.[140]

553. Loosening privacy in the public/private distinction. While the public/private divide is fluid in cyberspace, it is at the core of the implementation of the right to privacy, establishing a limit that will legitimize, or not, the action of sovereigns.[141] This divide also defines limits on coercive powers in the anti-trafficking framework after balancing all human rights and public interests at stake. Privacy is usually linked to the private (invisible) sphere as opposed to the public (visible[142]) sphere.[143] However, when the quality of spheres depends on people's perception and interpretation and their technical affordances,[144] privacy increasingly "*amounts to an*

---

functional reasons (M.-C. Roques-Bonnet, *Le droit peut-il ignorer la révolution numérique*, Michalon Editions, 2010, pp. 425-426), private spaces as commercially owned (S. Myers West, "Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms," *New Media & Society*, SAGE Publications, November 1, 2018, vol. 20, no. 11, p. 4367), private spaces due to the number of speakers and recipients (J. Adams, M. Albakajai, "Cyberspace," *op. cit.* note 133, p. 260), users perception (H.L. Barakat, E.M. Redmiles, "Community Under Surveillance: Impacts of Marginalization on an Online Labor Forum," SocArXiv, September 24, 2021, p. 4 citing G. Eysenbach, J.E. Till, "Ethical issues in qualitative research on internet communities," *BMJ*, November 10, 2001, vol. 323, no. 7321, pp. 1102-1105), etc. On the contrary, cyber spaces are seen as public spheres when they are "*environments where people can gather publicly through mediating technology*," d. boyd, "Social Network Sites: Public, Private, or What?," *Knowledge Tree*, August 1, 2010, vol. 13, pp. 2-3. Thus, all cyber spaces may have the "*potential to be a public sphere and lifeworld of communicative action*," C. Fuchs, "Social Media and the Public Sphere," *op. cit.* note 114, p. 89

[139] D.J. Haraway, *Simians, cyborgs, and women: the reinvention of nature*, Routledge, 2015, pp. 168-169. Nowadays, it is even considered that cyberspace is "*Public by Default, Private Through Effort*," d. boyd, *It's complicated: the social lives of networked teens*, Yale University Press, 2014, p. 61

[140] This fluidity is visible in the case law of the ECHR. The notion of private life gets an increased interpretation, especially when related to cyber spaces and new technologies, including in the concept of private life, for instance, telephone calls and emails from business premises, ECHR, *Copland v. the United Kingdom*, April 3, 2007, no. 62617/00, ¶¶ 30, 41, 44; ECHR, *Bărbulescu v. Romania*, September 5, 2017, no. 61496/08, ¶ 72; personal data, ECHR, *S. and Marper v. the United Kingdom*, December 4, 2008, 30562/04 et 30566/04, ¶ 103

[141] "*First, privacy functions as a protective barrier between behavior and policy, and calls into play the private/public distinction defined as a line between private individuals and government actors. Second, regarding the line between the political and domestic or personal spaces or realms, privacy protects […] the sanctity of the latter. Third, the private/public distinction is applied to information; privacy is called into play as a protection against access to private information*," H.F. Nissenbaum, *Privacy in context*, *op. cit.* note 113, p. 92

[142] C. Fuchs, "Social Media and the Public Sphere," *op. cit.* note 114, p. 74

[143] P.-Y. Gautier, "La preuve hors la loi ou comment, grâce aux nouvelles technologies, progresse la 'vie privée' des salariés," *Recueil Dalloz*, Dalloz, 2001, p. 3148

[144] Especially their control over their own data, Y. Deswarte, S. Gambs, "Protection de la vie privée : principes et technologies," *in* T. Allard, D. Le Métayer (eds.), *Les technologies de l'information au service*

expression of individual sovereignty"[145] as well as a collective value, as a "*constitutive value of democracy [and a] basis for an inclusive and pluralistic public sphere*."[146] Even so, when the public/private division is fluid, privacy is loosened; its area of implementation becomes wider, but its implementation is even more challenging. For instance, public spheres might need privacy to protect certain values, such as the secrecy of investigations to secure the prosecution of traffickers. Rather than a theoretical concept, the public/private divide and the implementation of privacy are based on "*an ongoing process*" that "*requires the ability to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics*."[147] Once again, the independence of sovereigns as they develop rights and affordances seems more like a myth than a comprehensive theory to legitimize the exercise of coercion.

554. Sovereignty relies on independence, which derives from the division between public and private spheres and, thus, norms. However, this divide seems fluid, almost disappearing, especially in cyberspace. Going further, this criterion challenges a comprehensive repression of cyber trafficking.

II. Independence as an obstacle to repress cyber human trafficking

555. Individual sovereignty. Independence was traditionally applied to states as sovereigns. As digital actors can be deemed sovereigns today, they also develop their own independence, while states learn how to cooperate with these new actors, especially to repress cyber trafficking. Once both states and digital actors are situated in the public sphere, their powers of coercion are legitimate, but they are restricted once they relate to the private sphere of individuals. Indeed, especially in theorizing digital sovereignty, authors identify a third actor in the interlinks of coercion: the individual. Individual sovereignty is "*inspired by the principles of popular sovereignty, according to which citizens are the source of all power [and] it corresponds to the right*

des droits: opportunités, défis, limites, Bruylant, Cahiers du Centre de recherches Informatique et droit no. 32, 2010, pp. 111-112

[145] H.F. Nissenbaum, *Privacy in context*, *op. cit.* note 113, p. 75

[146] I. Turégano Mansilla, "La dimensión social de la privacidad en un entorno virtual," *in* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 37-41

[147] d. boyd, *It's complicated*, *op. cit.* note 139, p. 60

of individuals to self-determination."[148] Joost theorizes individual sovereignty through four pillars: freedom of choice ("*individuals should be at liberty to decide on their own whether to do or not to do something*"); self-determination[149] ("*individuals' ability to retain control over important decisions*"); self-control (individuals "*are able to set their own limits and be aware of the consequences of their behavior*"); and security ("*different measures need to be in place to protect [individuals], and they have to be initiated by the state, by corporations and service providers as well as by the [persons] themselves*").[150] However, the legal field is still unwilling to recognize individual sovereignty. Instead, people are given fundamental rights as a way to limit sovereigns' coercion. Nonetheless, rights are static; on the contrary, capabilities and affordances are dynamic.

556. Human trafficking processes trigger the public sphere. The state's elements are violated, and digital actors are part of the protection of the values violated by the offense. Therefore, the private sphere and individual sovereignty are supposedly removed to legitimize the full exercise of sovereigns' coercion. However, this binary opposition between sovereign and individual independence and the priority of the former over the latter challenge the comprehensive repression of trafficking (A). Furthermore, the notion of independence hides possibilities for collective action, particularly for prevention (B).

A. Independence of sovereigns versus agency of individuals

557. The anti-trafficking carceral approach. The repression of cyber trafficking can be deemed to rely on a carceral approach. Once the threat is actual or even

---

[148] P. Türk, "Définition et enjeux de la souveraineté numérique," *Cahiers français*, La documentation française, June 2020, no. 415, p. 24

[149] Inspired by the right to "informational self-determination," declared by the German Federal Constitutional Court in 1983, Bundesverfassungsgericht, December 15, 1983, 1 BvR 209, 269, 362, 420, 440, 484/83. The Spanish Tribunal Supremo also recognized a fundamental right to one's own virtual environment, primarily understood as a control over data and a protection of privacy, P. Arrabal Platero, "El derecho fundamental al propio entorno virtual y su incidencia en el proceso," *in* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 431-441, see in particular Tribunal Supremo. Sala Segunda, de lo Penal, de Abril de 2013, no. 342/2013. The concept was also developed and operationalized under the notion of "*digital self-determination*, "*defined as the principle of respecting, embedding, and enforcing people's and peoples' agency, rights, interests, preferences, and expectations throughout the digital data life cycle in a mutually beneficial manner for all parties involved*," S.G. Verhulst, "Operationalizing digital self-determination," *Data & Policy*, Cambridge University Press, January 2023, vol. 5, p. 6.

[150] G. Joost, "Out of Balance The Impact of Digitalization on Social Cohesion," *in* B. Herlo (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, pp. 96-98

potential, sovereigns—in particular especially the states, and, by influence, digital actors—aim "*to solve the problem of trafficking through juridical means and the threat of incarceration*," developing "*politics of incarceration that employs market-based and punitive solutions to enforce harsh criminal and economic penalties against traffickers through carceral paradigms of social justice*."[151] This approach is complemented by the rescue industry:[152] The private sphere is erased in favor of strongly coercive means of identification of potential victims and the application of specific models of assistance,[153] such as "rehabilitation." The limitations on sovereigns' coercion exist only when a criminal procedure opens under the principles of due process. Similarly, the action of digital actors "*supports and sometimes expands carceral agendas*,"[154] for instance, by "*increasingly wield[ing] discretionary power to decide what qualifies and ultimately counts as sexual exploitation*."[155] The independence of sovereigns erases the independence of victims. This is justified by the ideal victim, full of suffering, hiding traffickers behind the visibility of the threat to people.[156] Empowered, proactive, and recovered survivors are usually absent from representations.[157] This passivity of victims is already embedded in the definition of trafficking: The consent of the victim is irrelevant.[158]. While the focus should be "*on the exploitative situation and exploitative*

---

[151] K.K. Hoang, "Perverse Humanitarianism and the Business of Rescue: What's Wrong with NGOs and What's Right about the 'Johns'?," *in* A.S. Orloff, R. Ray, E. Savcı (eds.), *Perverse Politics? Feminism, Anti-Imperialism, Multiplicity*, Emerald Group Publishing Limited, Political Power and Social Theory, 1st ed., January 1, 2016, vol. 30, p. 23 citing E. Bernstein, "Militarized Humanitarianism Meets Carceral Feminism," *op. cit.* note 9, pp. 45-71

[152] Term coined by L.M. Agustín, *Sex at the margins: migration, labour markets and the rescue industry*, Zed Books, 2nd ed., 2008

[153] With no consideration of the harm they can produce, see, for instance, S.D. Adhikari, "Beyond dichotomies: Exploring responses to tackling the sex industry in Nepal," *in* S. Dewey, I. Crowhurst, C.O. Izugbara (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 211-221; A. Ahmed, M. Seshu, "'We have the right not to be 'rescued'...': When Anti-Trafficking Programmes Undermine the Health and Well-Being of Sex Workers," *Anti-Trafficking Review*, June 1, 2012, no. 1. It must be underlined that these criticisms of anti-trafficking actions are mainly directed at those focusing on trafficking for sexual exploitation. However, it could also be applied to actions against trafficking for forced labor. For instance, the approach to the phenomenon is similarly carceral, based on sanctions and exclusion. That is the case with the European Commission, Proposal for a Regulation of the European Parliament and of the Council on prohibiting products made with forced labour on the Union market, September 14, 2022, COM(2022) 453 final. These measures will focus on exclusion from the market while not acting upon the origin of the problem. The products will continue to be produced and sold somewhere else. If not, it won't solve the necessity for people, including children, to work, even under poor labor conditions, to sustain themselves and their families.

[154] J. Musto, "The Limits and Possibilities," *op. cit.* note 6, p. 1166

[155] *Ibid.* p. 1150

[156] C. Gregoriou, I.A. Ras, "'Call for Purge on the People Traffickers'," *op. cit.* note 62, pp. 47-48. However, this control over victims that is visible in representations is far from being omnipotent, R. Andrijasevic, *Migration, agency, and citizenship*, *op. cit.* note 43, p. 60

[157] V. Saiz-Echezarreta, M.-C. Alvarado, P. Gómez-Lorenzini, "Incidencia política de las campañas contra la trata: Un relato controvertido," *Comunicar*, Grupo Comunicar, 2018, vol. 26, no. 55, p. 33

[158] Article 3.b of the Palermo Protocol

relationships between the parties involved,"[159] consent is usually considered in practice to identify ideal and deserving victims.[160] This understanding of victims and the independent application of sovereigns' coercion then faces a new concept: the agency of trafficked victims.

558. Concept of agency. Individual sovereignty is barely recognized in the legal discipline. On the contrary, from a sociological perspective, another concept is closely connected to the same idea and is widely recognized: the agency of individuals. This agency is defined as the "*independent capacity to act according to one's own will*,"[161] "*by constituting an economy of the self and a performance of the self that allows one to negotiate one's autonomy*."[162] For instance, studying agency within migration of women supposes to "*refer to the ways in which migrant women responded to, negotiated, or failed to negotiate the restrictions imposed on their mobility by the social and legal position they occupied and by the relations of power through which these were sustained*."[163] Exercising agency requires three elements: being able to act, having the opportunity to act, and wanting to act.[164] Agency is lacking when one is "*able to act (ha[s] the skills) and want[s] to act, but does not have the power [or opportunity] to act (for example, be disabled for some reason); or [when one has] the power to act […] and [is] able to do so (ha[s] the political education and ideas to pass on), but [does] not want to (lack of confidence to put oneself forward); or [when one has] the willingness and power to act but, without the knowledge or opportunities, feels helpless […] in front of the situation*."[165] These opportunities to act depend particularly on elements that shape daily life, such as law or technology.[166] Thus, the agency of

---

[159] M. Viuhko, *Restricted agency, control and exploitation - Understanding the agency of trafficked persons in the 21sst century Finland*, Thesis, University of Helsinki, 2019, p. 27

[160] M. Darley, "Entre droit et culture, l'exploitation sexuelle en procès," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, p. 118. Similarly, "*A rigid demarcation between victims of trafficking and those who apparently 'choose" to enter the industry may serve to place a burden of responsibility on prostituted women for the subsequent abuse and harm they experience within prostitution*," M. O'Connor, "Choice, agency consent and coercion: Complex issues in the lives of prostituted and trafficked women," *Women's Studies International Forum*, May 2017, vol. 62, p. 15

[161] C. Mackenzie, "Agency : un mot, un engagement," *Rives méditerranéennes*, TELEMME (UMR 6570), February 29, 2012, no. 41, p. 35

[162] J. Guilhaumou, "Autour du concept d'agentivité," *Rives méditerranéennes*, TELEMME (UMR 6570), February 29, 2012, no. 41, p. 27

[163] R. Andrijasevic, *Migration, agency, and citizenship*, *op. cit.* note 43, p. 17

[164] Differently, Feenberg cites three other but similar elements: "*knowledge, power and opportunity*." A. Feenberg, "Technique et agency," *Revue du MAUSS*, La Découverte, June 12, 2014, vol. n° 43, no. 1, p. 169

[165] C. Mackenzie, "Agency," *op. cit.* note 161, p. 36

[166] A. Feenberg, "Technique et agency," *op. cit.* note 164, p. 170

individuals also depends on their capabilities and affordances.

559. Agency for trafficked victims. The concept of agency should not produce a polarized debate.[167] It should not be a dichotomy between the full exercise of agency by trafficked victims to exclude them from sovereigns' protection and the full state of victimhood to bring them to the public spheres for sovereigns' protection. Instead, the recognition of agency should help adapt sovereigns' coercion to individuals' needs and their level of agency, improving the quality of victims' protection.[168] On the contrary, the independence of actors and the priority given to sovereign coercion hinder the adequacy of anti-trafficking measures in light of the variety of realities. Studies highlight the wide range of agency enjoyed by trafficked victims. It should be recognized that some victims "*strategized, and made decisions to maximize control of the situation*."[169] In these cases, "*acknowledging the agency of the victims of trafficking does not mean that they should be seen responsible for the exploitation they have encountered*."[170] To detail the complex realities faced by some trafficked victims, who exercise their agency depending on the limits drawn by structural institutions and by traffickers, Viuhko develops the concept of restricted agency, which "*means that victims of trafficking cannot act freely, but they are not passive objects without any agency either. Instead, they have to act within the limits of control imposed on them*."[171] As underlined by the scholar, the prevention and protection of trafficked persons should focus both on "*acknowledg[ing] the agency of those who are assisted*" by listening "*to the victims and their views on what kind of assistance is good for them*"[172] and on supporting the means of protection to rebuild the agency of victims who suffered the most serious forms of coercion.[173] Indeed, in some situations, traffickers can manage to neutralize the agency of victims, particularly minors, up to its core: The subjectivity and the discourses of the victims are then shaped by the trafficker.[174] Thus, agency appears

---

[167] M. Viuhko, *Restricted agency, control and exploitation*, *op. cit.* note 159, p. 51
[168] See, for instance, R. Andrijasevic, *Migration, agency, and citizenship*, *op. cit.* note 43, p. 3
[169] M. O'Connor, "Choice, agency consent and coercion," *op. cit.* note 160, p. 13
[170] M. Viuhko, *Restricted agency, control and exploitation*, *op. cit.* note 159, pp. 28-29
[171] *Ibid.* p. 48. "*Firstly, different forms of psychological, physical, sexual, emotional and economic control and violence have an impact on a person's health, well-being and bodily integrity, to mention a few. Secondly, the exploitative situation and control restrict one's agency […] Thirdly, the restrictions and control have an impact on one's sense of agency, that is their sense of being the subject of their own life and being capable of making decisions and implementing them*," *Ibid.* p. 84
[172] M. Viuhko, *Restricted agency, control and exploitation*, *op. cit.* note 159, p. 94
[173] In particular through "*the emancipation of victims from the bond of exploitation*," B. Lavaud-Legendre, "L'émergence d'un statut de traite," *op. cit.* note 45, p. 122
[174] To theorize these worst forms of coercion, Lavaud-Legendre relies on the concept of "influence relationships" (*relation d'emprise*), B. Lavaud-Legendre, C. Plessard, G. Encrenaz, *Prostitution de*

both as an objective of the protection of victims, rebuilding or empowering their agency, and a means of their protection, taking into account their own capabilities. The concept of agency can delimit and legitimize sovereign coercion. Victims protect their agency through human rights, particularly the right to privacy, although they usually lack direct implementation; victims' rights, although they reduce their understanding of themselves to the status of victims; and digital rights, which can be relevant to prevent trafficking or to protect them online. By recognizing agency, the independence of each actor might support trust and collaboration between them. It must be highlighted that the law is only one tool for this protection and that digital actors' affordances participate in the development of victims' capabilities.

560. To summarize, "*at the crossroads between agency for all and privacy for none, the fight for digital sovereignty rages on*,"[175] as do debates about the protection of trafficked victims. The independence of sovereigns must find a thin balance with the agency of individuals. While this individual approach is needed, it is still paradoxical considering the increasingly invasive interventions of sovereigns.[176] This opposition between the public and private spheres should then be complemented by a collective approach to ensure a comprehensive repression of cyber trafficking.

B. From individual independence to collective empowerment

561. Overcoming the vulnerabilities approach. To protect individual independence through agency and capabilities, the victims' vulnerabilities approach must be overcome.[177] This approach, for instance, is supported by the push and pull factors model.[178] Push factors are usually vulnerabilities to be found in the country of

---

mineures – Quelles réalités sociales et juridiques ?, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020, pp. 126-129, on the basis of the work of R. Dorey, "La relation d'emprise," *Troubles de la personnalité*, Dunod, Psychothérapies, 2013, pp. 88-112. Differently, Schlangen relies on the notion of coercive control, E.A. Schlangen, *The Application of Coercive Control Theory to Youth Sex Trafficking*, Master thesis, Northern Arizona University, 2022, on the basis of the work of E.D. Stark, *Coercive control: the entrapment of women in personal life*, Oxford University Press, Interpersonal violence, 2009. It should be underlined the role of new technologies to implement these forms of control, for an example regarding domestic violence, see D. Cuomo, N. Dolci, "New tools, old abuse: Technology-Enabled Coercive Control (TECC)," *Geoforum*, November 1, 2021, vol. 126, pp. 224-232

[175] C. Guarnieri, "Agency for All, Privacy for None," *op. cit.* note 8, p. 129

[176] S. Milivojević, "The State, Virtual Borders and E-Trafficking: Between Fact and Fiction," *in* S. Pickering, J. McCulloch (eds.), *Borders and crime Pre-crime, mobility and serious harm in an age of globalization*, Palgrave Macmillan, 2012, p. 82

[177] K. Kaye et al., "Neoliberal Vulnerability," *op. cit.* note 59, pp. 76-77

[178] See *supra* 24.

origin, leading to a "*bipolar framework of analysis opposing sending and receiving countries that reinforces the borders between the two*."[179] The vulnerabilities approach supports a management of precariousness and "*reduces the frame to decontextualized individuals (failing to see structural context and a more complete picture of need) and […] negatively judges many who suffer within neoliberal regimes, responding through a punitive moralism and the violence of securitization*."[180] Overcoming the vulnerabilities approach then leads to overcoming an individual protection approach to act upon general structures. Consequently, offering individual capabilities and affordances protecting the individual rests, then, on collective empowerment by sovereigns and partnerships with individuals.

562. Limits of the current prevention system. A focusing on agency can highlight capabilities and affordances needed at the collective level to prevent trafficking. Preventive actions are usually divided into three categories: "*The goal of primary prevention is complete prevention before a phenomenon occurs, the goal of secondary prevention is early intervention and mitigation of risk factors, and the goal of tertiary prevention is intervention and recovery*."[181] Tertiary prevention is usually understood

---

[179] S. Cheng, "A critical engagement with the 'pull and push' model Human trafficking and migration into sex work," *in* R.W. Piotrowicz, C. Rijken, B.H. Uhl (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 500. In particular, prior to a migration process, "*Human agency of the migrant […] is simultaneously erased and magnified, but rarely assessed in context*," *Ibid.* p. 503. Additionally, poverty is usually highlighted as a vulnerability, while "*research indicates that it is generally neither the poorest of the poor nor the least educated who migrate*," P. Marshall, S. Thatun, "Miles Away: The Trouble with Prevention in the Greater Mekong sub-region," *in* K. Kempadoo, J. Sanghera, B. Pattanaik (eds.), *Trafficking and prostitution reconsidered: new perspectives on migration, sex work, and human rights*, Paradigm Publishers, 2nd ed., 2012, pp. 46-48; L. Kiss et al., "The use of Bayesian networks for realist evaluation of complex interventions: evidence for prevention of human trafficking," *Journal of Computational Social Science*, May 2021, vol. 4, no. 1, p. 41. Similarly, vulnerabilities linked to women as a category "*reproduc[e] essentialist ideas about women, which are consistent with oppressive gender dualities*," D. Otto, "Lost in translation," *op. cit.* note 43, p. 345. For instance, "*Prohibitions on offering the choice to cooperate on the basis of an assumed vulnerability foreclose the possibility of empowerment through providing a platform for women's voices to be heard*," L. Kelly, M. Coy, "Ethics as Process, Ethics in Practice: Researching the Sex Industry and Trafficking," *in* D. Siegel, R. de Wildt (eds.), *Ethical Concerns in Research on Human Trafficking*, Springer International Publishing, Studies of Organized Crime, 2016, vol. 13, p. 42. It "*consistently deflects attention from the concentration of power and resources in the hands of men*," J. Turner, "Root Causes," *op. cit.* note 41, p. 206. See also S. Monteros Obelar, "La violencia de las fronteras legales: violencia de género y mujer migrante," *in* P. Laurenzo Copello, M.L. Maqueda Abreu, A. Rubio (eds.), *Género, violencia y derecho*, Tirant lo Blanch, Alternativa, 2008, p. 231; I. de Vries, J.A. Reid, A. Farrell, "From Responding to Uncertainties and Ambiguities to More Constructive and Inclusive Debates on Commercial Sex and Sex Trafficking," *Victims & Offenders*, Routledge, April 3, 2023, vol. 18, no. 3, pp. 592-595

[180] K. Kaye et al., "Neoliberal Vulnerability," *op. cit.* note 59, p. 97

[181] E.J. Alpert, S.E. Chin, "Human Trafficking: Perspectives on Prevention," *in* M. Chisolm-Straker, H. Stoklosa (eds.), *Human Trafficking Is a Public Health Issue: A Paradigm Expansion in the United States*, Springer International Publishing, 2017, p. 383

to be the protection of trafficked victims, while primary and secondary prevention usually focus on the reduction of vulnerabilities, which is the other side of the coin to fostering agency and capabilities. In supranational texts, prevention receives few details, and is focused mainly on "*research, information, and mass media campaigns*";[182] the reduction of vulnerabilities reduction for specific categories of potential victims;[183] the reduction of demand for services or products from trafficking persons, which is not linked to victims' agency;[184] and border control measures,[185] which are increasing measures reducing potential victims' agency.[186] Nonetheless, the Warsaw Convention considers measures "*to enable migration to take place legally, in particular, through dissemination of accurate information*"[187] and "*educational programs for boys and girls during their schooling, which stress […] the importance of*

[182] Article 9.2 of the Palermo Protocol, Article 5.2 of the Warsaw Convention, Article 18.2 of the Directive 2011/36/EU. Similarly, the French latest action plan against human trafficking only includes measures of research and awareness-raising for prevention, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, Secrétariat d'Etat chargé de l'égalité entre les femmes et les hommes et de la lutte contre les discriminations, "2nd plan d'action national contre la traite des êtres humains 2019-2021," France, 2019, Measures 1 to 12. Measures that could have been positive for agency are actually framed in a negative way: migrants are to be taught the risks of exploitation instead of sharing information on safe migration routes and labor rights; children are to be taught about human trafficking instead of fostering respect, equality, and sex education, Measures 6 and 7. Furthermore, these actions were mostly not implemented, CNCDH, "Avis - Evaluation du plan d'action national contre la traite des êtres humains (2019-2021)," January 12, 2023, pp. 9-23, A-2023-1. See also Centro de inteligencia contra el terrorismo y el crimen organizado, "Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023," Secretaría de Estado de seguridad, Ministerio del Interior, Spain, January 2022, Measures 1.1.A to 1.1.C. Further, it must be underlined that prevention actions are rarely evaluated, R. Konrad, A. Trapp, T. Palmbach, "Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications," *European Journal of Operational Research*, June 1, 2017, vol. 259, no. 2, p. 10

[183] Such as "*poverty, underdevelopment and lack of equal opportunity*," Article 9.4 of the Palermo Protocol; or "*inequality, poverty and all forms of discrimination and prejudice*," Office of the High Commissioner for Human Rights, "Recommended Principles and Guidelines on Human Rights and Human Trafficking," UN, 2010, Guideline 7; in particular, children, Article 5.5 of the Warsaw Convention

[184] Article 9.5 of the Palermo Protocol, Article 6 of the Warsaw Convention, Article 18.1 and 4 of the Directive 2011/36/EU

[185] This approach particularly limits a comprehensive perspective on the prevention of labor exploitation, J. van der Leun, "(EU) Migration Policy and Labour Exploitation," *in* C. Rijken (ed.), *Combating trafficking in human beings for labour exploitation*, Wolf Legal Publishers, 2011, pp. 425-441

[186] Articles 11 to 13 of the Palermo Protocol, Articles 7 to 9 of the Warsaw Convention. These measures are nowadays supported by technologies, by, for instance, digitalizing migration procedures, Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 73, p. 44; M. Latonero, B. Wex, S. Ahyaudin, *Technology and Labor Trafficking Project Framing Document*, USC Annenberg - Center on communication leadership & policy, June 2014, p. 9. However, it can reinforce a carceral approach, by focusing on exclusion by borders instead of agency, S. Milivojević, H. Moore, M. Segrave, "Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology," *Anti-Trafficking Review*, April 27, 2020, no. 14, p. 24

[187] Article 5.4 of the Warsaw Convention

gender equality and the dignity and integrity of every human being."[188]

563. Fostering collective empowerment. Therefore, a comprehensive plan to prevent human trafficking should focus on improving individual agency and capabilities instead on human trafficking processes. To this end, many collective-oriented policies could support the prevention of trafficking. Acting upon static poverty, instead of focusing on awareness-raising among the poorest populations, should actively include "*investment in early childhood*," "*inclusive education*," even a "*basic income for young adults*," and the "*prohibition of discrimination on grounds of socioeconomic adults*."[189] A comprehension of dynamic poverty should focus on the reduction of inequality.[190] General policies to access the financial sector could indirectly support the prevention of trafficking, since "*workers usually succumb to debt bondage because an employer is the only or primary source of credit*."[191] The technology sector could contribute to this goal through digital finance opportunities such as payments, wallets, and smartphones.[192] Other general policies could be based on the sharing of information. Instead of focusing on the risks of human trafficking, these measures should be directed towards information on legal migration;[193] complaint filing, free health care,

[188] Article 6.4 of the Warsaw Convention. Further capabilities-enhancing prevention actions can be found in soft law, such as "*developing programs that offer livelihood options, including basic education, skills training and literacy*," Office of the High Commissioner for Human Rights, *Recommended Principles and Guidelines on Human Rights and Human Trafficking*, *op. cit.* note 183, Guideline 7.2 to 4. In this perspective, the Spanish latest plan of action promotes "*the incorporation into the different levels of the educational system of a complete training on fundamental rights*," Centro de inteligencia contra el terrorismo y el crimen organizado, *Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023*, *op. cit.* note 182, Measure 1.1.D.

[189] Secretary-General, "Extreme poverty and human rights Note," General Assembly, UN, July 19, 2021, ¶¶ 43-53, A/76/177

[190] Nevertheless, it "*is likely to take a generations and in fact may prove to be an impossibility within the current global political and economic structures*," P. Marshall, S. Thatun, "Miles Away," *op. cit.* note 179, pp. 46-48

[191] J. Cockayne, *Innovation for inclusion: using digital technology to increase financial agency and prevent modern slavery*, Secretariat Briefing Paper 3, Financial Sector Commission Secretariat, UN University, Liechtenstein Initiative for a Financial Sector Commission on Modern Slavery and Human Trafficking, 2019, p. 2

[192] *Ibid.* p. 5

[193] P. Marshall, S. Thatun, "Miles Away," *op. cit.* note 179, pp. 48-50. For instance, Facebook developed a chat bot "*disseminating valuable migration information*," Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 73, p. 41

and NGOs for protection;[194] labor rights[195] and the labor market;[196] and sexual and affective education, et cetera. Fostering tolerance for diversity and reducing stereotypes also is accomplished through media representations, such as in advertisements. While the regulation of advertisements is limited under EU law,[197] international soft law requests commercial communication to "*respect human dignity and [to] not encourage or condone any form of discrimination*."[198] Both states and digital actors play a major role in sharing transparent, accurate, and non-stereotypical information on these topics. Finally, collective empowerment depends on digital literacy.[199] This "*set of skills needed to interact with digital media, deal with information online, or manage one's own data, etc.*" can be seen as the exercise of individual digital

[194] For instance, on websites hosting sexual services advertisements, Global programme against trafficking in human beings, "Toolkit to Combat Trafficking in Persons," UNODC, UN, 2008, p. 488; A. Horning, L. Stalans, "Oblivious 'Sex Traffickers': Challenging stereotypes and the fairness of US trafficking laws," *Anti-Trafficking Review*, April 19, 2022, no. 18, p. 85; or "*on search engine results for pornography*," L.M. Rhodes, "Human trafficking as cybercrime," *AGORA International Journal of Administration Sciences*, 2017, no. 1, p. 2

[195] Labor rights can partly be increased by the protection of labor contracts digitally, such as through block chain technology, to limit contract substitutions, J. Cockayne, *Innovation for inclusion*, *op. cit.* note 191, pp. 10-11

[196] Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, Tech Against Trafficking, *Leveraging innovation to fight trafficking in human beings*, *op. cit.* note 73, pp. 8, 40. Information can be shared on recruitment agencies and the modalities of hiring, S. Raets, J. Janssens, "Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business," *European Journal on Criminal Policy & Research*, Springer Nature, June 2021, vol. 27, no. 2, p. 226; M. Latonero et al., *Technology and Labor Trafficking in a Network Society - General Overview, Emerging Innovations, and Philippines Case Study*, USC Annenberg - USC University of Southern California, February 2015, p. 25. Information sharing is also developed within the sex work sector, J. Scoular et al., "Beyond the Gaze and Well Beyond Wolfenden: The Practices and Rationalities of Regulating and Policing Sex Work in the Digital Age," *Journal of Law and Society*, June 2019, vol. 46, no. 2, pp. 229-235

[197] See, for instance, Article 26 of the Digital Services Act and Chapter VII of the Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services

[198] Article 4, Chambre de commerce internationale, "Code ICC consolidé sur les pratiques de publicité et de communication commerciale," 2011. Spain took into consideration the role of advertisements in representations, and the need to limit gender stereotypes, see Articles 10, 13 and 14 of the Ley Orgánica 1/2004 de medidas de protección integral contra la violencia de género and Article 36 to 41 of the Ley Orgánica 3/2007 para la igualdad efectiva entre hombres y mujeres. See, for instance, J.M. Bernardo Paniagua et al. (eds.), *Retos de la comunicación ante la violencia de género: marco jurídico, discurso mediático y compromiso social*, Tirant lo Blanch, Monografías no. 656, 2009

[199] Spotlight Initiative, "Mobile women and mobile phones Women migrant workers' use of information and communication technologies in ASEAN," EU, ILO, 2019, p. 29. See, in particular, J. Elliott, K. McCartan, "The Reality of Trafficked People's Access to Technology," *The Journal of Criminal Law*, June 2013, vol. 77, no. 3, pp. 255-273. However, preventive actions are usually limited to online safety, in particular directed at minors, D. Dushi, "Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo," *International Review of Law, Computers & Technology*, January 2, 2018, vol. 32, no. 1, p. 96; Groupe de travail interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes - Rapport sur la cybercriminalité*, République française, February 2014, p. 103

sovereignty.[200] This requires opportunities ranging from "*a basic right for access*," to an actual provision of access on a large scale, and an understanding of "*individual needs and barriers as well as collective motivations*."[201]

564. Independence and equality of sovereigns and individuals, thus, are "*functional fiction [as they do] not coincide with a reality characterized by inequalities of power, phenomena of domination, and subordination*."[202] The theoretical perspective on independence cracks with a strict public/private divide, and its practical implementation challenges a comprehensive repression of trafficking, questioning the means of protection, and a restrictive perspective on prevention. Accordingly, comprehensive anti-cyber trafficking policies highlight interlinkages between actors, and interdependence appears as a criterion for legitimate sovereigns' coercion.

§2. The opportunities of interdependent sovereignties to repress cyber trafficking

565. Interdependence: concept. The notion of interdependence is usually limited between states[203] due to globalization.[204] This perspective can go further. First, interdependence could be understood between all actors involved in the resolution of a specific problem, here, cyber trafficking.[205] Second, the economic perspective,

---

[200] G. Joost, "Out of Balance," *op. cit.* note 150, p. 99

[201] *Ibid.* p. 101

[202] H. Ruiz Fabri, "Droits de l'homme et souveraineté de l'État," *op. cit.* note 137, p. 373. It must be underlined that, historically, "*State sovereignty was initially envisaged as a means of coexistence for states that have always been plural, unlike the empire. In other words, it supports independence just as much as it does interdependence. For a long time, the absolutism of sovereignty masked this dual facet*," J.-M. Sorel, "Le rôle de la soft law dans la gouvernance mondiale : vers une emprise hégémonique ?," *Revue Européenne du Droit*, Groupe d'études géopolitiques, 2021, vol. 2, no. 1, p. 50

[203] J. Charpentier, "Le phénomène étatique à travers les grandes mutations politiques contemporaines," *in* Société française pour le droit international (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 31. The theory of interdependence is also applied to human rights, M.J. Añón Roig, "Derechos sociales: cuestiones de legalidad y de legitimidad," *Anales de la Cátedra Francisco Suárez*, Imprenta de Francisco Ventura y Sabatel, 2010, no. 44, pp. 15-41

[204] J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018, p. 26

[205] It results that every sovereign actor "*should be seen as having both problems [such as cyber human trafficking,] (needs) and solutions (capacities), and as being mutually dependent on each other for their resolution and use*," J. Black, "Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world," *Current Legal Problems*, Oxford University Press, February 21, 2001, vol. 54, no. 1, p. 110. Black especially grounds these interdependencies in "*the rejection of a clear distinction between public and private*" spheres, J. Black, "Constructing and contesting legitimacy and accountability in polycentric regulatory regimes," *Regulation & Governance*, 2008, vol. 2, no. 2, p. 140. In general, interdependence is already implemented through "*jurisdictional solidarity*," under which "*supranational, shared legal rights […] must be protected through an equally shared effort*," G. Quintero Olivares, "Organizaciones y grupos criminales en el derecho penal de nuestro tiempo," *in* C. Villacampa Estiarte (ed.), *La delincuencia organizada: un reto a la política-criminal actual*, Aranzadi, Primera edición, 2013, p. 29

relying on the current model of capitalism, is insufficient. For instance, Black's notion of decentered regulation is based on the complementary notions of autonomy and interdependence. The fragmentation of powers needs the "*recognition of the autonomy of*" sovereign entities: "*Actors will continue to develop or act in their own way in the absence of intervention*."[206] Nevertheless, decentered regulation also rests on "*the existence and complexity of interactions and interdependencies between*" sovereigns.[207] Interdependence has also been developed under feminist theories: Relying only on an "*ideal of autonomy and agency*" negates "*the value of human interdependence*."[208] Focusing on the practical implementation of concepts, "*the recognition of interdependence, is […] the precondition for genuine, non-exploitative, interdependence*."[209] This inter-individual analysis, based on women's exploitation, could be applied at the sovereign actors' level.

566. New relationships between sovereigns are developed to comprehensively and effectively repress cyber trafficking, highlighting multiple interdependencies. Legitimizing their sovereignty increasingly seems to require strong, interdependent links. Here, effectivity can be understood as "*the degree to which a principle [or value] is implemented*,"[210] which requires, through interdependence, the definition of shared values (I) and the construction of bridges between diverse communities and actors to

---

[206] J. Black, "Decentring regulation," *op. cit.* note 205, p. 108

[207] *Ibid.* p. 109. Dubos, with its concept of "subreignty," gives an example of regulation interdependence due to the fragmentation of competence between the EU and its member states, O. Dubos, "L'Union européenne : sphynx ou énigme ?," *in* Collectif (ed.), *Les dynamiques du droit européen en début de siècle: études en l'honneur de Jean Claude Gautron*, Pedone, 2004, p. 29

[208] R. Lister, *Citizenship: feminist perspectives*, Palgrave Macmillan, 2nd ed., 2003, p. 107 Here, "*The opposition […] lies not so much between dependence and independence, with interdependence representing the synthesis […], but between dependence and independence on the one hand and interdependence on the other*," *Ibid.*. The former distinction is understood as the following: independence as autonomy is the ability, "*within the bounds of justice, to be able to make choices about one's life and to act on those choices without having to obey others, meet their conditions, or fear their threats and punishments*," while dependence is seen as the opposite of self-sufficiency, meaning "*not needing help or support from anyone in meeting one's needs and carrying out one's life plan*," I.M. Young, "Mothers, Citizenship, and Independence: A Critique of Pure Family Values," *Ethics*, University of Chicago Press, 1995, vol. 105, no. 3, pp. 548-549. For a historical study of the meanings of dependence and independence concluding with the negation of such a dichotomy, see N. Fraser, L. Gordon, "'Dependency' Demystified: Inscriptions of Power in a Keyword of the Welfare State," *Social Politics: International Studies in Gender, State & Society*, March 1, 1994, vol. 1, no. 1, pp. 4-31

[209] R. Lister, *Citizenship*, *op. cit.* note 208, p. 107

[210] L. Heuschling, "'Effectivité', 'efficacité', 'efficience', et 'qualité' d'une norme/d'un droit. Analyse des mots et des concepts," *in* M. Fatin-Rouge Stéfanini et al. (eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?*, Bruylant, À la croisée des droits 6, 2012, p. 44

implement these values[211] (II).[212]

I. Legitimizing sovereignties through interdependent values

567. Independent values: neutrality. Independence often goes accompanies neutrality: In private spheres, the state should be neutral. In its original meaning, a neutral state is one that will not, at least openly, participate in a conflict between states, usually, a war. When resolving a private conflict, the state's institutions, such as judges, must be impartial and neutral. This neutrality principle was adapted to digital actors: It "*ensures equal access to the network regardless of who the user is and the service that they connect to*."[213] Under EU law, "*end users shall have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, irrespective of the end user's or provider's location or the location, origin, or destination of the information, content, application, or service*." However, this principle is limited to being applied "*via their Internet access service*."[214] Accordingly, most digital actors, aside from Internet access service providers,[215] can draft their terms of service to discriminate against content.[216] For instance, search engines and various types of platforms hide or select content depending on the origin of the connection.[217] Even so, "*defining what is relevant involves guesswork and value*

[211] Foucault highlighted the need to define "us," meaning the concerned communities, after the definition of values, depending on the questions to be answered and changing depending on them, J.-A. Mazères, "Normativité, vérité, gouvernementalité : figures du juridique chez Michel Foucault," *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, no. 2, p. 74

[212] On the necessary complementarity between external values and procedures, see A.E. Waldman, "Algorithmic Legitimacy," *in* W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, 1st ed., October 31, 2020, p. 119

[213] B. Thieulin, *Towards a European digital sovereignty policy*, *op. cit.* note 135, p. 17. "*The core idea of neutrality is to prevent massive intermediaries from distorting either private commerce or the public sphere simply by virtue of their size, network power, or surveillance capacities*," F. Pasquale, "Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power," *Theoretical Inquiries in Law*, January 1, 2016, vol. 17, p. 489

[214] Article 3.1 of Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications. Additionally, "*Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used*," Article 3.3.

[215] However, even technical providers "*have been pushing for an increased ability to price discriminate online, including the ability to charge more for content provided by a competitor*," M.K. Land, "Toward an International Law of the Internet," *Harvard International Law Journal*, 2013, vol. 54, no. 2, p. 424

[216] Thus, the principle has been qualified as a "*myth*," T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018, p. 24

[217] B. Thieulin, *Towards a European digital sovereignty policy*, *op. cit.* note 135, p. 18

judgments."[218] This situation has led authors to advocate for the extension of the principle to hosting actors[219] and particularly to the functioning of algorithms classifying content.[220] However, this neutrality would reject the cooperation of digital actors in repressing cyber trafficking. Under a broad neutrality principle, a search engine should not establish a preference between the same services in different origins (for instance, between an official public service from a destination country to support migration processes for work and an unregulated broker in an origin country), even when trafficking indicators highlight more risks of exploitation in one case. Thus, neutrality denies the power of material and technical affordances, the embeddedness of politics in digital actors, and the interdependence of all sovereign actors. Therefore, a new positive meaning could be considered.

568. Interdependent values. "The net neutrality debate is a debate about power, and the right way to use it."[221] Still, "*networked technology is often more prone to concentrate power than it is to diffuse it*."[222] The current understanding of neutrality relies on the negative meaning of the absence of action or at least of differentiated actions. On the contrary, a positive meaning of neutrality could include the obligation to act to protect interdependent values. Under the current international framework, the protected values are established by the human rights framework and the balance is made by states in cases of competing interests.[223] Currently, this obligation to perform for digital actors relies mainly on removing content on the basis of interdependent objectives, such as the repression of trafficking, or on the basis of the terms of service, mainly defined arbitrarily by digital actors. However, to favor the agency of users,[224], digital actors could also be obligated to protect other content on the basis of additional

[218] C. Canca, "Did You Find It on the Internet? Ethical Complexities of Search Engine Rankings," *in* H. Werthner et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, p. 136; D. Lewandowski, "Is Google Responsible for Providing Fair and Unbiased Results?," *in* M. Taddeo, L. Floridi (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 61-77; E.B. Laidlaw, "Private Power, Public Interest: An Examination of Search Engine Accountability," *International Journal of Law and Information Technology*, March 1, 2009, vol. 17, no. 1, pp. 113-145

[219] B. Bayart, A. de Cornulier, "La neutralité du net," *Pouvoirs*, January 11, 2018, vol. N° 164, no. 1, p. 129

[220] B. Thieulin, *Towards a European digital sovereignty policy*, *op. cit.* note 135, p. 31

[221] B. Bayart, A. de Cornulier, "La neutralité du net," *op. cit.* note 219, p. 128

[222] F. Pasquale, "Platform Neutrality," *op. cit.* note 213, p. 498

[223] This balance can be influenced by the voting process, in which the population is asked to choose between programs that rest on different priorities regarding values.

[224] For instance, regarding search engines, by incorporating "*user settings to the search engine interface to encourage user agency and provide them with a catalog of setting options for ranking*," C. Canca, "Did You Find It on the Internet?," *op. cit.* note 218, p. 141

values such as freedom of expression, the protection of minorities, and diversity.[225] Indeed, as deletion policies exclude certain "*political aspects, [they] can widen the digital inequality gap, and reduces social issues to numbers*."[226] Interdependent values could be multiple, from legal to non-legal concepts such as "*well-being, efficiency, and democracy*."[227] The concept of human rights could offer a first basis for listing these shared values if going beyond a state-based approach. A comprehensive repression of trafficking could then ground its legitimacy in interdependent general values. Here, the law could support "*anchorage-based governance, since the aim is to enshrine […] a certain number of values that underpin society (hence the reference to a stabilizing anchorage). Viewed not from the internal, legal angle but from the external, social angle, [this function] should have the effect of […] legitimizing*"[228] sovereigns here in their anti-trafficking actions.

569. The current proposition is not to settle the content of these values but to offer a methodology to legitimize the action of interdependent sovereigns. Indeed, values, including human rights, can face many interpretations depending on their contextual implementation: "*Important and commonly held values do not provide a straightforward answer*."[229] Then, to legitimize the interpretation provided to shared values, new bridges should be built between sovereign actors to adapt interdependent values to local implementations.

II. Legitimizing sovereignties through interdependent communities

570. Building bridges: states and digital actors. There are many ways to implement values between sovereign states and digital actors. As developed all throughout this study,[230] this can materialize through the coercion of digital actors by states by reaching their criminal liability, or through collaboration on many topics. These partnerships differently implement the same interdependent value: the

---

[225] Indeed, it has been proven that current algorithms of content moderation hinder diversity, M.L. Stasi, "La exposición a la diversidad de contenidos en las redes sociales: Entre la regulación o la desagregación en la curación de contenidos," *Teoría y derecho: revista de pensamiento jurídico*, Tirant lo Blanch, 2022, no. 32, pp. 130-165

[226] J.L. Manfredi Sánchez, "La transformación política de la privacidad," *in* O. Fuentes Soriano, P. Arrabal Platero, M. Alcaraz Ramos (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, p. 96

[227] C. Canca, "Did You Find It on the Internet?," *op. cit.* note 218, p. 141

[228] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016, p. 225

[229] C. Canca, "Did You Find It on the Internet?," *op. cit.* note 218, p. 141

[230] See *supra* Part 2. Title 1. Chapter 1. to Part 2. Title 2. Chapter 1. .

repression of cyber trafficking. However, these relationships are usually limited in their ability to build a real bridge to discuss the implementation of values. One institution could support this aim: National referral mechanisms could coordinate the actions of all actors involved in repressing human trafficking.[231] Currently, within the EU, only Italy appears to include specific digital actors (phone operators) in its national referral mechanism.[232] While the French national action plan against child prostitution considers partnerships, including with digital actors,[233] no national referral mechanism exists. The EU supports the development of a transnational referral mechanism, which could coordinate victims' protection at the EU level by including digital actors. Even so, for now, transnational referral mechanisms are seen only as "*a platform to inform and connect counter-trafficking practitioners in countries of origin and countries of destination*" without "*the creation of an independent instrument*."[234]

571. Building bridges: digital actors and people. The legitimacy of democratic state coercion is particularly grounded in elections and representations and, subsequently, in values established in a constitutional document). Under this framework, the legitimacy of digital actors' coercion is not straightforward.[235] Nonetheless, "*as online speech platforms […] increasingly resemble governments, it is hardly surprising that end users expect them to abide by the basic obligations of those who govern populations in democratic societies*."[236] Therefore, implementing interdependent values requires building bridges between digital actors and people, particularly to legitimately implement anti-trafficking actions. When tensions arise in

---

[231] From a practical perspective, for the referral of victims, regarding national referral mechanisms in a strict sense; from an institutional perspective, for the setting of policies' priority and coordination, regarding similar coordination mechanisms.

[232] Directorate General for Migration and Home Affairs, *Study on reviewing the functioning of Member States' National and Transnational Referral Mechanisms*, European Commission, EU, 2020, pp. 36-38, priority 5, that does not include any specific action for its implementation.

[233] Gouvernement, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, France, November 15, 2021

[234] Directorate General for Migration and Home Affairs, *National and Transnational Referral Mechanisms*, *op. cit.* note 232, p. 18, citing I. Orfana, *Guidelines for development of a transnational referral mechanism for trafficked persons in Europe: TRM-EU*, Department of Equal Opportunities, Presidency of the Council of Ministers, Italy, ICMPD, 2010. However, the latter document does not close the door to an independent institution, as long as it does not "*replace nor duplicate any existing national anti-trafficking structures.*"

[235] Additionally, the Internet is highly criticized as a participatory system, C. Fuchs, "Class and Exploitation on the Internet," *in* T. Scholz (ed.), *Digital labor: the Internet as playground and factory*, Routledge, 2013, p. 270

[236] J. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation," *University of California Davis Law Review*, January 1, 2018, vol. 51, p. 1198

this process,[237] digital actors can involve users in resolving them. When digital actors' rules "*reflect morality rather than legality*,"[238] this morality should adapt to the people to whom the service is directed. For now, "*the ability of users to interact with the algorithm and choose their preferred settings*"[239] remains limited.[240] However, these settings could be particularly useful to increase the protection and empowerment of actual or potential trafficked victims. Differently, "*corporations have thus developed the type of dynamic feedback loop between disputes and policymaking to which the public system aspires*."[241] To achieve this aim, the Digital Services Act regulates a two-level dispute mechanism: an internal complaint-handling system and an out-of-court dispute settlement.[242] Both procedures are open to recipients of the digital service, which raises the question of the applicability of the procedure to non-recipients.[243] For example, this questions the use of these procedures by a trafficked victim who is not the recipient of the digital service but whose data were posted by the trafficker. Furthermore, these mechanisms regard the decisions of digital actors only with the following consequences: removal of access and restriction of visibility of content[244] and suspension or termination of the provision of the service, the account, or monetization.[245] Thus, these mechanisms are not applicable to a decision by a digital actor to ignore a complaint, which could reduce the possibility for trafficked victims to dispute their needs, such as a request for data deletion. More comprehensive means are still needed to connect different needs of individuals and to apply interdependent

---

[237] T. Gillespie, *Custodians of the internet*, *op. cit.* note 216, p. 213

[238] Y. Gerrard, H. Thornham, "Content moderation: Social media's sexist assemblages," *New Media & Society*, SAGE Publications, July 1, 2020, vol. 22, no. 7, p. 1276

[239] M.L. Stasi, "La exposición a la diversidad de contenidos en las redes sociales," *op. cit.* note 225, p. 146

[240] N. Elkin-Koren, "Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence," *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, p. 4

[241] R. Van Loo, "The Corporation as Courthouse," *op. cit.* note 106, pp. 563-564. Indeed, "*moderation has become a site of political contestation in many countries*," R. Gorwa, R. Binns, C. Katzenbach, "Algorithmic content moderation: Technical and political challenges in the automation of platform governance," *Big Data & Society*, SAGE Publications Ltd, January 1, 2020, vol. 7, no. 1, p. 11.

[242] Articles 20 and 21 of the Digital Services Act. Both are applicable to providers of online platforms, excluding micro and small companies, Article 19.1. That is odd, as these mechanisms are in reaction to a notice and action mechanism, which is an obligation for all providers of hosting services, Article 16.

[243] This is considered, on the contrary, in the notice and action mechanism regulation, Article 16.1 of the Digital Services Act.

[244] This includes the practice of shadow banning, which means "*that the platform, through the use of algorithmic or human content moderation, partially or entirely blocks the reach of some content without notifying the creators of that content*," K. Tiidenberg, E. van der Nagel, *Sex and social media*, *op. cit.* note 21, p. 53. This practice is particularly relevant against sex workers, D. Blunt et al., *Posting into the Void: studying the impact of shadowbanning on sex workers and activists*, Hacking//Hustling, 2020

[245] Article 20.1 of the Digital Services Act

values by digital actors, particularly to repress cyber human trafficking. However, building bridges between individual users and digital actors is insufficient: Communities should also be taken into account.

572. Building bridges: digital actors and communities. Relationships between digital actors and communities of people can support legitimacy in the implementation of interdependent values. According to Habermas, a "*deliberative model of democracy [… should include various] processes of public will formation*."[246] In particular, connecting with communities of survivors,[247] NGOs, migrants and work seekers,[248] and sex workers[249] could contribute to legitimizing digital actors' actions. However, "*when these platforms [… increasingly control our digital space, communities are at risk*."[250] These new communities could be imagined,[251] recognized, and connected to digital actors, and this aim is fulfilled by representation in democratic states. Nonetheless, it might be unlikely that dispute mechanisms exist within digital actors' governance

[246] A.G. Scherer, G. Palazzo, "The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy: Political Role of Business in a Globalized World," *Journal of Management Studies*, June 2011, vol. 48, no. 4, p. 918

[247] In particular, on the importance of survivors' narratives, see C. d'Estrée, "Voices from Victims and Survivors of Human Trafficking," *in* J. Winterdyk, B. Perrin, P.L. Reichel (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 79

[248] Both categories highly use online services when looking for ways to migrate and to find work, L. Rende Taylor, E. Shih, "Worker feedback technologies and combatting modern slavery in global supply chains: examining the effectiveness of remediation-oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking," *Journal of the British Academy*, 2019, vol. 7, no. 1, p. 142; A. Beduschi, "The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law," *Georgetown Journal of International Law*, 2018, vol. 49, no. 3, p. 982.

[249] On the involvement of sex workers' organizations to build bridges to regulate the sector, see L. Armstrong, "Sex worker rights activism and the decriminalisation of sex work in New Zealand," *in* S. Dewey, I. Crowhurst, C.O. Izugbara (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 138-147; C. Healy, C. Bennachie, A. Reed, "History of the New Zealand Prostitutes' Collective," *in* G. Abel et al. (eds.), *Taking the crime out of sex work: New Zealand sex workers' fight for decriminalisation*, Policy Press, 2010, p. 45. This kind of involvement could be adapted when facing digital actors' policies.

[250] C. Bronstein, "Pornography, Trans Visibility, and the Demise of Tumblr," *TSQ: Transgender Studies Quarterly*, May 1, 2020, vol. 7, no. 2, p. 251

[251] Anderson considers a nation "*an imagined political community - and imagined as both inherently limited and sovereign. It is imagined because the members of even the smallest nation will never know most of their fellow-members […] The nation is imagined as limited because even the largest of them, encompassing perhaps a billion living human beings, has finite, if elastic, boundaries, beyond which lie other nations […] It is imagined as sovereign because the concept was born in an age in which Enlightenment and Revolution were destroying the legitimacy of the divinely-ordained, hierarchical dynastic realm […] Finally, it is imagined as a community, because, regardless of the actual inequality and exploitation that may prevail in each, the nation is always conceived as a deep, horizontal comradeship*," B. Anderson, *Imagined communities: reflections on the origin and spread of nationalism*, Verso, Revised ed, 2006, pp. 22-23. Once sovereignty is applied to other entities than states, new political communities can be imagined.

institutions.[252]. In the current setting, the digital and technology sectors support "*toxic technocultures*"[253] by relying on the "*mainstream culture [of the] White, male, heterosexual, upper and middle class [individual] in its point of view and assumptions*."[254] The problem is not technical but deeply human. Diversity in the workplace is related mostly to the law of the country of the said workplace; in general, this is the United States. In the EU, another option to build bridges with communities was developed in the Digital Services Act: trusted flaggers, as individuals or collectives such as an NGO. They have "*particular expertise and competence for the purposes of detecting, identifying, and notifying illegal content*," leading digital actors to give priority to their notices.[255] This status is awarded by Digital Services Coordinators, which questions the procedure for applying it to transnational or multinational collectives. Furthermore, no criteria are established to determine the expertise of these coordinators, while they can weigh substantially in content moderation, and no requirement is set regarding their independence from governments.[256] While many perspectives can be adopted around the repression of human trafficking, this political diversity should be replicated by trusted flaggers who are dedicated to reporting content linked to this offense. While some have advocated for global syndicalism to limit exploitation,[257] new places for social dialogue could be developed to increasingly legitimize the implementation of interdependent values by digital actors.

573. Conclusion of the section. Sovereignty was developed for independent

---

[252] Members of the internal complaint-handling system should only act in "*non-arbitrary manner*," Article 20.1 of the Digital Services Act. Members of the out-of-court dispute settlement mechanism should be "*impartial and independent, including financially independent, of providers of online platforms and of recipients of the service*" and have "*the necessary expertise*," Article 21.3.a and b

[253] A. Massanari, "#Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures," *New Media & Society*, 2017, vol. 19, no. 3, p. 333

[254] C.S. Vance, "Pleasure and Danger: Toward a Politics of Sexuality," *in* C.S. Vance (ed.), *Pleasure and danger: exploring female sexuality*, Pandora Press ; Distributed in North America by New York University Press, 1992, p. 13. For instance, at first, Google Maps pronounced "Malcolm Ten Boulevard" instead of correctly interpreting Malcolm X, R. Benjamin, *Race after technology: abolitionist tools for the new Jim code*, Polity, 2019, p. 83. Additionally, the author of this thesis realized that the Google vocal recognition system in French does not recognize the masculine version of "prostitute" and always writes it in feminine, even when the article is masculine.

[255] Article 22.1 and 2.a of the Digital Services Act

[256] J.J. Castelló Pastor, "El alertador fiable como notificador de contenido ¿ilícito? en la red," *op. cit.* note 101, p. 64. However, the status can be suspended or revoked, in particular if "*a trusted flagger has submitted a significant number of insufficiently precise, inaccurate or inadequately substantiated notices*," Article 22.6 and 7

[257] S. Olarte Encabo, "El desafío del trabajo decente en las cadenas mundiales de suministros. Respuesta internacional, estatal, sindical y social," *in* M.I. Ramos Tapia et al. (eds.), *Formas contemporáneas de esclavitud y derechos humanos en clave de globalización, género y trata de personas*, Tirant lo Blanch, Homenajes & congresos, 2020, pp. 91-134

states. However, the repression of cyber human trafficking highlights the lack of independence and the need for coordination of a comprehensive strategy. The notion of independence rests on the traditional division between the public and private spheres, which receives a significant amount of criticism. This independence further challenges the comprehensive repression of cyber trafficking. It supports a security and criminal approach to the offense while not ignoring the agency of individuals, particularly victims. Therefore, individual independence appears to be a legitimate limit to coercive powers, but independence downgrades comprehensive strategies for prevention and protection, and a collective approach to repressing trafficking is needed. Facing the opportunities and limits of independence, a new standard, interdependence, arises to legitimize sovereigns' action. This concept "*challenge[s] the comfort of sovereignty*."[258] However, it is needed to "*assume our interdependence*,"[259] as a consequence of the evolution of relationships and powers between states and private actors, particularly digital ones. This study offers a methodological proposition to legitimize the actions of interdependent sovereigns. First, interdependent core values should be established. This implies upgrading the notion of neutrality by recognizing the involvement of private actors in establishing and implementing values. Second, the implementation of these values could rely on new bridges between sovereigns and people. The global architecture of norms turns towards "*the spirit of soft law: that the legitimacy of the norm is to be sought not in an ultimate authority held by a single instance, but in a dispersed interactivity according to fluid mechanisms of power sharing; that the validity of the norm is to be assessed not in a hierarchical framework guaranteed by a complete jurisdictional system controlling formal responsibilities, but in a horizontal plane regulated by a dynamic of emulation bringing concrete attributions into play*."[260] Such an interconnected network is currently required to include all actors who are concerned with the repression of human trafficking.

574. Conclusion of the chapter. While not all frameworks of cooperation between states and digital actors are dedicated to the repression of human trafficking, they contribute to softening the relationships between sovereigns as part of this common

[258] B. Badie, "D'une souveraineté fictive à une post-souveraineté incertaine," *op. cit.* note 110, p. 13
[259] J.-F. Jamet, "L'Europe au défi de la souveraineté technologique," *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, ¶ 21
[260] M.-L. Basilien-Gainche, "Gouvernance et efficacité des normes juridiques," *in* M. Fatin-Rouge Stéfanini et al. (eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?*, Bruylant, À la croisée des droits 6, 2012, p. 98

goal. However, this collaboration is insufficient to legitimize coercive powers. The fight against cyber trafficking has been framed under a security approach, and the protection of victims and prevention are downgraded. The former remains closely linked to criminal procedure. However, their status as users of digital actors' services unlocks new rights, particularly through the GDPR (for instance, the right to be forgotten) and the Digital Services Act (for instance, the notice of illegal content). Thus, the role of digital actors is based on the development of affordances. While digital actors intermediate the relationships between states and their population, states' laws intermediate the legitimacy of digital actors in front of people. This conclusion questions the basis of the theory of sovereignty: independence. This concept is criticized on both its theoretical grounds and its application to developing a comprehensive strategy against cyber trafficking. First, independent sovereigns' actions to repress trafficking clash with the protected independent sphere of action of individuals, especially with the victims' agency. Second, this concept limits comprehensive and collective means to repress trafficking, particularly for prevention. Thus, to build a strategy to fight human trafficking, especially when facilitated by new technologies, it is necessary to rethink sovereignty through interdependence to legitimize coercion. A potential methodology is drawn to develop such a new theory through the study of the anti-trafficking framework. Interdependent values will provide a basis for the legitimacy of sovereigns' actions, but they must be implemented and adapted to the context. This requires building bridges between actors to establish networks of discussions. New ways of connecting actors and developing an interdependent strategy could support both the repression of cyber human trafficking and the legitimacy of coercion from traditional and new sovereigns.

575. Conclusion of the title. The order of coercion with non-state sovereign actors was traditionally established by criminal law. However, a mere criminal law approach limits a comprehensive repression of human trafficking and cannot guarantee the protection of human rights. To go further than this first order, states and digital actors also seek to foster a second order based on collaboration. This approach tends to avoid the criminal law and is grounded in other fields and types of norms, particularly ones that are not traditionally related to the anti-trafficking framework. Collaboration arises from corporate social responsibility norms, which regulate compliance systems. Some of these national norms were adopted primarily to prevent and minimize the risks of human trafficking. However, this field of norms remains vague, especially regarding its scope. Their primary objective was to prevent trafficking within the value chains of corporations. Differently, the repression of cyber trafficking requires preventing the use of its services by perpetrators. Digital actors tend to focus on this perspective, thus changing the purpose behind the law. Due to the further limitation of the material, personal, and geographical scopes, a specific type of corporate social responsibility norm could support collaboration between states and digital actors in their anti-trafficking actions. Indeed, the EU is building a framework of norms dedicated to digital actors, particularly from a compliance perspective. These norms extend beyond mere transparency obligations and require digital actors and states to build points of contact to moderate online content linked to offenses and to avoid the violation of human rights. Although they are not dedicated to repressing trafficking, these norms could be effective in this fight. However, corporate social responsibility fosters few relationships between sovereigns and individuals, who are the ultimate recipients of coercion. Due to this lack of connection, the role of digital actors in repressing trafficking highlights a return to a security approach based on sanctions and border control. Since trafficked victims should not be understood only through a criminal procedure lens, states intermediate other rights implemented by digital actors. Based on data protection and content moderation, digital actors must offer new affordances to their users, some of which are of particular interest to trafficked victims and vulnerable people. This interconnection of sovereigns to comprehensively repress trafficking raises questions about the traditional basis of sovereignty: independence. This notion is based on a divide between the public and private spheres, a binary dichotomy that has been highly criticized. This divide is particularly challenging for the repression of human trafficking, as it tends to limit the consideration of victims' agency and the importance of balancing

individual needs and human rights to limit sovereign coercion. Independence further restricts a comprehensive approach to prevention by focusing on human trafficking, while the prevention of vulnerabilities should be complemented by collective empowerment actions. Thus, interdependence seems to offer a new basis for legitimate sovereign coercion. To implement this interdependence, a new methodology should be applied. Interdependent values could first be defined to settle general guidance, particularly to repress human trafficking. Nevertheless, local implementations require adaptation, defined through new bridges built among the various actors who are relevant to this fight.

576. Preliminary conclusion. Once the theory of sovereignty is applied to various types of entities, a second question arises: What is the order between their actions and coercion through the types of relationships they develop? This order can contribute to support or hinder a comprehensive repression of cyber human trafficking. At first, these relationships were based on the acme of state sovereignty: criminal law. Some states meant to reassert their coercion over digital actors, limiting their independence and leading to the internalization of the anti-trafficking fight in private policies. However, such a security approach based on facilitating the conviction of digital actors for trafficking does not offer a comprehensive repression of the offense; even worse, it favors censorship, limits its investigation, and threatens the independence of other sovereigns. As a consequence, it should be highlighted that other fields of law are relevant to repressing trafficking, and these fields adopt a different order of coercion based on collaboration. Corporate social responsibility, particularly compliance systems mandatory to digital actors, provides a first approach for this cooperation, despite the criticism it faces. The research regarding tools to implement human rights to comprehensively prevent trafficking and protect its victims highlights the weakness of the anti-trafficking framework alone. In particular, other frameworks can be triggered to protect trafficked victims, intermediated by state law and implemented by digital actors. Thus, "*here, the law is a militant weapon [as it is] used […] in support of a cause*."[1] The law is the current tool to establish values that are traditionally defined by states and internalized by digital actors, but law alone does not implement rights. Digital affordances are required to practically offer opportunities to victims. This highlights a current "*overconfidence in exactly how much can be achieved by law—particularly when it comes to meeting the needs of victims*."[2] This interconnection of sovereigns to reach a comprehensive repression of trafficking goes further than questioning the order of their coercion. Independence supports criminal law when the status of digital actors as sovereigns is denied, and it supports a division between digital actors and states in implementing human rights under the corporate social

[1] The concept is applied in the original text to laws on slavery, J.-P. Jean, "La mémoire du crime dans les deux lois de déclaration relative au génocide des Arméniens et à l'esclavage," *in* Institut de sciences criminelles de Poitiers, M. Danti-Juan (eds.), *La mémoire et le crime: dix-huitièmes Journées d'étude de l'Institut de sciences criminelles de Poitiers, vendredi 18 et samedi 19 juin 2010*, Éditions Cujas, Travaux de l'institut de sciences criminelles de Poitiers no. 27, 2011, p. 196

[2] N.A. Vincent, E.A. Jane, "Beyond law Protecting victims through engineering and design," *in* E. Martellozzo, E.A. Jane (eds.), *Cybercrime and its Victims*, Routledge, 1st ed., June 26, 2017, pp. 210-211

responsibility framework. Even so, the acknowledgment of independence is insufficient to interlink sovereigns' obligations and connect them to individuals' human rights, capabilities, and agency. Consequently, interdependence arises as a necessary basis for legitimate sovereign coercion under the current societal architecture. Instead of offering its content, due to the lack of a theory on interdependence, this study proposes a methodology to implement it, particularly to repress human trafficking. This methodology is grounded in the definition of interdependent core values, which could be human rights (or not). However, interdependent values are not enough, as their implementation depends on context and local interpretation, which are a way to maintain and protect sovereigns' independence. To achieve this aim, bridges between actors will be needed to legitimize coercion resulting from the balancing of these values.

GENERAL CONCLUSION

577. Cyber human trafficking: a case study for sovereignty. The offense of human trafficking, based on a process in which the consent of victims is nullified to lead to their exploitation, is facilitated by new technologies. Instead of a conclusion, this empirical statement was selected as a case study to explore an older legal theory: sovereignty. Indeed, as the repression of this phenomenon must adapt, new sources of coercion appear, and various types of relationships are to be drawn between them. The investigation and prosecution of cyber human trafficking faces all the challenges found in the investigation and prosecution of cybercrimes in general: territorial and extraterritorial jurisdiction, appropriate investigative techniques, procurement of electronic evidence, data retention, encryption, et cetera. Its purpose for exploitation and the potential violation of each and every human right of the victims make its repression a priority in many states and by many supranational organizations. Cyber human trafficking triggers the states' duty to protect and calls upon legal scholars to implement the theory of sovereignty. This theory, which was developed for states, gains additional perspectives as a result of challenges arising from new technologies, including digital sovereignty, under which states should maintain control over data and technologies. To achieve this aim, the state can exercise a new element of its monopoly on legitimate coercion: digital coercion. However, this exercise seems compromised as it is used in repressing cyber human trafficking.

578. Designating sovereigns. If the theory of sovereignty is linked to the exercise of coercion, it can then be disconnected from the state. This disconnection clearly appears as a result of the limits of the state's implementation. Regarding the repression of human trafficking, few prosecutions question jurisdiction, while cyber trafficking will increasingly challenge prosecution due to the commission of various elements through cyberspace. More interestingly, states have developed digital investigative techniques to adapt their response to crimes that are evolving through new technologies. While criminal procedure can still be found at the core of national sovereignty, the studied states rely on similar frameworks that are driven by the current state of technology and, thus, are highly limited by its evolution. Nevertheless, these amendments face various supranational and national legal requirements for the protection of the right to privacy

and the principle of due process. This study highlighted the limited quality of the drafting of the law, which is meant to solve a particular problem instead of considering the larger picture. Furthermore, the adaptation of the law is necessary, but its implementation requires material and human resources. Consequently, the theory of sovereignty faces pragmatic limitations, but the procurement of digital evidence remains at the core of prosecuting cyber human trafficking. Due to the restrictions on the implementation of state coercion, cooperation with other entities is needed. While cooperation with the business sector is still poorly developed by the anti-trafficking frameworks, digital actors here appear as core partners to repress human trafficking, and through the processing and control of data, they are able to exercise coercion. While digital actors were originally linked to states through their headquarters, the understanding of the complexities of worldwide data processing led to the evolution of this linkage. Through the location of the market, established particularly by users, digital actors are disconnected from one state and linked to various others. Supranational frameworks that are dedicated to the procurement of electronic evidence are increasingly recognizing the independence of digital actors by reducing traditional mutual legal assistance. Further independence is obtained by digital actors once states retreat regarding the regulation of digital elements, such as data retention and encryption, despite the fact that these are core challenges to the repression of cyber trafficking. Thus, by pragmatically acknowledging the power of digital actors to exercise or not to exercise coercion through their control over data and their increased level of independence in doing so, they appear to fit into a definition of sovereignty disconnected from states. Nonetheless, states are still sovereign, and, various sovereign entities coexist.

579. Ordering sovereigns. Once different types of entities are sovereign and are involved in repressing cyber human trafficking, these entities need to be ordered. A first reaction from traditional sovereigns—states—has been an attempt to control digital actors through their ultimate sovereignty power: criminal law. Indeed, as online services facilitate human trafficking, the owners of these were considered potential perpetrators of the crime. Benefiting from increasingly broader frameworks on corporate criminal liability, digital actors were not the primary perpetrators of trafficking, but because they facilitate the process, they were seen as bearing some responsibility. This responsibility appears to be social, as extralegal strategies, such as the closure of websites or a change in their terms of service, were developed mainly in the United

States to reach their goal without convictions. Therefore, digital actors internalized that they had to actively participate in the repression of human trafficking. However, this questions not only the independence of digital actors as new sovereigns but also the independence of other states. As technologies embed values and political choices, an application of the American perspective on the repression of human trafficking and the regulation of sex work threatens the autonomy of foreign states. Nonetheless, both the current frameworks on human rights and on personal data are not adapted to strengthen European sovereignties to face these threats. Consequently, imposing coercion between sovereigns both hinders the independent exercise of coercion and, thus, their sovereignty, and the effective repression of human trafficking. As a second option, collaboration between sovereigns arises as a strategy to protect each other's sovereignty and to seek a comprehensive repression of cyber trafficking. Even so, corporate social responsibility frameworks were not designed to consider the specific challenges of cyber human trafficking, and their force of obligation and control are limited. Digital social responsibility does not focus on human trafficking at all. Still, transparency and cooperation obligations and controls are more stringent, leading to a potential Brussels Effect. However, under this legal mindset, collaboration continues to have a limited impact on trafficked victims. Broadening the role of digital actors requires moving beyond a security perspective and implementing human rights through pragmatic affordances. Outside the realm of criminal law, digital actors may have obligations that are useful to helping trafficked victims through their control over the data. Here, the state appears as an intermediary in the implementation of human rights, while digital actors are the actual enforcers. Thus, "*the normative order of the internet […] is communal as it relies on legitimacy-enhancing norm-making processes that encompass all actors and provide them with a collective frame of reference*."[1] This collaborative setting acknowledges different coercion power while protecting rule-of-law standards. Furthermore, this setting questions the basis of the theory of sovereignty.

580. Rethinking the criteria for sovereignty. As a result, collaboration among various types of actors is at the core of preventing and repressing complex offenses that are facilitated by globalization and digitalization, such as cyber human trafficking.

[1] M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020, p. 323

Nonetheless, the theory of sovereignty has been based, since its origins, on independence and the lack of interference from other entities. However, this criterion hampers a comprehensive response to trafficking as well as the coercive powers of the different sovereigns. Independence is still required to negatively delimit sovereignty; it sets its restrictions. For instance, states and digital actors, on some topics and in some spaces, should still be independent in establishing norms. Even so, their powers should also be limited by individual or collective human rights. Independence alone is not sufficient to implement and legitimize norms, particularly human rights and anti-trafficking frameworks. Therefore, to develop an appropriate theory on sovereignty, considering society's evolution, a new criterion could be used to ground the legitimacy of sovereign actors: interdependence. This collaboration between states and digital actors offers various legal tools to protect and establish the rule-of-law principles defended by democratic societies. As for independence, interdependence as a general concept could be supported by the research of into a general theory (especially shared general values) and concrete tools, processes, and norms for its implementation, such as by establishing processes to build bridges between the different actors in society. This approach of sovereignty to interdependence leads to three comments.

581. Thoughts on the repression of human trafficking. The repression of cyber human trafficking requires many legal frameworks, some of which are disconnected from this specific topic. First, this result questions the strategy of various countries to adopt one comprehensive law to repress human trafficking.[2] This strategy aims to regulate all aspects of the repression of human trafficking and the protection of its victims in one legal instrument. This strategy recognizes the necessary interdisciplinary characteristic of the fight against trafficking, in particular, the need to go beyond criminal law. It aims to gather all victims' rights under one framework to obtain a clearer picture instead of various specific rights scattered among a number of laws and codes. Nevertheless, this study highlights that assistance and protection for trafficked victims should not be limited to their status as victims within the criminal process. Specifically, the repression of cyber trafficking underlines the importance of strengthening the

[2] See, for instance, in Spain, P. Lloria García, "El delito de trata de seres humanos y la necesidad de creación de una ley integral," *Estudios Penales y Criminológicos*, June 22, 2019, vol. 39, p. 353; C. Villacampa Estiarte, "¿Es necesaria una ley integral contra la trata de seres humanos?," *Revista General de Derecho Penal*, Iustel, 2020, no. 33, p. 16; Ministerio de Justicia et al., Anteproyecto de Ley Orgánica integral contra la trata y la explotación de seres humanos, 2022

protection of their victims' personal data and their control over their online environment. It could then seem superficial to limit the anti-trafficking framework to a comprehensive law. Furthermore, most challenges to the repression of cyber trafficking and to the protection of its victims are not exclusive to this offense: An improvement of the legal framework only to repress human trafficking might not be adequate, as law enforcement authorities face the same obstacles when investigating child pornography, cyber security threats, and organized crime in general.[3] Additionally, victims of forced labor, slavery, domestic violence, and rape might face challenges similar to those confronting trafficked victims. Second, this study questions the element at the core of the violation of human rights within the offense of human trafficking: the exploitation of people. This concept led to linking slavery and human trafficking under supranational case law, although without providing a definition.[4] Historically, slavery was organized, funded, and legally validated by states. It was a legal regime for the management of certain human beings.[5] It is noteworthy that the 1926 Slavery Convention does not criminalize such a legal state regime; rather, it obliges states to "*prevent and suppress the slave trade*."[6] In other words, it represses the intermediary entities who conduct, in practice, the process to obtain slaves. Even then, the criminalization of the process leading to slavery led to international pressure to abolish laws on slavery. Today, however, no law exists to validate the status of trafficked victims.[7] Thus, the criminalization of human trafficking could not have been created to pressure foreign countries to abolish a legal regime. Even so, criminalization hardly succeeds in preventing exploitation, as it is widely occurring in private settings. As states struggle to initiate supranational labor and social security standards, even within the ILO and the EU, the framework to repress trafficking, particularly when facilitated by new technologies, turns to new private actors who have leverage to prevent

[3] Similarly critcizing the multiplication of sectorial laws, see C. Villacampa Estiarte, "Acerca del Anteproyecto de Ley Orgánica Integral contra la Trata y la Explotación de Seres Humanos," *Diario La Ley*, Wolters Kluwer, 2023, no. 10267, p. 1

[4] M. Jovanovic, "The Essence of Slavery: Exploitation in Human Rights Law," *Human Rights Law Review*, December 9, 2020, vol. 20, no. 4, p. 685

[5] Even after the abolition of slavery, certain legal regimes, such as in French colonies, validated the exploitation of human beings, for instance, through forced labor, J.-P.L. Crom, *Histoire du droit du travail dans les colonies françaises (1848-1960)*, Rapport de recherche, halshs-01592836, Mission de recherche Droit et Justice, January 11, 2017, pp. 16-27

[6] Article 2.a of the Slavery Convention

[7] Although some legal frameworks might limit the protection of actual and potential victims, in particular regarding migration and the protection of trafficked victims subject to their cooperation with law enforcement authorities. On this topic, see J. O'Connell Davidson, "Absolving the State: the Trafficking-Slavery Metaphor," *Global Dialogue*, Summer/Autumn 2012, vol. 12, no. 2, pp. 31-41

exploitation. While slavery was implemented by states, international public law was partly adapted to pressure for its abolition. Still, the evolution of exploitation and the role of private actors in human trafficking highlight the limitations of the current standards of international public law, which are restricted to traditional sovereigns. As the repression of trafficking and diverse forms of exploitation increasingly reach private actors as enforcers of norms and values, it might be time to develop and legally define the notion of exploitation.[8] Third, this study questions, at the core of the prevention of cyber human trafficking, the necessity of this offense. It was created as a framework to facilitate state cooperation for mutual legal assistance and migration control. However, the prevention of cyber human trafficking questions core vulnerabilities in society, which do not always lead to trafficking. This offense is still a fuzzy concept, often not understood by people not who are not involved in the anti-trafficking framework, despite numerous awareness campaigns over the past many years. Thus, one solution among many to prevent trafficking would be to disconnect from the anti-trafficking framework. This disconnection would offer a more global picture and rely on actions for collective and individual empowerment. Indeed, "*Human trafficking is dependent on, and intertwined with, other systems of oppression. […] Addressing poverty is anti-trafficking work; addressing homelessness is anti-trafficking work; addressing racism is anti-trafficking work*."[9] For instance, improving digital literacy; safe, legal, and widely shared migration processes; sexual and affective education; mental health; the prevention and repression of early human rights violations, particularly within families; a culture of respect and consent; and the development of life opportunities, et cetera, could support the prevention of human trafficking. These actions cannot replace the need to develop actions to protect victims and prosecute traffickers, and individual actions cannot replace overall management of the structural and diverse causes of trafficking. Nonetheless, among the preventive actions, the adoption of measures based on individual and, consequently, collective empowerment could result in more changes to society than mere anti-trafficking awareness-raising campaigns. These thoughts question both the role of human rights and law and their

[8] For a doctrinal proposition, see M. Jovanovic, "The Essence of Slavery," *op. cit.* note 4, pp. 692-703
[9] R. Konrad et al., *Perspectives on How To Conduct Responsible Anti-Human Trafficking Research in Operations and Analytics*, arXiv:2006.16445, ArXiv, December 21, 2022, p. 14, online http://arxiv.org/abs/2006.16445 (retrieved on February 10, 2023)

relationship with legal literacy and other types of norms and actions.

582. Thoughts on human rights. The multiplication of sources of coercive powers and sovereign entities questions their collaboration not only for the repression of human trafficking, but also, more generally, for the regulation and implementation of human rights. It leads nowadays to "*the absence of a clearly assignable authority as debtor of these rights*."[10] However, within the framework of cyberspace, there is apparently a change of mindset. Digital actors are usually seen as intermediaries to enable people's connection. Furthermore, the acknowledgment of interdependent sovereigns offers a new understanding of intermediation. On the one hand, digital actors appear as intermediaries in the implementation of human rights, originally protected by states and in favor of people as users. On the other hand, states are intermediaries for digital actors in front of people as users, by lending them guidance and tools to legitimize their actions. As a consequence, the "*global nature of human rights*" requires an effort beyond a "*statist approach*."[11] However, partly due to a traditional understanding of sovereignty and the mainly capitalist and neoliberal approach of the business sector, this interconnectedness lacks a general theory. In particular, "*international human rights law does not assign clear obligations to non-state actors*," and there is no "*institutionalized sharing of responsibilities among states for seeing that these duties were fulfilled, since no state acting independently could be expected to hold these powerful non-state actors accountable*."[12] Nevertheless, obligations to non-state actors, for now, are adopted only on a case-by-case basis, especially for the regulation of online life. Even so, a comprehensive protection of human rights requires moving beyond abstract provisions and deriving from them concrete steps to undertake their improvement. As the traditional democratic process is not applied or may not be applicable to digital actors, establishing this general theory and its processes for implementation would need to seek a new basis for legitimacy. Such a process would support, firsthand, a discussion on values, both as general guidance and at an individual and collective application level. For now, human rights "*express a properly Western belief system*," complemented by other structures of

[10] F. Ost, *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016, p. 494

[11] M. Iglesias Vila, "Subsidiarity, margin of appreciation and international adjudication within a cooperative conception of human rights," *International Journal of Constitutional Law*, April 1, 2017, vol. 15, no. 2, pp. 397-398; L. Ferrajoli, P.Andrés. Ibáñez, *Por una Constitución de la Tierra La Humanidad en la Encrucijada*, Trotta, Editorial S.A., 2022, p. 46

[12] A.E. Buchanan, *The heart of human rights*, Oxford University Press, 2013, pp. 283-284

oppression.[13] This necessarily constant feedback from the universal to case applications highlights that "*the idea of law cannot claim universality*" from a comprehensive legitimacy.[14] To define these values, new bridges could be and are built between actors with the hope of improving communication and common understanding. These bridges could support a "*relational view*" of human rights, based "*on the capacity of normative relations or transactions between persons to generate mutual effective claims duties and liberties*."[15]

583. Thoughts on law. While human rights are a general framework that lacks guidance for daily implementation, the concept of law is supposed to reach generality. However, this study on the legal tools to repress cyber human trafficking has highlighted a downgrade in the quality of the law as a general tool. The law is increasingly technical and sectorial.: Regimes are not comprehensively amended, leading to problems of interpretation, a lack of guarantees, and, in general, perhaps a reduction in the legitimate force of state law. First, this is partly due to "*technological determinism*," meaning that, when "*a technology enters society and allows for certain activities that place significant strains on social orders, [then] existing law and legal concepts are applied but fall short, and necessary changes are made to account for the new technological capabilities*."[16] Nevertheless, this methodology applied to legal research and amendments disregards "*the cultural and political interpretation of technology*."[17] Second, and as a consequence, as theorized by Emeric under the notion of "*fluid law*," law "*is, first of all, the product of a political discourse, an ideal of reformers, a marketing presentation of the law*."[18] The law is seen as a tool to solve social problems, and criminal law is usually the answer selected by states to address a specific problem. Digital actors use a "*lawfulness response […] to regain or retain legitimacy for their business in the face of accusations of injustice. It does so in part by collapsing the distinction between lawfulness and legitimacy in the company's actions.*

[13] A. Supiot, *Homo juridicus essai sur la fonction anthropologique du droit*, Éditions du Seuil, 2005, p. 283
[14] *Ibid.* p. 284
[15] D. Rodin, "Two Visions of Human Rights: Relational and Beneficiary-Focused Theories," *in* D. Akande et al. (eds.), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment*, Oxford University Press, January 30, 2020, p. 76
[16] M. Jones, "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw," *Journal of law, technology & policy*, 2018, vol. 2, p. 103
[17] *Ibid.* p. 112
[18] N. Emeric, "Droit souple + droit fluide = droit liquide. Réflexion sur les mutations de la normativité juridique à l'ère des flux," *Revue interdisciplinaire d'études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, no. 2, p. 33

This separates out unlawful/illegitimate actions from lawful/legitimate ones."[19] The law is magnified as a solution, particularly to challenges derived from new technologies. However, this legal solutionism, taken to its extreme, forgets about other systems and spaces for the regulation of behaviors, such as education or the structuration of cyberspace. It also tends to hide the fact that "*claims of injustice often arise from the ways that existing law structures patterns of exchange and establishes a particular distribution of power among actors*."[20] This can be underlined by the following question: "*Are we confusing a technical tool with the culture that uses it for harm?*"[21] If other sources of norms and policies, including private ones, have a potential coercion on people, legal scholars might want to extend their perspective outside of positive state law. If the law is one tool aimed at promoting values, ordering society, and solving social challenges, its comprehensive study may not want to omit the acknowledgment of the reality of its implementation, the impact of preexisting social and economic structures, and the necessary flexibility to keep pace with society.

[19] S. Viljoen, "The Promise and Limits of Lawfulness: Inequality, Law, and the Techlash," *Journal of Social Computing*, September 2021, vol. 2, no. 3, p. 6
[20] *Ibid.* p. 7
[21] K. Maltzahn, *Digital dangers Information & communication technologies and trafficking in women*, APC-200608-WNSP-I-EN-P-0024, Association for progressive communications, Issue Papers, August 2006, p. 2

ANNEX: POSITIONING STATEMENT

While science and the production of scientific knowledge are required to the standard of scientific integrity, this standard tends to hide biases, and ignore that "*the governing rules*" "*for theories, for legal arguments, for scientific proofs*" are set by a "*dominant culture*."[1] When science, including the legal discipline, was found to be sexist, racist, homophobic, etc.[2], epistemology appeared as a tool to offer new perspectives on scientific results. To achieve this aim, those need to be situated in their original context. Indeed, "*because persistent patterns of power, based on lines of gender, racial, class, and age differences, have remained resilient and at the same time elusive under traditional political and legal ideas, arguments for looking to context carry critical power*."[3]

Thus, I recognize how relevant it is to facilitate situated knowledge[4]. I identify myself as a white, upper-middle-class woman with a non-normative sexual orientation and a high level of education. I developed this research during my mid-20s. I might be French, but I have been living in different countries (Spain, Vietnam, Romania) and traveling in various others. I moved many times already in my young life, voluntarily although pushed by the opportunities offered to me. I am also a digital native, and I have experienced the advantages and some risks it conveys. I undertook my research with the aim of feeding a better understanding of the complexities around the notions of choice and coercion, labor and exploitation, because such notions impact the individual, while being framed by the structures set by macro entities such as states and digital actors. I believe all of these facts have played a part in the creation of this research, in the focalization of its findings, and in my writing.

[1] M. Minow, "Feminist Reason: Getting It and Losing It [1988]," *in* K.T. Bartlett, R.T. Kennedy (eds.), *Feminist legal theory: readings in law and gender*, Westview Press, New perspectives on law, culture, and society, 1991, p. 360
[2] S.G. Harding, *The science question in feminism*, Cornell University Press, 1986, p. 20
[3] M. Minow, E.V. Spelman, "In Context - Symposium on the Renaissance of Pragmatism in American Legal Thought," *Southern California Law Review*, 1990 1989, vol. 63, no. 6, p. 1651
[4] D.J. Haraway, *Simians, cyborgs, and women: the reinvention of nature*, Routledge, 2015, p. 183

BIBLIOGRAPHY

§1. Books

AGNEW J.A., *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018.

AGUSTÍN L.M., *Sex at the margins: migration, labour markets and the rescue industry*, Zed Books, 2nd ed., 2008.

ALBALADEJO GARCIA M. (ed.), *Normas de Derecho internacional privado. Ambito de aplicación de los regímenes jurídicos civiles españoles*, Edersa, Comentarios al código civil y compilaciones forales, 2nd ed., 1992.

ALEMANY JORDÁN M., *La violencia contra las mujeres en los desastres, pandemias y otras emergencias humanitarias*, Tirant lo Blanch, Derechos humanos, 1st ed., 2022.

AMILHAT SZARY A.-L., *Qu'est-ce qu'une frontière aujourd'hui ?*, Presses Universitaires de France, 2015.

ANDERSON B., *Imagined communities: reflections on the origin and spread of nationalism*, Verso, Revised ed, 2006.

ANDRIJASEVIC R., *Migration, agency, and citizenship in sex trafficking*, Palgrave Macmillan, Migration, minorities and citizenship, 2010.

ANTONOPOULOS G., BARATTO G., DI NICOLA A., *Technology in human smuggling and trafficking: case studies from Italy and the United Kingdom*, Springer, Springerbriefs in criminology, 2020.

ARONOWITZ A., *Human trafficking, human misery: the global trade in human beings*, Praeger Publishers Inc, 1st ed., 2009.

BALES K., *Disposable people new slavery in the global economy*, University of California Press, 2012.

BANERJEE S.B., *Corporate social responsibility: the good, the bad and the ugly*, Edward Elgar, 2007.

BAUMAN Z., *Liquid times: living in an age of uncertainty*, Polity Press, 2007, 115 pages.

BEAUD O., *La puissance de l'Etat*, Presses universitaires de France, Léviathan, 1st ed., 1994.

BELLANGER P., *La souveraineté numérique*, Stock, 2014.

BELLIDO PENADÉS R., *La captación de comunicaciones orales directas y de imágenes y su uso en el proceso penal (propuestas de reforma)*, Tirant lo Blanch, 2020.

BENEDEK W., KETTEMANN M.C., *Liberté d'expression et internet*, Conseil de l'Europe, 2014.

BENJAMIN R., *Race after technology: abolitionist tools for the new Jim code*, Polity, 2019.

BERNARDO PANIAGUA J.M. et al. (eds.), *Retos de la comunicación ante la violencia de género: marco jurídico, discurso mediático y compromiso social*, Tirant lo Blanch, Monografías no. 656, 2009.

BERNSTEIN E., *Temporarily Yours: Intimacy, Authenticity, and the Commerce of Sex*, University of Chicago Press, November 1, 2007.

BIEGEL S., *Beyond our control? Confronting the limits of our legal system in the age of cyberspace*, MIT Press, 2001.

BODIN J., *Les six livres de la République - Un abrégé du texte de l'édition de Paris de 1583*, Librairie générale française, Le livre de poche - Classiques de la philosophie no. 4619, 1993.

BOURDIN-REVUZ A., *Le numérique, locomotive de la 3e révolution industrielle?*, Ellipses, 2013.

BOYD d., *It's complicated: the social lives of networked teens*, Yale University Press, 2014.

BRADFORD A., *The Brussels effect: how the European Union rules the world*, Oxford University Press, 2020.

BRATTON B.H., *The stack: on software and sovereignty*, MIT Press, Software studies, 2015.

BROUSSARD M., *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018.

BROWN S.S., HERMANN M.G., *Transnational Crime and Black Spots Rethinking Sovereignty and the Global Economy*, Palgrave MacMillan, International Political Economy Series, 2020.

BROWN I., MARSDEN C.T., *Regulating code: good governance and better regulation in the information age*, The MIT Press, Information revolution and global politics, 2013.

BUCHANAN A.E., *The heart of human rights*, Oxford University Press, 2013.

BUENO DE MATA F., *Las diligencias de investigación penal en la cuarta revolución industrial: principios teóricos y problemas prácticos*, Thomson Reuters Aranzadi, Aranzadi derecho penal no. 1151, Primera edición, 2019, 2019.

BYGRAVE L.A., *Internet governance by contract*, Oxford University Press, 1st ed., 2015.

CABANES FERRANDO M., *La trata de seres humanos: concepto desde el marco normativo: una aproximación al delito*, J.M. Bosch Editor, 2022.

CARBONNIER J., *Flexible droit: pour une sociologie du droit sans rigueur*, Librairie Générale de Droit et de Jurisprudence, 7th ed., 1992.

CASTELLS M., *La sociedad red*, Alianza Editorial SA, La era de la información: economía, sociedad y cultura, June 30, 2005, vol. 1.

CHAUMONT J.-M., MACHIELS C., *Du sordide au mythe: l'affaire de la traite des Blanches (Bruxelles, 1880)*, Presses universitaires de Louvain, Histoire, justice, sociétés, 2009.

CHAWKI M., *La traite des êtres humains à l'ère numérique*, Éditions de Saint-Amans, 2010.

CHEVALLIER J., *L'État de droit*, LGDJ, Clefs, 6th ed., 2017.

CHEVALLIER J., JACQUES C., *L'État post-moderne*, LGDJ, 4th ed., 2017.

CLAPHAM A., *Human rights obligations of non-state actors*, Oxford University Press, The collected courses of the Academy of European Law no. v. 15/1, 2006.

COCKBAIN E., *Offender and Victim Networks in Human Trafficking*, Taylor & Francis Ltd, 2020.

COHEN J.E., *Between truth and power: the legal constructions of informational capitalism*, Oxford University Press, 2019.

COHEN J.L., *Globalization and sovereignty: rethinking legality, legitimacy and constitutionalism*, Cambridge University Press, 2012.

COLE M.D., ETTELDORF C., ULLRICH C., *Updating the Rules for Online Content Dissemination - Legislative Options of the European Union and the Digital Services Act Proposal*, Nomos Verlagsgesellschaft mbH & Co. KG, 2021.

CRAWFORD K., *Atlas of Ai: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021.

CRIADO-PEREZ C., *Invisible women: data bias in a world designed for men*, Abrams Press, 2019.

DAUVERGNE C., *Making people illegal: what globalization means for migration and law*, Cambridge University Press, Law in context, 2008.

DAVID M., *La souveraineté du peuple*, Presses universitaires de France, Questions, 1st ed., 1996.

DE GREGORIO G., *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge University Press, Cambridge studies in European law and policy, 2022.

DE VIDO S., *Violence against women's health in international law*, *Violence against women's health in international law*, Manchester University Press, June 12, 2020.

DEBARD T., GUINCHARD S., *Lexique des termes juridiques 2021-2022*, Dalloz, Lexiques, 29th ed., 2021.

DELMAS-MARTY M., *Le relatif et l'universel*, Éditions du Seuil, Les forces imaginantes du droit no. 1, 2004.

DELMAS-MARTY M., *Résister, responsabiliser, anticiper, ou, Comment humaniser la mondialisation*, Seuil, 2013.

DELMAS-MARTY M., *Trois défis pour un droit mondial*, Seuil, Seuil essais, 1998.

DELMAS-MARTY M., *Libertés et sûreté dans un monde dangereux*, Seuil, La couleur des idées, Éditions du seuil, 2010.

DELMAS-MARTY M., *Le flou du droit: du code pénal aux droits de l'homme*, Presses universitaires de France, Les Voies du droit, 1st ed., 1986.

DELMAS-MARTY M., *Le pluralisme ordonné*, Éditions du Seuil, Les forces imaginantes du droit no. 2, 2004.

DELMAS-MARTY M., *La refondation des pouvoirs*, Éditions du Seuil, Les forces imaginantes du droit no. 3, 2007.

DONNEDIEU DE VABRES H., *Les principes modernes du droit pénal international*, Editions Panthéon-Assas, 2005.

FERAL-SCHUHL C., *Cyberdroit: le droit à l'épreuve de l'Internet*, Praxis Dalloz, Dalloz, 2020.

FERRAJOLI L., IBÁÑEZ P.Andrés., *Por una Constitución de la Tierra La Humanidad en la Encrucijada*, Trotta, Editorial S.A., 2022.

FORRAY V., PIMONT S., *Décrire le droit... et le transformer: essai sur la décriture du droit*, Dalloz, 2017.

FURNELL S., *Cybercrime: vandalizing the information society*, Addison-Wesley, A Pearson Education book, 1st ed., 2002.

GALLAGHER A., *The international law of human trafficking*, Cambridge University Press, 2010.

GARAPON A., LASSEGUE J., *Justice digitale: révolution graphique et rupture anthropologique*, Presses universitaires de France, 1re édition, 2018.

GARAPON A., SERVAN-SCHREIBER P. (eds.), *Deals de justice: le marché américain de l'obéissance mondialisée*, Presses universitaires de France, 2013.

GILLESPIE T., *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*, Yale University Press, 2018.

GOLDSMITH J.L., WU T., *Who controls the Internet? Illusions of a borderless world*, Oxford University Press, 2006.

GOLTZBERG S., *Le droit comparé*, Presses Universitaires de France, Que sais-je ?, 2018.

GÓMEZ TOMILLO M., *Introducción a la responsabilidad penal de las personas jurídicas*, Thomson Reuters Aranzadi, Colección Monografías Aranzadi Aranzadi derecho penal no. 768, Segunda edición, 2015.

GUINCHARD S. et al., *Lexique des termes juridiques*, Dalloz, Lexiques, 28th ed., 2020.

HABERMAS J., *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*, MIT Press, Studies in contemporary German social thought, 1989.

HARAWAY D.J., *Simians, cyborgs, and women: the reinvention of nature*, Routledge, 2015.

HARDING S.G., *The science question in feminism*, Cornell University Press, 1986.

HERNERT P., *Les algorithmes*, Presses universitaires de France, 2002.

HERZOG D., *Sovereignty, RIP*, Yale University Press, 2020.

HUSOVEC M., *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?*, Cambridge University Press, Cambridge Intellectual Property and Information Law, 2017.

GINDRE E., *L'émergence d'un droit pénal de l'Union européenne*, Fondation Varenne, LGDJ, Collection des thèses no. 31, 2009.

JULIA L., KHAYAT O., *L'intelligence artificielle n'existe pas*, First éditions, 2019.

KANT I. et al., *Idée d'une histoire universelle au point de vue cosmopolite*, Gallimard, 2009.

KENWAY E., *The truth about modern slavery*, Pluto Press, 2021.

KETTEMANN M., *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020.

KOTISWARAN P., *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017.

LASTOWKA F.G., *Virtual justice: the new laws of online worlds*, Yale University Press, 2012.

LAVAUD-LEGENDRE B., *Où sont passées les bonnes mœurs?*, Presses universitaires de France, Collection "Partage du savoir," 2005.

LESSIG L., *Code*, Basic Books, 2nd ed., 2006, 410 pages.

LHUILIER G., *Le droit transnational*, Dalloz, Méthodes du droit, 2016.

LISTER R., *Citizenship: feminist perspectives*, Palgrave Macmillan, 2nd ed., 2003.

LLORIA GARCÍA P., *Violencia sobre la mujer en el siglo XXI: Violencia de control y nuevas tecnologías: habitualidad, sexting y stalking*, Iustel, 1st ed., 2020.

LOCKE R.M., *The Promise and limits of private power: promoting labor standards in a global economy*, Cambridge University Press, Cambridge studies in comparative politics, 2013.

MACKINNON R., *Consent of the Networked. The worldwide struggle for internet freedom*, Basic Books, 2017.

MAGRO SERVET V., *Guía práctica sobre responsabilidad penal de empresas y planes de prevención (compliance)*, La Ley, 2017.

MAINSANT G., *Sur le trottoir, l'État: la police face à la prostitution*, Éditions du Seuil, La Couleur des idées, 2021.

MANTELERO A., *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, T.M.C. Asser Press; Springer, Information Technology and Law Series, 2022, vol. 36.

MENECEUR Y., *L'intelligence artificielle en procès: Plaidoyer pour une réglementation internationale et européenne*, Bruylant, 2020.

MERABET S., BARBIER H., *Vers un droit de l'intelligence artificielle*, Dalloz, Nouvelle Bibliothèque de Thèses, 2020, vol. 197.

MOROZOV E., *To save everything, click here: the folly of technological solutionism*, PublicAffairs, 1st ed., 2013.

MUÑOZ VELA J.M., *Cuestiones éticas de la Inteligencia Artificial y repercusiones jurídicas: de lo dispositivo a lo imperativo*, Thomson Reuters Aranzadi, 1st ed., 2021.

NISSENBAUM H.F., *Privacy in context: technology, policy, and the integrity of social life*, Standford University Press, 2010.

NOBLE S.U., *Algorithms of oppression: how search engines reinforce racism*, New York University Press, 2018.

NUSSBAUM M.C., *Creating Capabilities – The Human Development Approach*, Harvard University Press, 2013.

NUSSBAUM M.C., *Women and human development: the capabilities approach*, Cambridge University Press, 2000.

ORTEGO RUIZ M., *Prestadores de servicios de Internet y alojamiento de contenidos ilícitos*, Reus, Colección de propiedad intelectual, 1st ed., 2015.

OST F., *A quoi sert le droit ? Usages, fonctions, finalités*, Bruylant Edition, Penser le droit no. 25, 2016.

OST F., KERCHOVE M. Van de, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications des facultés universitaires Saint-Louis, 2010.

OTAMENDI ZOZAYA F., *Las últimas reformas de la ley de enjuiciamento criminal una visión práctica tras un año de vigencia*, Dykinson, 2017.

PAASONEN S. et al., *Objectification: on the difference between sex and sexism*, Routledge, Gender insights, 2020.

PAASONEN S., JARRETT K., LIGHT B., *NSFW: sex, humor, and risk in social media*, The MIT Press, 2019.

PANSIER F.-J., JEZ E., *La criminalité sur l'internet*, Presses universitaires de France, 2001.

PARISER E., *The filter bubble: how the new personalized web is changing what we read and how we think*, Penguin Books, 2014.

PASQUALE F., *The black box society: the secret algorithms that control money and information*, Harvard University Press, 2015.

PEGUERA POCH M., *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Derecho de la sociedad de la información no. 15, 2007.

PETERS A.W., *Responding to human trafficking - sex, gender, and culture in the law*, University of Pennsylvania Press, Pennsylvania Studies in Human Rights, 2015.

PLOUFFE-MALETTE K., *La protection des victimes de traite des êtres humains: approches internationales et européennes*, Bruylant, Mondialisation et droit international no. 25, 2013.

POMARES CINTAS E., *El Derecho Penal ante la explotación laboral y otras formas de violencia en el trabajo*, Tirant lo Blanch, Monografías, 2013, vol. 822.

PRICE M.E., *Media and sovereignty: the global information revolution and its challenge to state power*, MIT Press, 2002.

QUEMENER M., *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018.

RAUFER X., *Cyber-criminologie*, CNRS Éditions, 2015.

ROBERTS S.T., *Derrière les écrans*, La Découverte, October 15, 2020.

ROQUES-BONNET M.-C., *Le droit peut-il ignorer la révolution numérique*, Michalon Editions, 2010.

ROSANVALLON P., *La contre-démocratie: la politique à l'âge de la défiance*, Seuil, Les livres du nouveau monde, 2006.

SALAS D., *La volonté de punir : essai sur le populisme pénal*, Hachette littératures, 2008.

SANDERS T. et al., *Internet sex work - Beyond the gaze*, Springer Berlin Heidelberg, 2017.

SANDERS T., BRENTS B.G., WAKEFIELD C., *Paying for sex in a digital age: US and UK perspectives*, Routledge, 2020.

SHAPIRO A.L., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Century Foundation, May 15, 2000.

SHELLEY L., *Human trafficking A global perspective*, Cambridge University Press, 2010.

SIMON J., *Governing through crime: how the war on crime transformed American democracy and created a culture of fear*, Oxford University Press, Studies in crime and public policy, 2007.

SLAUGHTER A.-M., *A new world order*, Princeton University Press, 2004.

SMITH M., MAC J., *Revolting prostitutes: the fight for sex workers' rights*, Verso, 2018.

SONTAG KOENIG S., *Technologies de l'information et de la communication et défense pénale*, Mare & Martin, Bibliothèque des thèses, 2016.

STARK E.D., *Coercive control: the entrapment of women in personal life*, Oxford University Press, Interpersonal violence, 2009.

STJERNFELT F., LAURITZEN A.M., *Your post has been removed: tech giants and freedom of speech*, SpringerOpen, 2020.

SUPIOT A., *Homo juridicus essai sur la fonction anthropologique du droit*, Éditions du Seuil, 2005.

SUPIOT A., *L'esprit de Philadelphie la justice sociale face au marché total*, Seuil, 2010.

TIIDENBERG K., NAGEL E. Van der, *Sex and social media*, 2020.

VAIDHYANATHAN S., *The googlization of everything: and why we should worry*, University of California Press, Updated edition, 2012.

VELASCO NÚÑEZ E., SANCHÍS CRESPO C., *Delincuencia informática: tipos delictivos e investigación: con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, 2019.

WAGNER B., *Global Free Expression - Governing the Boundaries of Internet Content*, Springer International Publishing, Law, Governance and Technology Series no. 28, 1st ed., 2016.

WALKOWITZ J.R., *Prostitution and Victorian Society: Women, Class, and the State*, Cambridge University Press, 1980.

YORK J., *Silicon values: the future of free speech under surveillance capitalism*, Verso, 2021.

ZUGALDÍA ESPINAR J.M., *La responsabilidad criminal de las personas jurídicas, de los entes sin personalidad y de sus directivos: análisis de los arts. 31 bis y 129 del Código Penal*, Tirant lo Blanch, Collección delitos no. 95, 2013.

I. Manuals

BOULOC B., *Droit pénal général*, Dalloz, Précis, 27th ed., 2021.

BOULOC B., STEFANI G., LEVASSEUR G., *Procédure pénale*, Dalloz, Précis, 27th ed., 2020.

CHAMPEIL-DESPLATS V., *Méthodologies du droit et des sciences du droit*, Dalloz, Méthodes du droit, 2e édition, 2016.

CODRON C., *La surveillance diffuse : entre Droit et Norme*, Thesis, Université de Lille, June 15, 2018.

COMBACAU J., SUR S., *Droit international public*, LGDJ, 2014.

COSTES L., *Le Lamy, droit du numérique: guide : solutions et applications, pratique contractuelle*, Wolters Kluwer France, 2020.

LAURIER NGOMBE Y., *Fiches de droit du numérique: rappels de cours et exercices corrigés*, Ellipses, Fiches de, 2022.

MAYAUD Y., GAYET C., *Code pénal: annoté*, Dalloz, Codes Dalloz, 120th ed., 2022.

MELIN-SOUCRAMANIEN F., PACTET P., *Droit constitutionnel: 2021*, 2020.

MELÓN MUÑOZ A., *Procesal penal 2021*, Francis Lefebvre, Memento práctico, 2020.

PRADEL J., *Droit pénal comparé*, Dalloz, 2016.

REVERDY A., MATSOPOULOU H., MASCALA C., *Le Lamy, droit pénal des affaires*, Wolters Kluwer France, 2020.

TAMBOU O., LOPEZ AGUILAR J.F., *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, Droit administratif no. 28 28, 2020.

VERNY É., *Procédure pénale*, Dalloz, Cours Dalloz, 7th ed., 2020.

ZUGALDÍA ESPINAR J.M., MORENO-TORRES HERRERA M.R., *Lecciones de derecho penal: parte general*, 2021.

VALPUESTA GASTAMINZA E.M., HERNÁNDEZ PEÑA J.C. (eds.), *Tratado de Derecho Digital*, Wolters Kluwer Legal & Regulatory España, 2021.

II. Books chapters

AAS K.F., "Beyond 'the desert of the real': crime control in a virtual(ised) reality," *in* JEWKES Y. (ed.), *Crime online*, Willan, 2007, p. 160.

ABEL SOUTO M., "Blanqueo de dinero y responsabilidad penal de las personas jurídicas," *in* DEL VICENTE REMESAL J., BACIGALUPO ZAPATER E., LUZÓN PEÑA D.-M. (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, pp. 1421-1430.

ACIÉN GONZÁLEZ E., "Mujeres migrantes nigerianas. La realidad frente al relato trafiquista," *in* CORDERO RAMOS N., ZÚÑIGA CRUZ P. (eds.), *Trata de personas, género y migraciones en Andalucía (España), Costa Rica y Marruecos: retos y propuestas para la defensa y garantía de los derechos humanos*, Dykinson, 2019, p. 67.

ADHIKARI S.D., "Beyond dichotomies: Exploring responses to tackling the sex industry in Nepal," *in* DEWEY S., CROWHURST I., IZUGBARA C.O. (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 211-221.

ALBA CLADERA F., GARCÍA MARTÍNEZ G., "Blanqueo de capitales y agente encubierto en internet," *in* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 191-201.

ALBERS M., "Data Retention in Germany," *in* ZUBIK M., PODKOWIK J., RYBSKI R. (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 117-136, DOI:10.1007/978-3-030-57189-4_8.

ALBURY K., "Sexual Expression in Social Media," *in* BURGESS J., MARWICK A. (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 444.

ALCARAZ RAMOS M., "Preguntas de la explosión tecnológica del conocimiento a la política democrática y al derecho," *in* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 55-86.

ALDEN DINAN K., "Globalization and national sovereignty: From migration to trafficking," *in* CAMERON S., NEWMAN E. (eds.), *Trafficking in humans: social, cultural and political dimensions*, UN University Press, 2008, p. 58.

ALEJANDRA SUÁREZ M., "Diligencias de investigación tecnológicas. La licitud de la actividad probatoria de un dron," *in* BUENO DE LA MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L.M.

(eds.), *Fodertics 9.0: Estudios sobre tecnologías disruptivas y justicia*, Comares, 2021, pp. 393-403.

ALLAIN J., "Genealogies of human trafficking and slavery," *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 3.

ALPERT E.J., CHIN S.E., "Human Trafficking: Perspectives on Prevention," *in* CHISOLM-STRAKER M., STOKLOSA H. (eds.), *Human Trafficking Is a Public Health Issue: A Paradigm Expansion in the United States*, Springer International Publishing, 2017, pp. 379-400, DOI:10.1007/978-3-319-47824-1_22.

ALTINK S., VAN LIEMPT I., WIJERS M., "The Netherlands," *in* JAHNSEN S.Ø., WAGENAAR H. (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, p. 62.

ALVAREZ RUBIO J.J., YIANNIBAS K., "Conclusion," *in* ALVAREZ RUBIO J.J., YIANNIBAS K. (eds.), *Human rights in business: removal of barriers to access to justice in the European Union*, Routledge, 2017, p. 139.

ARRABAL PLATERO P., "El derecho fundamental al propio entorno virtual y su incidencia en el proceso," *in* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 431-441.

ASKOLA H., "Regional Responses to Human Trafficking in Southeast Asia and Australasia," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 901-915, DOI:10.1007/978-3-319-63058-8_92.

BACHMAIER WINTER L., "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: algunas cuestiones sobre el principio de proporcionalidad," *in* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017.

BADINTER R., "Conclusion," *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 331.

BALES K., GARDNER A., "Free Soil, Free Produce, Free Communities," *in* BLIGHT D.W., LEBARON G., PLILEY J.R. (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, pp. 73-96, DOI:10.1017/9781108902519.005.

BARANGER D., "The apparition of sovereignty," *in* KALMO H., SKINNER Q. (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 47.

BARFIELD W., "Towards a law of artificial intelligence," *in* BARFIELD W., PAGALLO U. (eds.), *Research handbook on the law of artificial intelligence*, Edward Elgar Publishing, 2018, p. 2.

BARRON I.M., FROST C., "Men, Boys, and LGBTQ: Invisible Victims of Human Trafficking," *in* WALKER L., GAVIRIA G., GOPAL K. (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 73-84, DOI:10.1007/978-3-319-73621-1_8.

BARTLETT K.T., "Feminist Legal Methods [1990]," *in* BARTLETT K.T., KENNEDY R.T. (eds.), *Feminist legal theory: readings in law and gender*, Westview Press, New perspectives on law, culture, and society, 1991, p. 370.

BASILIEN-GAINCHE M.-L., "Gouvernance et efficacité des normes juridiques," *in* FATIN-ROUGE STEFANINI M. et al. (eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?*, Bruylant, À la croisée des droits 6, 2012, p. 85.

BEAUVAIS P., "Les mutations de la souveraineté pénale," *in* COLLECTIF (ed.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 71.

BEAUVAIS P., “La nouvelle surveillance pénale,” *in* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l’honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 259-274.

BELLI L., ZINGALES N., “Online Platforms’ Roles and Responsibilities: a Call for Action,” *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 25.

BELTRÁN E., “Justicia, democracia y ciudadanía: las vías hacia la igualdad,” *in* BELTRÁN E., MAQUIEIRA V. (eds.), *Feminismos, debates teóricos contemporáneos*, Alianza Editorial, El Libro universitario no. 069, 2001, p. 189.

BERNSTEIN E., “Brokered Subjects and Sexual Investability,” *in* KOTISWARAN P. (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, pp. 329-358.

BLANCO CORDERO I., “Responsabilidad penal de la sociedad matriz por los delitos cometidos en el grupo de empresas,” *in* SUÁREZ LÓPEZ J.M. et al. (eds.), *Estudios jurídicos penales y criminológicos: en homenaje al Prof. Dr. Dr. H. C. Mult. Lorenzo Morillas Cueva*, Dykinson SL, 2018, p. 53.

BLUME C., RAUCHBAUER M., “How to Be a Digital Humanist in International Relations: Cultural Tech Diplomacy Challenges Silicon Valley,” *in* WERTHNER H. et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, pp. 101-107, DOI:10.1007/978-3-030-86144-5_15.

BOIZARD M., “La tentation de nouveaux droits fondamentaux face à Internet : vers une souveraineté individuelle ? Illustration à travers le droit à l’oubli numérique,” *in* BLANDIN-OBERNESSER A. (ed.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, pp. 31-55.

BOULON O., “Une justice négociée,” *in* GARAPON A., SERVAN-SCHREIBER P. (eds.), *Deals de justice: le marché américain de l’obéissance mondialisée*, Presses universitaires de France, 2013, p. 41.

BOWEN P., “Prosecution of cases of human trafficking in a common law system,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 213.

BOYD d., “Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life,” *in* BUCKINGHAM D. (ed.), *Youth, Identity, and Digital Media*, MIT Press, The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, January 4, 2008, pp. 119-142.

BOYD S.B., “1. Challenging the Public/Private Divide: An Overview,” *in* BOYD S.B. (ed.), *Challenging the Public/Private Divide*, University of Toronto Press, January 31, 1997, pp. 3-36, DOI:10.3138/9781442672819-003.

BRACH-THIEL D., “La compétence des juridictions pénales françaises face aux infractions commises via Internet,” *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

BRENNER S.W., “Cybercrime: re-thinking crime control strategies,” *in* JEWKES Y. (ed.), *Crime online*, Willan, 2007, p. 12.

BRIGANT J.-M., “Mesures d’investigation face au défi numérique en droit français,” *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

BROEDERS D., TAYLOR L., “Does Great Power Come with Great Responsibility? The Need to Talk About Corporate Political Responsibility,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 315-323, DOI:10.1007/978-3-319-47852-4_17.

BRUCKMÜLLER K., "Trafficking of Human Beings for Organ (Cells and Tissue) Removal," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 319-337, DOI:10.1007/978-3-319-63058-8_20.

BRUCKMÜLLER K., SCHUMANN S., "Crime Control versus Social Work Approaches in the Context of the '3P' Paradigm - Prevention, Protection, Prosecution," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 103.

BUENO DE MATA F., "El agente encubierto en Internet como instrumento para la lucha contra el 'child grooming' y el 'sexting,'" *in* BUENO DE MATA F. et al. (eds.), *Cambio de paradigma en la prevención y erradicación de la violencia de género*, Editorial Comares, Estudios de Derecho constitucional, 2017, pp. 3-16.

BUENO DE MATA F., "Peculiaridades probatorias del DRON como diligencia de investigación tecnológica," *in* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 169-204.

BUENO DE MATA F., "Análisis crítico de las futuras órdenes europeas en materia de prueba electrónica," *in* BUENO DE MATA F., GONZÁLEZ PULIDO I. (eds.), *La cooperación procesal internacional en la sociedad del conocimiento*, Atelier Libros Jurídicos, Processus iudicii no. 59, 2019, pp. 319-329.

BUSS D.E., "14. Going Global: Feminist Theory, International Law, and the Public/Private Divide," *in* BOYD S.B. (ed.), *Challenging the Public/Private Divide*, University of Toronto Press, January 31, 1997, pp. 360-384, DOI:10.3138/9781442672819-016.

CAHN O., "Les interactions normatives entre les régimes de common law et de droit romano-germanique," *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL, UBEDA-SAILLARD M. (eds.), *La souveraineté pénale de l'État au XXI^{ème} siècle*, Éditions Pedone, 2018, p. 77.

CAMERON H., "The New Raw Resources Passing Through the Shadows," *in* MALLOCH M., RIGBY P. (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 210-223.

CANCA C., "Did You Find It on the Internet? Ethical Complexities of Search Engine Rankings," *in* WERTHNER H. et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, pp. 135-144, DOI:10.1007/978-3-030-86144-5_19.

CARBONELL MATEU J.C., "La persona jurídica como sujeto activo del delito," *in* DEL VICENTE REMESAL J., BACIGALUPO ZAPATER E., LUZÓN PEÑA D.-M. (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70^{o} aniversario*, Reus, 2020, p. 523.

CASTELLÓ PASTOR J.J., "El alertador fiable como notificador de contenido ¿ilícito? en la red," *in* MARTÍNEZ NADAL A., AIGE MUT M.B., MARTÍ MIRAVALLS J. (eds.), *Plataformas digitales: aspectos jurídicos*, Aranzadi, Estudios, 1st ed., 2021, pp. 49-69.

BUCHER T., HELMOND A., "The Affordances of Social Media Platforms," *in* BURGESS J., MARWICK A. (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 234.

CASTETS-RENARD C., NDIOR V., RASS-MASSON L., "Introduction," *in* CASTETS-RENARD C., NDIOR V., RASS-MASSON L. (eds.), *Enjeux internationaux des activités économiques: entre logique territoriale des États et puissance des acteurs privés*, Larcier, Création, information, communication, 2020, p. 9.

CEDEÑO HERNÁN M., "Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos," *in* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017.

CHAPARRO MATAMOROS P., "La responsabilidad de los prestadores de servicios de la sociedad de la información," *in* MARTÍNEZ VÁZQUEZ DE CASTRO L., ESCRIBANO TORTAJADA P. (eds.),

Internet y los derechos de la personalidad: la protección jurídica desde el punto de vista del derecho privado, Tirant lo Blanch, Homenajes y congresos, 2019, pp. 99-142.

CHAPELLE B. de L., FEHLINGER P., "Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation," *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 726-748, DOI:10.1093/oxfordhb/9780198837138.013.38.

CHENG S., "A critical engagement with the 'pull and push' model Human trafficking and migration into sex work," *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 499.

CHOI K.-S., "Cyber-Routine Activities Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization," *in* JAISHANKAR K. (ed.), *Cyber criminology: exploring Internet crimes and criminal behavior*, CRC Press, 2011, p. 229.

CHRISTIE N., "The Ideal Victim," *in* FATTAH E.A. (ed.), *From Crime Policy to Victim Policy: Reorienting the Justice System*, Palgrave Macmillan UK, 1986, pp. 17-30, DOI:10.1007/978-1-349-08305-3_2.

CHURAKOVA I., VAN DER WESTHUIZEN A., "Human Trafficking in the Russian Federation: Scope of the Problem," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1071-1092, DOI:10.1007/978-3-319-63058-8_63.

COCKBAIN E., BOWERS K., VERNON L., "Using Law Enforcement Data in Trafficking Research," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1709-1732, DOI:10.1007/978-3-319-63058-8_100.

COHEN D., "Le juge européen et les données personnelles," *in* COLLECTIF (ed.), *L'exigence de justice: mélanges en l'honneur de Robert Badinter*, Dalloz, 2016, p. 249.

COPIĆ S., SIMEUNOVIĆ-PATIĆ M., "Victims of Human Trafficking Meeting Victims' Needs?," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 265.

CÓRDOBA MORENO S., "¿Son las bandas latinas en España crimen organizado?," *in* ZÚÑIGA RODRÍGUEZ L. (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, pp. 163-193.

CORRÊA DA SILVA W., "La interseccionalidad en la trata de seres humanos: un encuentro necesario para el enfoque de derechos humanos," *in* CORDERO RAMOS N., ZÚÑIGA CRUZ P. (eds.), *Trata de personas, género y migraciones en Andalucía (España), Costa Rica y Marruecos: retos y propuestas para la defensa y garantía de los derechos humanos*, Dykinson, 2019, p. 37.

CORTÉS BECHIARELLI E., "Límites a la extinción de la responsabilidad penal de la persona jurídica (CP art.130.2)," *in* JUANES PECES Á. (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 1100.

COUDERT F., VERBRUGGEN F., "Conservation des données de communications électroniques en Belgique : un juste équilibre ?," *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

D'ESTRÉE C., "Voices from Victims and Survivors of Human Trafficking," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 79.

DANET A., "Romania," *in* JAHNSEN S.Ø., WAGENAAR H. (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, pp. 258-271.

DANIELE M., CALVANESE E., “Evidence Gathering,” *in* KOSTORIS R.E. (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, pp. 353-391, DOI:10.1007/978-3-319-72462-1_9.

DANIELSEN D., “Corporate power and global order,” *in* ORFORD A. (ed.), *International Law and its Others*, Cambridge University Press, 2006, pp. 85-99, DOI:10.1017/CBO9780511494284.012.

DARLEY M. et al., “France,” *in* JAHNSEN S.Ø., WAGENAAR H. (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, pp. 92-106.

DE CARBONNIERES L., “Le droit pénal, expression de l’autorité du souverain : *imperium* ou *jurisdictio*,” *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL, UBEDA-SAILLARD M. (eds.), *La souveraineté pénale de l’État au XXIème siècle*, Éditions Pedone, 2018, p. 45.

DE JORGE PÉREZ C., “El escondite virtual y el nuevo agente encubierto,” *in* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 245-253.

DE LA CUESTA J.L., “Organised Crime Control Policies in Spain: A ‘Disorganised’ Criminal Policy for ‘Organised’ Crime,” *in* FIJNAUT C., PAOLI L. (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime no. 4, 1st ed., 2006, p. 795.

DE LA MATA BARRANCO N.J., “Tipos penales para los que se prevé responsabilidad penal. Lagunas y deficiencias a la luz de la normativa europea,” *in* JUANES PECES Á. (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 1300.

DE MARCO E., “La captation des données,” *in* BLAY-GRABARCZYK K. et al. (eds.), *Le nouveau cadre législatif de la lutte contre le terrorisme à l’épreuve des droits fondamentaux*, Institut Universitaire Varenne, Collection “Colloques & Essais” no. 44, 2017, p. 88.

DE VAUPLANE H., “Une nouvelle géopolitique de la norme,” *in* GARAPON A., SERVAN-SCHREIBER P. (eds.), *Deals de justice: le marché américain de l’obéissance mondialisée*, Presses universitaires de France, 2013, p. 23.

DE VRIES I., JOSE M.A., FARRELL A., “It’s Your Business: The Role of the Private Sector in Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 745-762, DOI:10.1007/978-3-319-63058-8_45.

DECIMA O., “De la loyauté de la preuve pénale et de ses composantes,” *Recueil Dalloz*, Dalloz, 2018, no. 02, p. 103.

DEL ROSAL BLASCO B., “La transferencia de la responsabilidad penal (y civil, derivada del delito) en los supuestos de sucesión de empresa,” *in* SUÁREZ LÓPEZ J.M. et al. (eds.), *Estudios jurídicos penales y criminológicos: en homenaje al Prof. Dr. Dr. H. C. Mult. Lorenzo Morillas Cueva*, Dykinson SL, 2018, p. 179.

DELMAS-MARTY M., “Les processus de mondialisation du droit,” *in* MORAND C.-A. (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no. 46, 2001, p. 63.

DELMAS-MARTY M., “Le phénomène de l’harmonisation : L’expérience contemporaine,” *in* FAUVARQUE-COSSON B., MAZEAUD D. (eds.), *Pensée juridique française et harmonisation européenne du droit*, Société de législation comparée, Droit privé comparé et européen no. 1, 2003, p. 39.

DELPECH X., “Propos introductifs,” *in* DELPECH X. (ed.), *L’émergence d’un droit des plateformes*, Editions Dalloz, 2021, p. 9.

DECKERT K., “Corporate Criminal Liability in France,” *in* PIETH M., IVORY R. (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, pp. 147-176, DOI:10.1007/978-94-007-0674-3_5.

DEROSIER J.-P., “Les limites du concept de souveraineté numérique,” *in* TÜRK P., VALLAR C. (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 77.

DESFORGES A., “Les stratégies européennes dans le cyberespace,” *in* BLANDIN-OBERNESSER A. (ed.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, pp. 31-55.

DESWARTE Y., GAMBS S., “Protection de la vie privée : principes et technologies,” *in* ALLARD T., LE METAYER D. (eds.), *Les technologies de l’information au service des droits: opportunités, défis, limites*, Bruylant, Cahiers du Centre de recherches Informatique et droit no. 32, 2010, p. 107.

DÍAZ MARTÍNEZ M., “La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos,” *in* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 85-112.

DINWOODIE G., “Who are Internet Intermediaries?,” *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 35-56, DOI:10.1093/oxfordhb/9780198837138.013.2.

DOCARMO T.E., “Major International Counter-Trafficking Organizations: Addressing Human Trafficking from Multiple Directions,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1429-1444, DOI:10.1007/978-3-319-63058-8_78.

DOCQUIR P.F., “La confrontation entre droits fondamentaux et puissances privées vues à travers le prime de la liberté d’expression,” *in* VAN ENIS Q., DE TERWANGNE C. (eds.), *L’Europe des droits de l’homme à l’heure d’internet*, Emile Bruylant, 2018, p. 75.

DONOSO ABARCA L., “Legitimidad de los sistemas de videovigilancia activa como medida de investigación tecnológica,” *in* BUENO DE MATA F., GONZÁLEZ PULIDO I., BUJOSA VADELL L. (eds.), *Fodertics 8.0: estudios sobre tecnologías disruptivas y justicia*, Comares, 2020, pp. 245-257.

DOUVILLE T., “Quel droit pour les plateformes ?,” *in* DELPECH X. (ed.), *L’émergence d’un droit des plateformes*, Editions Dalloz, 2021, p. 217.

DRYJANSKA L., “Toward a Sustainable Theory of Human Trafficking and Contemporary Slavery,” *in* WALKER L., GAVIRIA G., GOPAL K. (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 21-37, DOI:10.1007/978-3-319-73621-1_4.

DUBOS O., “L’Union européenne : sphynx ou énigme ?,” *in* COLLECTIF (ed.), *Les dynamiques du droit européen en début de siècle: études en l’honneur de Jean Claude Gautron*, Pedone, 2004, p. 29.

DUONG K.A., “Human Trafficking and Migration: Examining the Issues from Gender and Policy Perspectives,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1819-1833, DOI:10.1007/978-3-319-63058-8_131.

DURÁN BERNARDINO M., “El método comparado en los trabajos de investigación,” *in* MARCHAL ESCALONA N., MUÑOZ GONZÁLEZ M.C., MUÑOZ GONZÁLEZ S. (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 48.

EL ZEIN S., “L’indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie,” *in* PIATTI M.-C. (ed.), *Les libertés individuelles à l’épreuve des nouvelles technologies de l’information*, Presses universitaires de Lyon, 2001, p. 153.

ELKIN-KOREN N., PEREL M., “Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law,” *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 668-678, DOI:10.1093/oxfordhb/9780198837138.013.34.

FARRELL A., “Improving Law Enforcement Identification and Response to Human Trafficking,” *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 181.

FARRELL A., DE VRIES I., “Measuring the Nature and Prevalence of Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 147-162, DOI:10.1007/978-3-319-63058-8_6.

FARRELL A., KANE B., “Criminal Justice System Responses to Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 641-657, DOI:10.1007/978-3-319-63058-8_40.

FERNÁNDEZ AVILÉS J.A., “El método comparado en el Derecho del trabajo, relaciones laborales y Seguridad Social ('Pertinencia y Prudencia' en su uso),” *in* MARCHAL ESCALONA N., MUÑOZ GONZÁLEZ M.C., MUÑOZ GONZÁLEZ S. (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 291.

FERNÁNDEZ TERUELO J.G., “Regulación vigente. Exigencias legales que permiten la atribución de responsabilidad penal a la persona jurídica y estructura de imputación (CP art.31 bis 1,2 inciso 1º y 5),” *in* JUANES PECES Á. (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 300.

FERNÁNDEZ TERUELO J.G., “La responsabilidad penal de los dirigentes, representantes de la persona jurídica o de quienes ostentan facultades de organización y control de la misma,” *in* JUANES PECES Á. (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 1600.

FINCKENAUER J.O., CHIN K., “Sex trafficking: a target for situational crime prevention?,” *in* BULLOCK K., CLARKE R.V.G., TILLEY N. (eds.), *Situational prevention of organised crimes*, Willan, Crime science series, 2010, p. 58.

FOOT K., “Multisector Collaboration Against Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 659-672, DOI:10.1007/978-3-319-63058-8_41.

FOOT K., “Actors and activities in the anti–human trafficking movement,” *in* HEINE J., THAKUR R.C. (eds.), *The dark side of globalization*, UN University Press, 2011, p. 249.

FOURNIER A., “Aperçu critique du principe de double incrimination en droit pénal international,” *in* BOULOC B., ALT-MAES F. (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, pp. 333-344.

FRANSEN D., “Face à l’internationalisation : existe-t-il des compétences irréductibles du juge interne ?,” *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL, UBEDA-SAILLARD M. (eds.), *La souveraineté pénale de l’État au XXIème siècle*, Éditions Pedone, 2018, p. 161.

FRANSSEN V., FLORE D., “Introduction : le droit pénal à l’ère numérique,” *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

FRANSSEN V., LEROUX O., “Recherche policière et judiciaire sur Internet : analyse critique du nouveau cadre législatif belge,” *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

FRASER N., “Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy,” *in* CALHOUN C.J. (ed.), *Habermas and the public sphere*, MIT Press, Studies in contemporary German social thought, Nachdr., 1993, pp. 109-142.

FRÍGOLS I BRINES E., "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías," *in* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 37-92.

FROSIO G., HUSOVEC M., "Accountability and Responsibility of Online Intermediaries," *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 611-630, DOI:10.1093/oxfordhb/9780198837138.013.31.

FUCHS C., "Class and Exploitation on the Internet," *in* SCHOLZ T. (ed.), *Digital labor: the Internet as playground and factory*, Routledge, 2013, p. 265.

FUENTES SORIANO O., "Europa ante el reto de la prueba digital. El establecimiento de instrumentos probatorios comunes. Las órdenes europeas de entrega y conservación de pruebas electrónicas," *in* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 281-319.

GALÁN MUÑOZ A., "Unión Europea y represión penal del discurso terrorista. ¿Origen, excusa o posible referente restrictivo?," *in* LEÓN ALAPONT J. (ed.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Homenajes y Congresos, 2020, pp. 351-388.

GALLAGHER A.T., "Trafficking in transnational criminal law," *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 21.

GARCÍA ARÁN M., "Trata de personas y regulación de la prostitución," *in* PÉREZ ALONSO E. (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 655-675.

GARCÍA RIVAS N., "Responsabilidad penal de las personas jurídicas en la trata sexual y protección de las víctimas," *in* LLORIA GARCÍA P., CRUZ ÁNGELES J. (eds.), *La violencia sobre la mujer en el S. XXI: género, derecho y TIC*, Aranzadi, Estudios, 2019, pp. 59-80.

GARSTKA K., ERDOS D., "Hiding in Plain Sight: Right to be Forgotten and Search Engines in the Context of International Data Protection Frameworks," *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 147.

GEENS K., "Défis de la société numérique : perspectives politiques," *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

GEIGER C., FROSIO G., IZYUMENKO E., "Intermediary Liability and Fundamental Rights," *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 137-152, DOI:10.1093/oxfordhb/9780198837138.013.7.

GIL NOBAJAS M.S., "Respuesta penal a la criminalidad empresarial en supuestos de explotación laboral," *in* GÓMEZ LANZ J., BENITO SÁNCHEZ D., MARTÍNEZ DE BRINGAS A. (eds.), *Sistema penal y exclusión social*, Aranzadi, Monographs in comparative and transnational law no. 10, 2020, pp. 173-204.

GIACOMETTI M., "Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ?," *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019.

GINDRE E., "Discussion L'harmonisation pénale accessoire. Éléments de réflexion sur la place du droit pénal au sein de l'Union européenne," *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l'Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 197.

GIUDICELLI-DELAGE G., "Introduction générale," *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l'Union*

européenne au lendemain du Traité de Lisbonne, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 17.

GODEFROY T., "The Control of Organised Crime in France: A Fuzzy Concept but a Handy Reference," *in* FIJNAUT C., PAOLI L. (eds.), *Organised crime in Europe: concepts, patterns and control policies in the European Union and beyond*, Springer, Studies of organized crime no. 4, 1st ed., 2006, p. 763.

GOLDMAN E., "An Overview of the United States' Section 230 Internet Immunity," *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 153-171, DOI:10.1093/oxfordhb/9780198837138.013.8.

GÓMEZ SOLER E., "La utilización de dispositivos técnicos de captación de la imagen de seguimiento y de localización. Cuando la práctica forense no puede esperar," *in* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 113-134.

GÓMEZ TOMILLO M., "Algunos déficits en la regulación de la responsabilidad penal de las personas jurídicas: en particular los delitos contra la seguridad e higiene en el trabajo," *in* DEL VICENTE REMESAL J., BACIGALUPO ZAPATER E., LUZÓN PEÑA D.-M. (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, pp. 1633-1640.

GONZÁLEZ CUSSAC J.L., "El modelo español de responsabilidad penal de las personas jurídicas," *in* GÓMEZ COLOMER J.L., BARONA VILAR S., CALDERÓN CUADRADO P. (eds.), *El derecho procesal español del siglo XX a golpe de tango: Juan Montero Aroca : liber amicorum, en homenaje y para celebrar su LXX cumpleaños*, Tirant lo Blanch, 2012, p. 1018.

GOODEY J., "Data on Human Trafficking Challenges and Policy Context," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 39.

GRABOWSKA-MOROZ B., "Data Retention in the European Union," *in* ZUBIK M., PODKOWIK J., RYBSKI R. (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 3-17, DOI:10.1007/978-3-030-57189-4_1.

GRACIA MARTÍN L., "¿Tiene hoy sentido -y si lo tiene, en qué dirección y con qué alcance- algún debate sobre la posibilidad de penar y sancionar a la persona jurídica?," *in* SILVA SÁNCHEZ J.-M., MIR PUIG S. (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 115.

GREGORIOU C., RAS I.A., "Representations of Transnational Human Trafficking: A Critical Review," *in* GREGORIOU C. (ed.), *Representations of Transnational Human Trafficking*, Springer International Publishing, 2018, pp. 1-24, DOI:10.1007/978-3-319-78214-0_1.

GREGORIOU C., RAS I.A., "'Call for Purge on the People Traffickers': An Investigation into British Newspapers' Representation of Transnational Human Trafficking, 2000–2016," *in* GREGORIOU C. (ed.), *Representations of Transnational Human Trafficking*, Springer International Publishing, 2018, pp. 25-59, DOI:10.1007/978-3-319-78214-0_2.

GUAMÁN HERNÁNDEZ A., "La prostitución como actividad económica, la incidencia de la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas sobre la cuestión," *in* SERRA CRISTÓBAL R. (ed.), *Prostitución y trata: marco jurídico y régimen de derechos*, Tirant lo Blanch, Tirant monografías no. 484, 2007, pp. 255-294.

GUARNIERI C., "Agency for All, Privacy for None," *in* HERLO B. (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, p. 121.

GUTIÉRREZ PÉREZ E., "Los *compliance programs* o la vuelta al *no body to kick, no soul to damn*. Una aproximación a la luz de la reforma del Código Penal por la Ley Orgánica 1/2015," *in* DÍAZ

CORTÉS L.M. et al. (eds.), *Propuestas penales: nuevos retos y modernas tecnologías*, Ediciones Universidad de Salamanca, 2016, pp. 379-394.

HEALY C., BENNACHIE C., REED A., "History of the New Zealand Prostitutes' Collective," *in* ABEL G. et al. (eds.), *Taking the crime out of sex work: New Zealand sex workers' fight for decriminalisation*, Policy Press, 2010, p. 45, DOI:10.1332/policypress/9781847423344.001.0001.

HERZ A., "Human Trafficking and Police Investigations," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 129.

HEUSCHLING L., "'Effectivité', 'efficacité', 'efficience', et 'qualité' d'une norme/d'un droit. Analyse des mots et des concepts," *in* FATIN-ROUGE STEFANINI M. et al. (eds.), *L'efficacité de la norme juridique: nouveau vecteur de légitimité ?*, Bruylant, À la croisée des droits 6, 2012, p. 27.

HIAH J., "(Anti-)trafficking for Labor Exploitation in Romania: A Labor Perspective," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1133-1149, DOI:10.1007/978-3-319-63058-8_102.

HOANG K.K., "Perverse Humanitarianism and the Business of Rescue: What's Wrong with NGOs and What's Right about the 'Johns'?," *in* ORLOFF A.S., RAY R., SAVCI E. (eds.), *Perverse Politics? Feminism, Anti-Imperialism, Multiplicity*, Emerald Group Publishing Limited, Political Power and Social Theory, 1st ed., January 1, 2016, vol. 30, pp. 19-43, DOI:10.1108/S0198-871920160000030007.

HOLMES L., "Introduction: the issue of human trafficking," *in* HOLMES L. (ed.), *Trafficking and human rights: European and Asia-Pacific perspectives*, Edward Elgar, 2010, p. 1.

HOWELL S., "Systemic Vulnerabilities on the Internet and the Exploitation of Women and Girls: Challenges and Prospects for Global Regulation," *in* KURY H., REDO S., SHEA E. (eds.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, pp. 575-601, DOI:10.1007/978-3-319-28424-8_22.

HUNECKE I., "Germany," *in* JAHNSEN S.Ø., WAGENAAR H. (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, First issued in paperback, 2019, pp. 107-121.

HUSSON-ROCHCONGAR C., "La gouvernance d'Internet et les droits de l'homme," *in* VAN ENIS Q., DE TERWANGNE C. (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 41.

IBÁÑEZ SOLAZ M., "Algunas consideraciones sobre la prueba en los delitos de violencia de género," *in* MARTÍNEZ GARCÍA E. (ed.), *La prevencion y erradicación de la violencia de género: un estudio multidisplinar y forense*, Aranzadi, 2012, p. 435.

JEFFREYS E., "Public encounters with whorephobia: Making sense of hostility toward sex worker advocates," *in* DEWEY S., CROWHURST I., IZUGBARA C.O. (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 505-515, 11 pages.

JIN D.Y., "Facebook's Platform Imperialism: The Economics and Geopolitics of Social Media," *in* BOYD-BARRETT O., MIRRLEES T. (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, pp. 187-198.

JONES J., "Is It Time to Open a Conversation About a New United Nations Treaty to Fight Human Trafficking That Focuses on Victim Protection and Human Rights?," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1803-1818, DOI:10.1007/978-3-319-63058-8_129.

JOOST G., "Out of Balance The Impact of Digitalization on Social Cohesion," *in* HERLO B. (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, p. 91.

JUANATEY DORADO C., DOVAL PAIS A., “Límites de la protección penal de la intimidad frente a la grabación de conversaciones o imágenes,” *in* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 127-170.

KAKAR S., “Child/Forced/Servile Marriages ⇄ Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 503-519, DOI:10.1007/978-3-319-63058-8_30.

KALMO H., SKINNER Q., “Introduction : a concept in fragments,” *in* KALMO H., SKINNER Q. (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 1.

KAYE K. et al., “Neoliberal Vulnerability and the Vulnerability of Neoliberalism,” *in* JAKOBSEN J., BERNSTEIN E. (eds.), *Paradoxes of Neoliberalism*, Routledge, 1st ed., December 7, 2021, pp. 71-108, DOI:10.4324/9781003252702-3.

KELLY L., COY M., “Ethics as Process, Ethics in Practice: Researching the Sex Industry and Trafficking,” *in* SIEGEL D., DE WILDT R. (eds.), *Ethical Concerns in Research on Human Trafficking*, Springer International Publishing, Studies of Organized Crime, 2016, vol. 13, pp. 33-50, DOI:10.1007/978-3-319-21521-1_3.

KOBRIN S.J., “Sovereignty@Bay: Globalization, Multinational Enterprise, and the International Political System,” *in* RUGMAN A.M., BREWER T. (eds.), *The Oxford Handbook of International Business*, Oxford University Press, September 2, 2009, DOI:10.1093/oxfordhb/9780199234257.003.0007.

KONDAKOV A., ZHAIVORONOK D., “Re-assembling the feminist war machine: State, feminisms and sex workers in Russia,” *in* DEWEY S., CROWHURST I., IZUGBARA C.O. (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 250-262, 13 pages.

KOSTORIS R.E., “European Law and Criminal Justice,” *in* KOSTORIS R.E. (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, pp. 3-63, DOI:10.1007/978-3-319-72462-1_1.

KRSMANOVIĆ E., “Mediated Representation of Human Trafficking: Issues, Context, and Consequence,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 865-880, DOI:10.1007/978-3-319-63058-8_101.

KURZ F., “Prosecution of trafficking in human beings in civil law systems The example of Belgium,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 224.

LAIDLAW E.B., “Online Platform Responsibility and Human Rights,” *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 65.

LAIDLAW E.B., “Myth or Promise? The Corporate Social Responsibilities of Online Service Providers for Human Rights,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 135-155, DOI:10.1007/978-3-319-47852-4_8.

LAMBINE M., GAVIRIA G., “Organized Crime, Gangs, and Trafficking,” *in* WALKER L., GAVIRIA G., GOPAL K. (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 111-116, DOI:10.1007/978-3-319-73621-1_12.

LAMMASNIEMI L., “International Legislation on White Slavery and Anti-trafficking in the Early Twentieth Century,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 67-78, DOI:10.1007/978-3-319-63058-8_112.

LARA AGUADO Á., “Capítulo IV. Violencia contra la mujer extranjera y trata desde la perspectiva de género,” *in* GIL RUIZ J.M. (ed.), *El convenio de Estambul: como marco de derecho antisubordiscriminatorio*, Dykinson, 2018, pp. 101-133.

LASALLE M., “Souverainetés et responsabilités dans la collecte internationale de preuves - L’exemple de l’accès aux données bancaires en matière pénale,” *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL, UBEDA-SAILLARD M. (eds.), *La souveraineté pénale de l’État au XXI^{ème} siècle*, Éditions Pedone, 2018, p. 275.

LAVAUD-LEGENDRE B., “Introduction,” *in* LAVAUD-LEGENDRE B. (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 7.

LAVAUD-LEGENDRE B., “L’émergence d’un statut de traite des êtres humains en droit français,” *in* LAVAUD-LEGENDRE B. (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 101.

LAZERGES C., “Dédoublement de la procédure pénale et garantie des droits fondamentaux,” *in* BOULOC B., ALT-MAES F. (eds.), *Les droits et le droit: mélanges dédiés à Bernard Bouloc*, Dalloz, 2007, pp. 573-590.

LE COZ N., “Les apports du droit européen et du Conseil de l’Europe à la lutte contre la traite des êtres humains,” *in* LAVAUD-LEGENDRE B. (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 159.

LEARY R., THOMAS J., “How Complexity Theory is Changing the Role of Analysis in Law Enforcement and National Security,” *in* AKHGAR B., YATES S. (eds.), *Intelligence Management*, Springer London, Advanced Information and Knowledge Processing, 2011, pp. 61-78, DOI:10.1007/978-1-4471-2140-4_5.

LEBARON G., “A Market in Deception? Ethically Certifying Exploitative Supply Chains,” *in* BLIGHT D.W., LEBARON G., PLILEY J.R. (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, pp. 156-178, DOI:10.1017/9781108902519.009.

LEE M., “Introduction : Understanding human trafficking,” *in* LEE M. (ed.), *Human trafficking*, Willan, 2007, p. 1.

LEWANDOWSKI D., “Is Google Responsible for Providing Fair and Unbiased Results?,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 61-77, DOI:10.1007/978-3-319-47852-4_4.

LIGETI K., ROBINSON G., “Transnational Enforcement of Production Orders for Electronic Evidence: Beyond Mutual Recognition?,” *in* KERT R., LEHNER A. (eds.), *Vielfalt des Strafrechts im internationalen Kontext. Festschrift für Frank Höpfel zum 65. Geburtstag*, NWV Verlag, 1st ed., January 19, 2018, pp. 625-644.

LINCHUAN QIU J., “Labor and Social Media: The Exploitation and Emancipation of (almost) Everyone Online,” *in* BURGESS J., MARWICK A. (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 298.

LLOYD D., “Human Trafficking in Supply Chains and the Way Forward,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 815-837, DOI:10.1007/978-3-319-63058-8_50.

LOBEL O., “Coase and the Platform Economy,” *in* INFRANCA J.J., FINCK M., DAVIDSON N.M. (eds.), *The Cambridge Handbook of the Law of the Sharing Economy*, Cambridge University Press, Cambridge Law Handbooks, 2018, pp. 67-77, DOI:10.1017/9781108255882.006.

LÓPEZ ORTEGA J.J., “La utilización de medios técnicos de observación y vigilancia en el proceso penal,” *in* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 261-334.

LÓPEZ-BARAJAS PEREA I., "El derecho a la protección del entorno virtual y sus límites. El registro de los sistemas informáticos," *in* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 135-168.

LÖWSTEDT A., "Fighting Censorship: A Shift from Freedom to Diversity," *in* DEFLEM M., SILVA D.M.D. (eds.), *Sociology of Crime, Law and Deviance*, Emerald Publishing Limited, April 23, 2021, pp. 9-23, DOI:10.1108/S1521-613620210000026002.

MALLOCH M., "Criminalising Victims of Human Trafficking: State Responses and Punitive Practices," *in* MALLOCH M., RIGBY P. (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 175-193.

MALLOCH M., RIGBY P., "Contexts and Complexities," *in* MALLOCH M., RIGBY P. (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 1-16.

MANFREDI SÁNCHEZ J.L., "La transformación política de la privacidad," *in* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 87-96.

MAPP S.C., "Domestic Sex Trafficking of Children," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 353-370, DOI:10.1007/978-3-319-63058-8_21.

MAQUIEIRA V., "Genero, diferencia y desigualdad," *in* BELTRÁN E., MAQUIEIRA V. (eds.), *Feminismos, debates teóricos contemporáneos*, Alianza Editorial, El Libro universitario no. 069, 2001, p. 125.

MARGUENAUD J.-P., "La réécriture du droit criminel français sous la dictée de la cour européenne des droits de l'homme," *in* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 923-938.

MARSHALL P., THATUN S., "Miles Away: The Trouble with Prevention in the Greater Mekong sub-region," *in* KEMPADOO K., SANGHERA J., PATTANAIK B. (eds.), *Trafficking and prostitution reconsidered: new perspectives on migration, sex work, and human rights*, Paradigm Publishers, 2nd ed., 2012, p. 43.

MARTÍN DIZ F., "Planteamiento y estructura de soluciones extrajudiciales online de controversias y conflictos generados in Internet," *in* BUENO DE MATA F. (ed.), *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*, Editorial Comares, 2017, p. 661.

MARTIN-CHENUT K., "Droits de l'homme et RSE : vers un humanisme responsable ?," *in* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l'honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 125-144.

MARTÍNEZ SANTOS A., "Las grabaciones obtenidas a través de sistemas de videovigilancia en el proceso penal: derechos fundamentales afectados y tipología de supuestos," *in* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017.

MAYER F.W., "Leveraging private governance for public purpose: business, civil society and the state in labour regulation," *in* PAYNE A., PHILLIPS N. (eds.), *Handbook of the International Political Economy of Governance*, Edward Elgar Publishing, 2014, pp. 344-360, DOI:10.4337/9780857933485.00026.

MCGONAGLE T., "Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation," *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 466-485, DOI:10.1093/oxfordhb/9780198837138.013.24.

MCNAMEE J., FERNÁNDEZ PÉREZ M., "Fundamental Rights and Digital Platforms in the European Union: a Suggested Way Forward," *in* BELLI L., ZINGALES N. (eds.), *Platform*

regulations: how platforms are regulated and how they regulate us, FGV Digital Repository, November 2017, p. 99.

MENDOZA ENRÍQUEZ O.A., "Derecho al olvido en la economía digital," *in* BUENO DE MATA F. (ed.), *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*, Editorial Comares, 2017, p. 369.

MESTRE DELGADO E., "El principio de culpabilidad en la determinación de la responsabilidad penal de las personas jurídicas," *in* DEL VICENTE REMESAL J., BACIGALUPO ZAPATER E., LUZÓN PEÑA D.-M. (eds.), *Libro Homenaje al Profesor Diego-Manuel Luzón Peña con motivo de su 70º aniversario*, Reus, 2020, p. 269.

MEZZADRA S., NUNES R., "The gaze of autonomy Capitalism, migration and social struggles," *in* SQUIRE V. (ed.), *The contested politics of mobility: borderzones and irregularity*, Routledge, Routledge advances in international relations and global politics no. v. 87, 2011, pp. 121-142.

MICEK P., AYDIN D.D., "Non-financial Disclosures in the Tech Sector: Furthering the Trend," *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 241-261, DOI:10.1007/978-3-319-47852-4_13.

MIDDLETON J., "From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 467-480, DOI:10.1007/978-3-319-63058-8_23.

MILIVOJEVIĆ S., "Gendered exploitation in the digital border crossing?: An analysis of the human trafficking and information-technology nexus," *in* SEGRAVE M., VITIS L. (eds.), *Gender, Technology and Violence*, Routledge, 2017, pp. 28-44.

MILIVOJEVIĆ S., "The State, Virtual Borders and E-Trafficking: Between Fact and Fiction," *in* PICKERING S., MCCULLOCH J. (eds.), *Borders and crime Pre-crime, mobility and serious harm in an age of globalization*, Palgrave Macmillan, 2012, p. 72.

MINOW M., "Feminist Reason: Getting It and Losing It [1988]," *in* BARTLETT K.T., KENNEDY R.T. (eds.), *Feminist legal theory: readings in law and gender*, Westview Press, New perspectives on law, culture, and society, 1991, p. 357.

MIRRLEES T., "GAFAM and Hate Content Moderation: Deplatforming and Deleting the Alt-right," *in* DEFLEM M., M. D. SILVA D. (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, pp. 81-97, DOI:10.1108/S1521-613620210000026006.

MONTEROS OBELAR S., "La violencia de las fronteras legales: violencia de género y mujer migrante," *in* LAURENZO COPELLO P., MAQUEDA ABREU M.L., RUBIO A. (eds.), *Género, violencia y derecho*, Tirant lo Blanch, Alternativa, 2008, pp. 231-250.

MORAWSKA E., "Trafficking into and from Eastern Europe," *in* LEE M. (ed.), *Human trafficking*, Willan, 2007, p. 92.

MORENO HERNÁNDEZ M., "Algunas reflexiones político-criminales y dogmáticas sobre la responsabilidad penal de las personas jurídicas. ¿Es necesaria una teoría general del delito empresarial?," *in* SILVA SÁNCHEZ J.-M., MIR PUIG S. (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 155.

MORILLAS CUEVA L., "La compleja delimitación de la autoría y participación en los delitos cometidos con empleo de medios o soportes de difusión mecánicos," *in* LORENZO SALGADO J.M., ABEL SOUTO M. (eds.), *Estudios penales en homenaje al profesor José Manuel Lorenzo Salgado*, Tirant lo Blanch, Homenajes & congresos, 1st ed., 2021, pp. 973-986.

MOSLEY J.L., "The 'john': Our new folk devil," *in* DEWEY S., CROWHURST I., IZUGBARA C.O. (eds.), *Routledge International Handbook of Sex Industry Research*, Routledge, Routledge international handbooks, 1st ed., 2018, pp. 352-365, 14 pages.

MOSSE M., “Le numérique et le retour de la souveraineté,” *in* TÜRK P., VALLAR C. (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 55.

MUSKAT-GORSKA Z., “Human Trafficking and Forced Labour: Mapping Corporate Liability,” *in* KOTISWARAN P. (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, pp. 443-470.

NANDA V.P., “Corporate Criminal Liability in the United States: Is a New Approach Warranted?,” *in* PIETH M., IVORY R. (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, pp. 63-89, DOI:10.1007/978-94-007-0674-3_2.

NIETO MARTÍN A., “La autoregulación preventiva de la empresa como objeto de la política criminal,” *in* SILVA SÁNCHEZ J.-M., MIR PUIG S. (eds.), *Estudios de derecho penal: homenaje al profesor Santiago Mir Puig*, Euros, 2017, p. 167.

O’CONNELL DAVIDSON J., “The Right to Locomotion? Trafficking, Slavery and the State,” *in* KOTISWARAN P. (ed.), *Revisiting the law and governance of trafficking, forced labor and modern slavery*, University Press, Cambridge studies in law and society, 2017, pp. 157-178.

OLARIU O., “El papel del Derecho comparado en la enseñanza del Derecho Internacional Público: el ejemplo de la asignatura Derecho Internacional de los Derechos Humanos,” *in* MARCHAL ESCALONA N., MUÑOZ GONZÁLEZ M.C., MUÑOZ GONZÁLEZ S. (eds.), *El Derecho Comparado en la Docencia y la Investigación*, Dykinson, S.L., 2017, p. 276.

OLARTE ENCABO S., “El desafío del trabajo decente en las cadenas mundiales de suministros. Respuesta internacional, estatal, sindical y social,” *in* RAMOS TAPIA M.I. et al. (eds.), *Formas contemporáneas de esclavitud y derechos humanos en clave de globalización, género y trata de personas*, Tirant lo Blanch, Homenajes & congresos, 2020, pp. 91-134.

OTTO D., “Lost in translation: re-scripting the sexed subjects of international human rights law,” *in* ORFORD A. (ed.), *International Law and its Others*, Cambridge University Press, 2006, pp. 318-356, DOI:10.1017/CBO9780511494284.012.

OUTSHOORN J., “European Union and prostitution policy,” *in* JAHNSEN S.Ø., WAGENAAR H. (eds.), *Assessing prostitution policies in Europe*, Routledge, Taylor & Francis Group, Interdisciplinary studies in sex for sale no. 3, 1st ed., 2019, pp. 363-375.

PATAKI K.A., ROBISON K.M., “The Concept of Choice,” *in* WALKER L., GAVIRIA G., GOPAL K. (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 39-43, DOI:10.1007/978-3-319-73621-1_5.

PECK G., “Counting Modern Slaves: Historicizing the Emancipatory Work of Numbers,” *in* BLIGHT D.W., LEBARON G., PLILEY J.R. (eds.), *Fighting Modern Slavery and Human Trafficking: History and Contemporary Policy*, Cambridge University Press, Slaveries since Emancipation, 2021, pp. 34-55, DOI:10.1017/9781108902519.003.

PÉREZ ALONSO E., “Tratamiento jurídico-penal de las formas contemporáneas de esclavitud,” *in* PÉREZ ALONSO E. (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 333-366.

PÉREZ ALONSO E.J., “El bien jurídico protegido en el delito de trata de seres humanos,” *in* MARÍN DE ESPINOSA CEBALLOS E.B. et al. (eds.), *El derecho penal en el siglo XXI: Liber amicorum en honor al profesor José Miguel Zugaldía Espinar*, Tirant lo Blanch, 1st ed., 2021, pp. 521-546.

PERRY BARLOW J., “Déclaration d’indépendance du cyberespace,” *in* BLONDEAU O., LATRIVE F. (eds.), *Libres enfants du savoir numérique*, éd. de l’éclat, 2000, pp. 47-54.

PETIN J., POELEMANS M., “La réponse de l’Union européenne à la traite des êtres humains,” *in* LAVAUD-LEGENDRE B. (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 123.

PIETH M., IVORY R., “Emergence and Convergence: Corporate Criminal Liability Principles in Overview,” *in* PIETH M., IVORY R. (eds.), *Corporate Criminal Liability*, Springer Netherlands, 2011, pp. 3-60, DOI:10.1007/978-94-007-0674-3_1.

PIN X., “Discussion Subsidiarité versus efficacité,” *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l’Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l’UMR de droit comparé de Paris no. 28, 2012, p. 47.

PIOTROWICZ R., SORRENTINO L., “The non-punishment provision with regard to victims of trafficking A human rights approach,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 171.

PLANCHADELL GARGALLO A., “Investigación y enjuiciamiento del delito de trata: aspectos procesales desde la jurisprudencia,” *in* VILLACAMPA ESTIARTE C., PLANCHADELL GARGALLO A. (eds.), *La trata de seres humanos tras un decenio de su incriminación: ¿es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, 2022, pp. 851-888.

PLANT R., “Mettre fin à l’exploitation, réflexions sur l’expérience nigériane et internationale,” *in* LAVAUD-LEGENDRE B. (ed.), *Prostitution nigériane : entre rêves de migration et réalités de la traite*, ÉdKarthala, Hommes et sociétés, 2013, p. 213.

PLUMAUZILLE C., “Prostitution,” *in* RENNES J. (ed.), *Encyclopédie critique du genre*, La Découverte, 2021, pp. 588-600.

POHLE J., THIEL T., “Digital Sovereignty,” *in* HERLO B. (ed.), *Practicing sovereignty. Digital involvement in times of crises*, Transcript Verlag, 2021, p. 47.

POULLET Y., “Quelques réflexions d’avant-propos,” *in* VAN ENIS Q., DE TERWANGNE C. (eds.), *L’Europe des droits de l’homme à l’heure d’internet*, Emile Bruylant, 2018, p. 7.

QUINTERO OLIVARES G., “Organizaciones y grupos criminales en el derecho penal de nuestro tiempo,” *in* VILLACAMPA ESTIARTE C. (ed.), *La delincuencia organizada: un reto a la política-criminal actual*, Aranzadi, Primera edición, 2013, pp. 23-44.

RANKIN G., KINSELLA N., “Human Trafficking – The Importance of Knowledge Information Exchange,” *in* AKHGAR B., YATES S. (eds.), *Intelligence Management*, Springer London, Advanced Information and Knowledge Processing, 2011, pp. 159-180, DOI:10.1007/978-1-4471-2140-4_11.

RENZETTI C.M., “Service providers and their perceptions of the service needs of sex trafficking victims in the United States,” *in* DRAGIEWICZ M. (ed.), *Global Human Trafficking Critical issues and contexts*, Routledge, 2014, pp. 138-152.

RENZIKOWSKI J., “Trafficking in human beings as a crime and as a human rights violation,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 13.

RIJKEN C., “Trafficking in persons A victim’s perspective,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 239.

RIORDAN J., “A Theoretical Taxonomy of Intermediary Liability,” *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 56-89, DOI:10.1093/oxfordhb/9780198837138.013.3.

RIZO GÓMEZ B., “La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica,” *in* ASENCIO MELLADO J.M., FERNÁNDEZ LÓPEZ M. (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1st ed., 2017, pp. 97-123.

ROBERT V., USUNIER L., “Conclusion. Du bon usage du droit comparé,” *in* DELMAS-MARTY M., UNIVERSITE DE PARIS I: PANTHEON-SORBONNE (eds.), *Critique de l’intégration normative: l’apport du droit comparé à l’harmonisation des droits*, Presses Universitaires de France, Les voies du droit, 1st ed., 2004, pp. 226-255.

RODIN D., “Two Visions of Human Rights: Relational and Beneficiary-Focused Theories,” *in* AKANDE D. et al. (eds.), *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment*, Oxford University Press, January 30, 2020, p. 76, DOI:10.1093/oso/9780198824770.003.0004.

RODRÍGUEZ ÁLVAREZ A., “Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal,” *in* ASENCIO MELLADO J.M., FERNÁNDEZ LÓPEZ M. (eds.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Monografías, 1st ed., 2017, pp. 149-182.

RODRÍGUEZ ÁLVAREZ A., “Cinco preguntas y algunas respuestas sobre los tweets en el proceso penal,” *in* BUENO DE MATA F., GONZÁLEZ PULIDO I. (eds.), *Fodertics 7.0: estudios sobre derecho digital*, Comares, 2019, p. 269.

ROUJOU DE BOUBEE I., “Cryptographie : ses nécessités, ses dérives,” *in* PIATTI M.-C. (ed.), *Les libertés individuelles à l’épreuve des nouvelles technologies de l’information*, Presses universitaires de Lyon, 2001, p. 125.

GAYLE R., “Thinking Sex: Notes for a Radical Theory of the Politics of Sexuality,” *in* GAYLE R. (ed.), *Deviations: a Gayle Rubin reader*, Duke University Press, 2011, pp. 137-181, DOI:10.1215/9780822394068-006.

RUIZ FABRI H., “Droits de l’homme et souveraineté de l’État : les frontières ont-elles été substantiellement redéfinies ?,” *in* COLLECTIF (ed.), *Les droits individuels et le juge en Europe: mélanges en l’honneur de Michel Fromont*, Presses universitaires de Strasbourg, 2001, p. 371.

ŞANDRU S., “Data Retention in Romania,” *in* ZUBIK M., PODKOWIK J., RYBSKI R. (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 189-202, DOI:10.1007/978-3-030-57189-4_12.

SANSÓ-RUBERT PASCUAL D., “Fenómenos criminales organizados y déficit democrático. Hacia una reinterpretación del nexo político-criminal,” *in* CARPIO DELGADO J. Del (ed.), *Criminalidad en un mundo global: criminalidad de empresa, transnacional, organizada y recuperación de activos*, Tirant lo Blanch, Monografías, 2020, pp. 357-393.

SANSÓ-RUBERT PASCUAL D., “Estrategias geopolíticas de la criminalidad organizada. Desafíos de la inteligencia criminal,” *in* ZÚÑIGA RODRÍGUEZ L. (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, pp. 105-140.

SARACHAGA-BARATO N., “Forced Child and Arranged Marriages,” *in* WALKER L., GAVIRIA G., GOPAL K. (eds.), *Handbook of Sex Trafficking*, Springer International Publishing, 2018, pp. 85-92, DOI:10.1007/978-3-319-73621-1_9.

SATZGER H., “Le principe de légalité,” *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l’Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l’UMR de droit comparé de Paris no. 28, 2012, p. 85.

SAX H., “Child trafficking - a call for rights-based integrated approaches,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 251.

SCARPA S., “UN Palermo Trafficking Protocol Eighteen Years On: A Critique,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 623-640, DOI:10.1007/978-3-319-63058-8_38.

SCARPA S., “The Nebulous Definition of Slavery: Legal Versus Sociological Definitions of Slavery,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 131-144, DOI:10.1007/978-3-319-63058-8_5.

SCHENDEL W. Van, “Spaces of Engagement How Borderlands, Illegal Flows, and Territorial States Interlock,” *in* SCHENDEL W. Van, ABRAHAM I. (eds.), *Illicit flows and criminal things: states, borders, and the other side of globalization*, Indiana University Press, Tracking globalization, 2005, p. 38.

SCHENDEL W. Van, ABRAHAM I., “Introduction The Making of Illicitness,” *in* SCHENDEL W. Van, ABRAHAM I. (eds.), *Illicit flows and criminal things: states, borders, and the other side of globalization*, Indiana University Press, Tracking globalization, 2005, p. 1.

SCHEPEL H., “Constituting Private Governance Regimes: Standards Bodies in American Law,” *in* JOERGES C., SAND I.-J., TEUBNER G. (eds.), *Transnational governance and constitutionalism*, Hart, International studies in the theory of private law, 2004, p. 161.

SCHUMANN S., “Corporate Criminal Liability on Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1651-1669, DOI:10.1007/978-3-319-63058-8_10.

SEKHON G., “Combating Trafficking in Persons Through Public Awareness and Legal Education of Duty Bearers in India,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 725-744, DOI:10.1007/978-3-319-63058-8_44.

SERRA CRISTÓBAL R., “La vigilancia de datos y de comunicaciones digitales en la lucha por la seguridad nacional: especial referencia a las previsiones legislativa de España,” *in* FLORES GIMÉNEZ F., RAMÓN CHORNET C. (eds.), *Análisis de los riesgos y amenazas para la seguridad*, Tirant lo Blanch, Derechos humanos, 1st ed., 2017, pp. 105-136.

SERRA CRISTÓBAL R., “El control del *terror speech* en la red. El papel de las empresas proveedoras de servicios de internet,” *in* LEÓN ALAPONT J. (ed.), *Estudios jurídicos en memoria de la profesora doctora Elena Górriz Royo*, Tirant lo Blanch, Homenajes y Congresos, 2020, pp. 761-784.

SERRA CRISTÓBAL R., “Intimidad de la víctima en el proceso. Un ejemplo en la mujer víctima de la trata,” *in* BOIX REIG J., JAREÑO LEAL Á. (eds.), *La protección jurídica de la intimidad*, Iustel, 2010, pp. 231-260.

SHELLEY L., “Human trafficking as a form of transnational crime,” *in* LEE M. (ed.), *Human trafficking*, Willan, 2007, p. 116.

SKINNER Q., “The sovereign state: a genealogy,” *in* KALMO H., SKINNER Q. (eds.), *Sovereignty in fragments: the past, present and future of a contested concept*, Cambridge University Press, 2010, p. 26.

SMITH C.J., KANGASPUNTA K., “Defining Human Trafficking and Its Nuances in a Cultural Context,” *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 19.

SOTIS C., “Les principes de nécessité et de proportionnalité,” *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l’Union européenne au lendemain du Traité de Lisbonne*, Société de législation comparée, Collection de l’UMR de droit comparé de Paris no. 28, 2012, p. 59.

SPAPENS T., “The business of trafficking in human beings,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 535.

SPENCER J.R., “The Principle of Mutual Recognition,” *in* KOSTORIS R.E. (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, pp. 281-295, DOI:10.1007/978-3-319-72462-1_7.

STALLA-BOURDILLON S., “Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 275-293, DOI:10.1007/978-3-319-47852-4_15.

STEARNS J., “Street Gangs and Human Trafficking,” *in* PALMIOTTO M. (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 149.

STEVENSON M., “From Hypertext to Hype and Back Again: Exploring the Roots of Social Media in Early Web Culture,” *in* BURGESS J., MARWICK A. (eds.), *The Sage handbook of social media*, SAGE inc, 1st ed., 2017, p. 69.

STOYANOVA V., “European Court of Human Rights and the Right Not to Be Subjected to Slavery, Servitude, Forced Labor, and Human Trafficking,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1393-1407, DOI:10.1007/978-3-319-63058-8_94.

SURDEN H., “Ethics of AI in Law: Basic Questions,” *in* DUBBER M.D., PASQUALE F., DAS S. (eds.), *The Oxford Handbook of Ethics of AI*, Oxford University Press, July 9, 2020, pp. 718-736, DOI:10.1093/oxfordhb/9780190067397.013.46.

SYKIOTOU A., “Cyber trafficking: recruiting victims of human trafficking through the net,” *in* KOURAKĒS N.E., SPINELLIS C.D. (eds.), *Europe in crisis: crime, criminal justice, and the way forward: essays in honour of Nestor Courakis*, Ant. N. Sakkoulas Publications L.P., 2017.

TADDEO M., “The Civic Role of OSPs in Mature Information Societies,” *in* FROSIO G. (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, May 4, 2020, pp. 121-137, DOI:10.1093/oxfordhb/9780198837138.013.6.

TADDEO M., FLORIDI L., “New Civic Responsibilities for Online Service Providers,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 1-10, DOI:10.1007/978-3-319-47852-4_1.

TADDEO M., FLORIDI L., “The Moral Responsibilities of Online Service Providers,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 13-42, DOI:10.1007/978-3-319-47852-4_2.

TERRANOVA T., “Free Labor,” *in* SCHOLZ T. (ed.), *Digital labor: the Internet as playground and factory*, Routledge, 2013, p. 46.

TESSIER M., HERZOG J., MADZOU L., “Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness,” *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 175.

THIBIERGE C., “Le concept de 'force normative,'” *in* THIBIERGE C. (ed.), *La force normative : naissance d’un concept*, LGDJ-Lextenso éd. Bruylant, 2009, p. 813.

TOSZA S., “Cross-border gathering of electronic evidence: mutual legal assistance, its shortcomings and remedies,” *in* FRANSSEN V., FLORE D., STASIAK F. (eds.), *Société numérique et droit pénal : Belgique, France, Europe*, Bruylant, 2019, p. 269.

TRAUTMAN L., MOELLER M., “The Role of the Border and Border Policies in Efforts to Combat Human Trafficking: A Case Study of the Cascadia Region of the US-Canada Border,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 985-999, DOI:10.1007/978-3-319-63058-8_61.

TREGUER F., “Anonymat et chiffrement, composantes essentielles de la liberté de communication,” *in* VAN ENIS Q., DE TERWANGNE C. (eds.), *L’Europe des droits de l’homme à l’heure d’internet*, Emile Bruylant, 2018, p. 295.

TRICOT J., “L’hypothèse de la gouvernance pénale,” *in* ALIX J. et al. (eds.), *Humanisme et justice: mélanges en l’honneur de Geneviève Giudicelli-Delage*, Dalloz, 2016, pp. 1021-1037.

TROUNSON J., PFEIFER J., “The Human Trafficking of Men: The Forgotten Few,” *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 541-555, DOI:10.1007/978-3-319-63058-8_32.

TRUDEL P., “La lex electronica,” *in* MORAND C.-A. (ed.), *Le droit saisi par la mondialisation*, Bruylant; Helbing & Lichtenhahn, Collection de droit international no. 46, 2001, p. 221.

TULLOUE C., “L’irréalisable souveraineté française sur les données : quels enjeux économiques ?,” *in* TÜRK P., VALLAR C. (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 121.

TURÉGANO MANSILLA I., “La dimensión social de la privacidad en un entorno virtual,” *in* FUENTES SORIANO O., ARRABAL PLATERO P., ALCARAZ RAMOS M. (eds.), *Era digital, sociedad y derecho*, Tirant lo Blanch, Monografías, 2020, pp. 27-50.

TÜRK P., “La 'souveraineté numérique' : un concept pertinent en droit constitutionnel ?,” *in* TÜRK P., VALLAR C. (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 19.

TURNER J., “Root Causes, Transnational Mobility and Formations of Patriarchy in the Sex Trafficking of Women,” *in* MALLOCH M., RIGBY P. (eds.), *Human Trafficking: The Complexities of Exploitation*, Edinburgh University Press, 2016, pp. 194-209.

TUSIKOV N., “Revenue Chokepoints: Global Regulation by Payment Intermediaries,” *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 213.

TUSIKOV N., “Censoring Sex: Payment Platforms’ Regulation of Sexual Expression,” *in* DEFLEM M., M. D. SILVA D. (eds.), *Media and Law: Between Free Speech and Censorship*, Emerald Publishing Limited, Sociology of Crime, Law and Deviance, January 1, 2021, vol. 26, pp. 63-79, DOI:10.1108/S1521-613620210000026005.

VALCKE P., KUCZERAWY A., OMBELET P.-J., “Did the Romans Get It Right? What Delfi, Google, eBay, and UPC TeleKabel Wien Have in Common,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 101-116, DOI:10.1007/978-3-319-47852-4_6.

VALIÑO CES A., “El agente encubierto informático y la ciberdelincuencia. El intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil,” *in* BUENO DE MATA F. (ed.), *Fodertics 5.0.: estudios sobre nuevas tecnologías y justicia*, Comares, 2016, pp. 275-285.

VALLAR C., “La souveraineté numérique : rapport de synthèse,” *in* TÜRK P., VALLAR C. (eds.), *La souveraineté numérique : le concept, les enjeux*, 2018, p. 219.

VALLÉS CAUSADA L., “Utilidad de los datos conservados de las comunicaciones electrónicas para la resolución de emergencias,” *in* BUENO DE LA MATA F., DÍAZ MARTÍNEZ M., LÓPEZ-BARAJAS PEREA I. (eds.), *La nueva reforma procesal penal: derechos fundamentales e innovaciones tecnológicas*, Tirant lo blanch, Monografías, 2018, pp. 49-84.

VAN DE HEYNING C., “Data Retention in Belgium,” *in* ZUBIK M., PODKOWIK J., RYBSKI R. (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 53-74, DOI:10.1007/978-3-030-57189-4_4.

VAN DE KERCHOVE M., “Le principe de subsidiarité,” *in* GIUDICELLI-DELAGE G., LAZERGES C., ASSOCIATION DE RECHERCHES PENALES EUROPEENNES (eds.), *Le droit pénal de l’Union*

européenne au lendemain du Traité de Lisbonne, Société de législation comparée, Collection de l'UMR de droit comparé de Paris no. 28, 2012, p. 27.

VAN DER LEUN J., "(EU) Migration Policy and Labour Exploitation," *in* RIJKEN C. (ed.), *Combating trafficking in human beings for labour exploitation*, Wolf Legal Publishers, 2011, pp. 425-441.

VAN DER WATT M., "A Complex Systems Stratagem to Combating Human Trafficking," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 763-782, DOI:10.1007/978-3-319-63058-8_46.

VAN DER WATT M., KRUGER B., "Breaking Bondages: Control Methods, 'Juju,' and Human Trafficking," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 935-951, DOI:10.1007/978-3-319-63058-8_54.

VAN DIJCK J., "Guarding Public Values in a Connective World: Challenges for Europe," *in* BOYD-BARRETT O., MIRRLEES T. (eds.), *Media imperialism: continuity and change*, Rowman & Littlefield, 2020, pp. 175-186.

VAN DIJK J., "Measuring Trafficking in Persons Better: Problems and Prospects," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1671-1688, DOI:10.1007/978-3-319-63058-8_91.

VAN DOORNINCK M., "Changing the system from within The role of NGOs in the flawed antitrafficking framework," *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 419.

VAN ENIS Q., "Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression," *in* VAN ENIS Q., DE TERWANGNE C. (eds.), *L'Europe des droits de l'homme à l'heure d'internet*, Emile Bruylant, 2018, p. 133.

VAN MEETEREN M., BANNINK S., "A Transnational Field Approach to the Study of Labor Trafficking," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1751-1763, DOI:10.1007/978-3-319-63058-8_104.

VAN MEETEREN M., HIAH J., "Self-Identification of Victimization of Labor Trafficking," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1605-1618, DOI:10.1007/978-3-319-63058-8_86.

VAN RIJ J., MCALISTER R., "Using Criminal Routines and Techniques to Predict and Prevent the Sexual Exploitation of Eastern-European Women in Western Europe," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1689-1708, DOI:10.1007/978-3-319-63058-8_96.

VANCE C.S., "Pleasure and Danger: Toward a Politics of Sexuality," *in* VANCE C.S. (ed.), *Pleasure and danger: exploring female sexuality*, Pandora Press ; Distributed in North America by New York University Press, 1992, p. 1.

VEGAS TORRES J., "Las medidas de investigación tecnológica," *in* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017.

VELASCO NÚÑEZ E., "Medios de investigación y prueba en los delitos cometidos por persona jurídica," *in* JUANES PECES Á. (ed.), *Responsabilidad penal y procesal de las personas jurídicas*, Francis Lefebvre, Memento experto Francis Lefebvre, 2015, p. 2500.

VERNET PERNA B., "Estrategias de respuesta ante la criminalidad de empresas," *in* CARPIO DELGADO J. Del (ed.), *Criminalidad en un mundo global: criminalidad de empresa, transnacional, organizada y recuperación de activos*, Tirant lo Blanch, Monografías, 2020, pp. 33-62.

VILLACAMPA ESTIARTE C. et al., “Dimensión de la trata de seres humanos en España,” in ESTIARTE C.V., GARGALLO A.P. (eds.), *La trata de seres humanos tras un decenio de su incriminación: ¿es necesaria una ley integral para luchar contra la trata y la explotación de seres humanos?*, Tirant lo Blanch, 2022, pp. 181-216.

VILLACAMPA ESTIARTE C., “El delito de trata de seres humanos en derecho penal español tras la reforma de 2015,” *in* PÉREZ ALONSO E. (ed.), *El derecho ante las formas contemporáneas de esclavitud*, Tirant lo Blanch, Homenajes y congresos, 2017, pp. 447-467.

VILLACAMPA ESTIARTE C., “La trata de seres humanos para explotación sexual: relevancia penal y confluencia con la prostitución,” *in* VILLACAMPA ESTIARTE C., BARBERÀ I GOMIS J.R. (eds.), *Prostitución: ¿hacia la legalización?*, Tirant lo Blanch [u.a.], Tirant monografías no. 783, 2012, pp. 215-268.

VILLAMARÍN LÓPEZ M.L., “La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado,” *in* CEDEÑO HERNÁN M. (ed.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, Estudios, 1st ed., 2017.

VRANA J., SINGH R., “Digitization, Digitalization, and Digital Transformation,” *in* MEYENDORF N. et al. (eds.), *Handbook of Nondestructive Evaluation 4.0*, Springer International Publishing, 2021, pp. 1-17, DOI:10.1007/978-3-030-48200-8_39-1.

WALDMAN A.E., “Algorithmic Legitimacy,” *in* BARFIELD W. (ed.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, 1st ed., October 31, 2020, pp. 107-120, DOI:10.1017/9781108680844.

WEBER R.H., “Data Ownership in Platform Markets,” *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 147.

WEMMERS J.-A., CYR K., “Gender and Victims’ Expectations Regarding Their Role in the Criminal Justice System: Towards Victim-Centred Prosecutorial Policies,” *in* KURY H., REDO S., SHEA E. (eds.), *Women and Children as Victims and Offenders: Background, Prevention, Reintegration*, Springer International Publishing, 2016, pp. 233-248, DOI:10.1007/978-3-319-28424-8_9.

WENTRUP R., STRÖM P., “Online Service Providers: A New and Unique Species of the Firm?,” *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 157-177, DOI:10.1007/978-3-319-47852-4_9.

WEYEMBERGH A., “Enhanced cooperation in criminal matters: past, present and future,” *in* KERT R., LEHNER A. (eds.), *Vielfalt des Strafrechts im internationalen Kontext. Festschrift für Frank Höpfel zum 65. Geburtstag*, NWV Verlag, 1st ed., January 19, 2018, pp. 605-624.

WEYEMBERGH A., “History of the Cooperation,” *in* KOSTORIS R.E. (ed.), *Handbook of European Criminal Procedure*, Springer International Publishing, 2018, pp. 173-199, DOI:10.1007/978-3-319-72462-1_4.

WEYEMBERGH A., “Two crucial challenges in cross-border criminal investigations,” *in* CARRERA S., MITSILEGAS V., KING J. (eds.), *Constitutionalising the Security Union: effectiveness, rule of law and rights in countering terrorism and crime*, Centre for European Policy Studies (CEPS), 2017, p. 21.

WIJERS M., “Fifteen years lifting of the ban on brothels The struggle of policy makers between sex workers as agents or victims,” *in* PIOTROWICZ R.W., RIJKEN C., UHL B.H. (eds.), *Routledge handbook of human trafficking*, Routledge, Taylor & Francis Group, 2018, p. 487.

WILLIAMS P., “Trafficking in women: The role of transnational organized crime,” *in* CAMERON S., NEWMAN E. (eds.), *Trafficking in humans: social, cultural and political dimensions*, UN University Press, 2008, p. 126.

WINTERDYK J., "Explaining Human Trafficking: Modern Day-Slavery," *in* WINTERDYK J., JONES J. (eds.), *The Palgrave International Handbook of Human Trafficking*, Springer International Publishing, 2020, pp. 1257-1274, DOI:10.1007/978-3-319-63058-8_68.

WINTERDYK J., PERRIN B., REICHEL P.L., "Introduction," *in* WINTERDYK J., PERRIN B., REICHEL P.L. (eds.), *Human trafficking: exploring the international nature, concerns, and complexities*, CRC Press, 2012, p. 1.

YANNOPOULOS G.N., "The Immunity of Internet Intermediaries Reconsidered?," *in* TADDEO M., FLORIDI L. (eds.), *The Responsibilities of Online Service Providers*, Springer International Publishing, Law, Governance and Technology Series, 2017, vol. 31, pp. 43-59, DOI:10.1007/978-3-319-47852-4_3.

YIANNIBAS K., ROORDA L., "Introduction," *in* ALVAREZ RUBIO J.J., YIANNIBAS K. (eds.), *Human rights in business: removal of barriers to access to justice in the European Union*, Routledge, 2017, p. 1.

YU S., "Human Trafficking and the Internet," *in* PALMIOTTO M. (ed.), *Combating human trafficking: a multidisciplinary approach*, CRC Press, 2015, p. 61.

ZARKADAKIS G., "The Internet Is Dead: Long Live the Internet," *in* WERTHNER H. et al. (eds.), *Perspectives on Digital Humanism*, Springer International Publishing, 2022, pp. 47-52, DOI:10.1007/978-3-030-86144-5_7.

ZOLYNSKI C., "What Legal Framework for Data Ownership and Access? The French Digital Council's Opinion," *in* BELLI L., ZINGALES N. (eds.), *Platform regulations: how platforms are regulated and how they regulate us*, FGV Digital Repository, November 2017, p. 163.

ZUBIK M., PODKOWIK J., RYBSKI R., "Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remarks," *in* ZUBIK M., PODKOWIK J., RYBSKI R. (eds.), *European Constitutional Courts towards Data Retention Laws*, Springer International Publishing, Law, Governance and Technology Series, 2021, vol. 45, pp. 229-249, DOI:10.1007/978-3-030-57189-4_15.

ZÚÑIGA RODRÍGUEZ L., "Tratamiento jurídico penal de las sociedades instrumentales. Entre la criminalidad organizada y la criminalidad empresarial," *in* ZÚÑIGA RODRÍGUEZ L. (ed.), *Criminalidad organizada trasnacional: una amenaza a la seguridad de los estados democráticos*, Universidad de Salamanca, Ars iuris, 2017, pp. 197-246.

III. Fiction books

ALONSO A., PELEGRÍN J., *La torre y la isla*, Anaya, La llave del tiempo no. 1, 2006.

§2. Articles

ABEL SOUTO M., "Algunas discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el código penal español," *Revista General de Derecho Penal*, Iustel, 2021, no. 35, p. 1.

ABIZADEH A., "Democratic Legitimacy and State Coercion: A Reply to David Miller," *Political Theory*, 2010, vol. 38, no. 1, pp. 121-130.

ADAMS J., ALBAKAJAI M., "Cyberspace: A New Threat to the Sovereignty of the State," *Management Studies*, September 29, 2016, vol. 4, no. 6, pp. 256-265, DOI:10.17265/2328-2185/2016.06.003.

AFORI O., "Online Rulers as Hybrid Bodies: The Case of Infringing Content Monitoring," *University of Pennsylvania Journal of Constitutional Law*, April 2021, vol. 23, no. 2, pp. 350-408.

AGUSTINA J.R., “Sobre la utilización oculta de GPS en investigaciones criminales y detección de fraudes laborales: análisis jurisprudencial comparado en relación con el derecho a la intimidad,” *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2013, no. 102, p. 2.

AHMED A., SESHU M., “'We have the right not to be ‘rescued’...': When Anti-Trafficking Programmes Undermine the Health and Well-Being of Sex Workers,” *Anti-Trafficking Review*, June 1, 2012, no. 1, DOI:10.14197/atr.201219.

AKORRI S., “La responsabilité pénale des entreprises transnationales : de l’influence du droit international sur le droit national,” *Actualité juridique Pénal*, Dalloz, 2018, p. 556.

ALAPONT J.L., “Criminal Compliance: análisis de los arts. 31 bis 2 a 5 CP y 31 quater CP,” *Revista General de Derecho Penal*, Iustel, 2019, no. 31, p. 1.

ALAUZEN M., “L’Etat plateforme et l’identification numérique des usagers - Le processus de conception de FranceConnect,” *Réseaux*, La Découverte, 2019, vol. 2019/1, no. 213, pp. 2012-239.

ALBERT K. et al., “FOSTA in legal context,” *Columbia Human Rights Law Review*, Columbia University. School of Law, 2021, vol. 52, no. 3, pp. 1084-1158, DOI:10.3316/agispt.20210513046493.

ALBRIGHT E., D’ADAMO K., “Decreasing Human Trafficking through Sex Work Decriminalization,” *AMA Journal of Ethics*, January 2017, vol. 19, no. 1, pp. 122-126.

ALIX J., “Fallait-il étendre la compétence des juridictions pénales en matière terroriste ? (à propos de l’article 2 de la loi n° 2012-1432 du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme),” *Recueil Dalloz*, 2013, p. 518.

ALONSO LECUIT J., “El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea,” *Análisis del Real Instituto Elcano*, Real Instituto Elcano de Estudios Internacionales y Estratégicos, 2021, no. 4, p. 1.

ÁLVAREZ TEJERO A., “La solicitud de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación en el marco de la instrucción: reflexión sobre la Ley 25/2007,” *Revista de Jurisprudencia El Derecho*, May 1, 2014, no. 2.

ALVARI H., SHAKARIAN P., SNYDER J.E.K., “Semi-supervised learning for detecting human trafficking,” *Security Informatics*, December 2017, vol. 6, no. 1, p. 1, DOI:10.1186/s13388-017-0029-8.

AMAESHI K., OSUJI O., NNODIM P., “Corporate Social Responsibility in Supply Chains of Global Brands: A Boundaryless Responsibility? Clarifications, Exceptions and Implications,” *Journal of Business Ethics*, 2008, vol. 81, no. 1, pp. 223-234.

AMMORI M., “The 'new' 'New York Times': free speech lawyering in the age of Google and Twitter,” *Harvard Law Review*, The Harvard Law Review Association, 2014, vol. 127, no. 8, pp. 2259-2295.

AMORÓS PUENTE C., “Conceptualizar es politizar,” *Género, violencia y derecho*, Tirant lo Blanch, Alternativa, 2008, pp. 15-26.

ANDREWS S., BREWSTER B., DAY T., “Organised crime and social media: a system for detecting, corroborating and visualising weak signals of organised crime online,” *Security Informatics*, December 2018, vol. 7, no. 1, p. 3, DOI:10.1186/s13388-018-0032-8.

ANGELOPOULOS C., SMET S., “Notice-and-fair-balance: how to reach a compromise between fundamental rights in European intermediary liability,” *Journal of Media Law*, Routledge, December 6, 2016, vol. 8, no. 2, pp. 266-301, DOI:10.1080/17577632.2016.1240957.

ANIL KUMAR J., “The impact of human trafficking in ASEAN: Singapore as a case-study,” *Asian Journal of International Law*, Research Collection School Of Law, 2018, vol. 8, no. 1, pp. 189-224.

AÑÓN ROIG M.J., “Derechos sociales: cuestiones de legalidad y de legitimidad,” *Anales de la Cátedra Francisco Suárez*, Imprenta de Francisco Ventura y Sabatel, 2010, no. 44, pp. 15-41.

ARE C., “The Shadowban Cycle: an autoethnography of pole dancing, nudity and censorship on Instagram,” *Feminist Media Studies*, Routledge, May 19, 2021, vol. 0, no. 0, pp. 1-18, DOI:10.1080/14680777.2021.1928259.

ARE C., PAASONEN S., “Sex in the shadows of celebrity,” *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, pp. 411-419, DOI:10.1080/23268743.2021.1974311.

ARMSTRONG L., “Decriminalisation of sex work in the post-truth era? Strategic storytelling in neo-abolitionist accounts of the New Zealand model,” *Criminology & Criminal Justice*, SAGE Publications, July 1, 2021, vol. 21, no. 3, pp. 369-386, DOI:10.1177/1748895820918898.

ARMSTRONG L., “Decriminalisation and the rights of migrant sex workers in Aotearoa/New Zealand: Making a case for change,” *Women’s Studies Journal*, December 2017, vol. 31, no. 2, pp. 69-76.

ARMSTRONG L., “Sex worker rights activism and the decriminalisation of sex work in New Zealand,” *Routledge International Handbook of Sex Industry Research*, Routledge, 1st ed., 2018, pp. 138-147, 10 pages.

ARNAUD M., “Le WHOIS, talon d’Achille de la protection des données personnelles,” *Hermes, La Revue*, C.N.R.S. Editions, 2009, vol. 53, no. 1, pp. 104-108.

ARONOWITZ A., “Smuggling and Trafficking in Human Beings: The Phenomenon, The Markets that Drive It and the Organisations that Promote It,” *European Journal on Criminal Policy and Research*, 2001, vol. 9, no. 2, pp. 163-195, DOI:10.1023/A:1011253129328.

ARROYO AMAYUELAS E., “La responsabilidad de los intermediarios en internet ¿puertos seguros a prueba de futuro?,” *Cuadernos Derecho Transnacional*, 2020, vol. 12, no. 1, pp. 808-837.

ARROYO ZAPATERO L., “Quelle méthode pour une harmonisation pénale ?,” *Revue Européenne du Droit*, Groupe d’études géopolitiques, 2021, vol. 2, no. 1, pp. 7-13.

ASCIONE LE DREAU C., “QPC dans l’affaire EncroChat : des jours heureux pour Big Brother ? Décision rendue par Conseil constitutionnel,” *Actualité juridique Pénal*, Dalloz, 2022, p. 376.

ASSOCIATION INTERNATIONALE DE DROIT PENAL, “XV^{ème} congrès international de droit pénal (Rio de Janeiro, 4 – 10 septembre 1994),” *Revue internationale de droit pénal*, ERES, 2015, vol. 86, no. 2015/1, pp. 147-170.

AURIEL P., “La liberté d’expression et la modération des réseaux sociaux dans la proposition de Digital Services Act,” *Revue de l’Union européenne*, 2021, p. 413.

AVILA PINTO R., “Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies,” *Sur - International Journal on Human Rights*, July 16, 2018, vol. 15, no. 27, pp. 15-27.

AZCÁRRAGA MONZONÍS C., “La mujer inmigrante en la extranjería y el asilo,” *El principio de igualdad ante el derecho privado: una visión multidisciplinar*, Dykinson, 2013, pp. 237-262.

AZOULAI L., RITLENG D., “« L’État, c’est moi ». Le Conseil d’État, la sécurité et la conservation des données,” *Revue trimestrielle de droit européen*, 2021, p. 349.

BADIE B., “D’une souveraineté fictive à une post-souveraineté incertaine,” *Studia Diplomatica*, Egmont Institute, 2000, vol. 53, no. 5, pp. 5-13.

BADOUARD R., “Ce que peut l’État face aux plateformes,” *Pouvoirs*, April 27, 2021, vol. N° 177, no. 2, pp. 48-58.

BAILLEUX A., OST F., “Droit, contexte et interdisciplinarité : refondation d’une démarche,” *Revue interdisciplinaire d’études juridiques*, Université Saint-Louis - Bruxelles, 2013, vol. 70, no. 1, pp. 25-44, DOI:10.3917/riej.070.0025.

BAIN C., “Entrepreneurship and Innovation in the Fight Against Human Trafficking,” *Social Inclusion*, June 23, 2017, vol. 5, no. 2, pp. 81-84, DOI:10.17645/si.v5i2.924.

BALES K., LIZE S., “Investigating Human Trafficking,” *FBI Law Enforcement Bulletin*, April 2007, vol. 76, no. 4, p. 24.

BALFOUR A.W., “Where One Marketplace Closes, (Hopefully) Another Won’t Open: In Defense of FOSTA,” *Boston College Law Review*, 2019, vol. 60, no. 8, pp. 2474-2510.

BALKIN J., “Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation,” *University of California Davis Law Review*, January 1, 2018, vol. 51, pp. 1149-1210.

BALKIN J.M., “Old-school/New-school speech regulation,” *Harvard Law Review*, The Harvard Law Review Association, 2014, vol. 127, no. 8, pp. 2296-2342.

BARATA I MIR J., “Libertad de expresión, regulación y moderación privada de contenidos,” *Teoría y derecho: revista de pensamiento jurídico*, Tirant lo Blanch, 2022, no. 32, pp. 88-107.

BARBERIS J.A., “Les liens juridiques entre l’Etat et son territoire : perspectives théoriques et évolution du droit international,” *Annuaire français de droit international*, 1999, vol. 45, no. 1, pp. 132-147, DOI:10.3406/afdi.1999.3556.

BARNEY D., “Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking,” *Pepperdine Law Review*, 2018, vol. 45, no. 4, p. 746.

BARTELS M.R., “Programmed Defamation: Applying Sec. 230 of the Communications Decency Act to Recommendation Systems,” *Fordham Law Review*, 2020, vol. 89, no. 2, p. 650.

BARZILAI-NAHON K., “Toward a theory of network gatekeeping: A framework for exploring information control,” *Journal of the American Society for Information Science and Technology*, 2008, vol. 59, no. 9, pp. 1493-1512, DOI:10.1002/asi.20857.

BASSENS D., HENDRIKSE R., “Asserting Europe’s technological sovereignty amid American platform finance: Countering financial sector dependence on Big Tech?,” *Political Geography*, August 1, 2022, vol. 97, DOI:10.1016/j.polgeo.2022.102648.

BASSINI M., “Fundamental rights and private enforcement in the digital age,” *European Law Journal*, March 2019, vol. 25, no. 2, pp. 182-197, DOI:10.1111/eulj.12310.

BATTESTI A.M., “La coopération des plateformes,” *Legipresse*, 2019, vol. N° 61, no. HS1, pp. 44-48.

BAYART B., CORNULIER A. De, “La neutralité du net,” *Pouvoirs*, January 11, 2018, vol. N° 164, no. 1, pp. 127-136.

BEAUD O., “Le Souverain,” *Pouvoirs*, 1993, no. 67, pp. 33-45.

BEAUSSONIE G., “L’installation de la victime dans le procès pénal,” *Actualité juridique Pénal*, Dalloz, 2015, p. 526.

BECKERS A., “L’image juridique évolutive des chaînes de valeur mondiales Introduction au numéro spécial,” *Revue internationale de droit économique*, Association internationale de droit économique, 2021, vol. t. XXXV, no. 4, pp. 5-18, DOI:10.3917/ride.354.0005.

BECKERS A., “Chaînes de valeur mondiales : théorie et dogme des obligations de l’entreprise,” *Revue internationale de droit économique*, Association internationale de droit économique, 2021, vol. t. XXXV, no. 4, pp. 123-149, DOI:10.3917/ride.354.0123.

BEDUSCHI A., “The Big Data of International Migration: Opportunities and Challenges for States Under International Human Rights Law,” *Georgetown Journal of International Law*, 2018, vol. 49, no. 3, p. 980.

BELLANGER P., “Les données personnelles : une question de souveraineté,” *Le débat*, Gallimard, 2015, vol. 2015/1, no. 183, pp. 14-25.

BELLANGER P., “De la souveraineté numérique,” *Le débat*, Gallimard, 2012, vol. 2012/3, no. 170, pp. 149-159.

BELLET P., “La coopération judiciaire en matière de traite des êtres humains,” *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29.

BENOIT A., “Responsabilité pénale des personnes morales : l’auteur de l’infraction doit avoir la qualité d’organe ou de représentant de la société,” *Gazette du Palais*, Lextenso, April 3, 2018, no. 13, p. 50.

BERG L., FARBENBLUM B., KINTOMINAS A., “Addressing Exploitation in Supply Chains: Is technology a game changer for worker voice?,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 47-66, DOI:10.14197/atr.201220144.

BERGER S., “No End in Sight: Why the 'End Demand' Movement is the Wrong Focus for Efforts to Eliminate Human Trafficking,” *Harvard Journal of Law and Gender*, 2012, vol. 35, p. 523.

BERMAN J., “(Un)Popular Strangers and Crises (Un)Bounded: Discourses of Sex-trafficking, the European Political Community and the Panicked State of the Modern State,” *European Journal of International Relations*, SAGE Publications Ltd, March 1, 2003, vol. 9, no. 1, pp. 37-86, DOI:10.1177/1354066103009001157.

BERNSTEIN E., “Militarized Humanitarianism Meets Carceral Feminism: The Politics of Sex, Rights, and Freedom in Contemporary Antitrafficking Campaigns,” *Signs: Journal of Women in Culture and Society*, The University of Chicago Press, September 1, 2010, vol. 36, no. 1, pp. 45-71, DOI:10.1086/652918.

BERNSTEIN E., “Redemptive Capitalism and Sexual Investability,” *Perverse Politics? Feminism, Anti-Imperialism, Multiplicity*, Emerald Group Publishing Limited, Political Power and Social Theory, January 1, 2016, vol. 30, pp. 45-80, DOI:10.1108/S0198-871920160000030001.

BERTHIER P.-E., “Les incitations légales,” *Semaine sociale Lamy*, June 8, 2015, no. 1680 supplément, p. 36.

BILGIC S., “Something old, something new, and something moot: the privacy crisis under the cloud act,” *Harvard Journal of Law & Technology*, 2018, vol. 32, no. 1, p. 321.

BINION G., “Human Rights: A Feminist Perspective,” *Human Rights Quarterly*, Johns Hopkins University Press, 1995, vol. 17, no. 3, pp. 509-526.

BINSARD R. et al., “Secret-défense : la raison d’État et le droit,” *Dalloz Actualité*, October 6, 2021.

BIRKENTHAL S., “Human Trafficking: A Human Rights Abuse with Global Dimensions,” *Interdisciplinary Journal of Human Rights Law*, 2012 2011, vol. 6, no. 1, pp. 27-40.

BISMUTH R., “Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ?,” *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, no. 3, pp. 680-694.

BLACK J., “Critical Reflection on Regulation,” *Australian Journal of Legal Philosophy*, January 1, 2002, vol. 27.

BLACK J., “Decentring regulation: understanding the role of regulation and self regulation in a 'post-regulatory' world,” *Current Legal Problems*, Oxford University Press, February 21, 2001, vol. 54, no. 1, pp. 103-146.

BLACK J., “Constitutionalising Self-Regulation,” *Modern Law Review*, 1996, vol. 59, no. 1, pp. 24-55.

BLACK J., “Constructing and contesting legitimacy and accountability in polycentric regulatory regimes,” *Regulation & Governance*, 2008, vol. 2, no. 2, pp. 137-164, DOI:10.1111/j.1748-5991.2008.00034.x.

BLUNT D., STARDUST Z., “Automating whorephobia: sex, technology and the violence of deplatforming,” *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, pp. 350-366, DOI:10.1080/23268743.2021.1947883.

BLUNT D., WOLF A., “Erased: The impact of FOSTA-SESTA and the removal of Backpage on sex workers,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 117-121, DOI:10.14197/atr.201220148.

BOISTER N., “Human rights protections in the suppression conventions,” *Human Rights Law Review*, October 1, 2002, vol. 2, no. 2, pp. 199-227, DOI:10.1093/hrlr/2.2.199.

BONNITCHA J., MCCORQUODALE R., “The Concept of ‘Due Diligence’ in the UN Guiding Principles on Business and Human Rights,” *European Journal of International Law*, November 13, 2017, vol. 28, no. 3, pp. 899-919, DOI:10.1093/ejil/chx042.

BORN E.J., “Too Far and Not Far Enough: Understanding the Impact of FOSTA,” *New York University Law Review*, 2019, vol. 94, no. 6, pp. 1622-1653.

BOSSAN J., “Le droit pénal confronté à la diversité des intermédiaires de l’internet,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2013, p. 295.

BOSSAN J., “Les réquisitions judiciaires relatives aux données de connexion : suite... et fin ? Commentaire des dispositions issues de la loi du 2 mars 2022 visant à combattre le harcèlement scolaire,” *Droit pénal*, LexisNexis, August 2022, no. 7-8, pp. 9-14.

BOTTON A., “Droit au respect de la vie privée dans un cadre d’enquête : la stratégie d’évitement du Conseil constitutionnel,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 415.

BOUCHET M., “Les drones face aux enjeux de droit pénal et de libertés fondamentales,” *Dalloz IP/IT*, Dalloz, 2022, p. 299.

BOUNDS D. et al., “Uncovering Indicators of Commercial Sexual Exploitation,” *Journal of Interpersonal Violence*, December 2020, vol. 35, no. 23-24, pp. 5607-5623, DOI:10.1177/0886260517723141.

BOVENKERK F., VAN SAN M., “Loverboys in the Amsterdam Red Light District: A realist approach to the study of a moral panic,” *Crime, Media, Culture: An International Journal*, August 2011, vol. 7, no. 2, pp. 185-199, DOI:10.1177/1741659011412124.

BOYD d., “Social Network Sites: Public, Private, or What?,” *Knowledge Tree*, August 1, 2010, vol. 13.

BOYLE J., “Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors,” *University of Cincinnati Law Review*, January 1, 1997, vol. 66, pp. 177-205.

BOZA MORENO E., “La prostitución en España: el limbo de la alegalidad,” *Estudios Penales y Criminológicos*, September 8, 2019, vol. 39, DOI:10.15304/epc.39.5330.

BRACH-THIEL D., “Le nouvel article 113-13 du code pénal : contexte et analyse,” *Actualité juridique Pénal*, Dalloz, 2013, p. 90.

BRANSCUM C., CAIN C.M., FALLIK S.W., “Exploring the Nature of Anti-trafficking Laws: A Content Analysis of State Statutes,” *Journal of Human Trafficking*, Routledge, July 3, 2023, vol. 9, no. 3, pp. 348-362, DOI:10.1080/23322705.2021.1917213.

BRAUM S., “‘Rechtsstaat’ and European criminal law – From the end of sovereignty,” *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 1, 2021, vol. 12, no. 1, pp. 14-22, DOI:10.1177/2032284420973088.

BRAVO K.E., “Interrogating the State’s Role in Human Trafficking,” *Indiana International & Comparative Law Review*, 2015, vol. 25, no. 1, pp. 8-32.

BRAYLEY H., COCKBAIN E., LAYCOCK G., “The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking,” *Policing*, June 1, 2011, vol. 5, no. 2, pp. 132-143, DOI:10.1093/police/par024.

BREAKSTONE C., "'I Don't Really Sleep': Street-Based Sex Work, Public Housing Rights, and Harm Reduction Notes," *CUNY Law Review*, 2015 2014, vol. 18, no. 2, pp. 337-374.

BRECKENRIDGE K.D., "Justice Beyond Borders: A Comparison of Australian and U.S. Child-Sex Tourism Laws," *Pacific Rim Law & Policy Journal*, 2004, vol. 13, p. 404.

BRESLOW J., "Moderating the 'worst of humanity': sexuality, witnessing, and the digital life of coloniality," *Porn Studies*, Routledge, July 3, 2018, vol. 5, no. 3, pp. 225-240, DOI:10.1080/23268743.2018.1472034.

BRIDY A., "Internet Payment Blockades," *Florida Law Review*, October 10, 2016, vol. 67, no. 5, p. 1523.

BRIGHAM J., SCHREINER A.T.M., "The Semiotics of Digital Law Introduction," *International Journal for the Semiotics of Law*, 2004, vol. 17, no. 3, pp. 259-266.

BROEDERS D., CRISTIANO F., KAMINSKA M., "In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions," *JCMS: Journal of Common Market Studies*, 2023, pp. 1-20, DOI:10.1111/jcms.13462.

BRONSTEIN C., "Deplatforming sexual speech in the age of FOSTA/SESTA," *Porn Studies*, Routledge, October 2, 2021, vol. 8, no. 4, pp. 367-380, DOI:10.1080/23268743.2021.1993972.

BRONSTEIN C., "Pornography, Trans Visibility, and the Demise of Tumblr," *TSQ: Transgender Studies Quarterly*, May 1, 2020, vol. 7, no. 2, pp. 240-254, DOI:10.1215/23289252-8143407.

BROWN I., "Communications Data Retention in an Evolving Internet," *International Journal of Law and Information Technology*, July 5, 2010, vol. 19, no. 2, pp. 95-109.

BRUCH E.M., "Models wanted: The search for an effective response to human trafficking," *Stanford Journal of International Law*, 2004, vol. 40, p. 2.

BRUNET F., "La contrainte du droit," *Pouvoirs*, April 27, 2021, vol. N° 177, no. 2, pp. 70-82.

BUENO DE MATA F., "Protección de datos, investigación de infracciones penales e inteligencia artificial: novedades y desafíos a nivel nacional y europeo en la era postcovid," *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2021, no. 150, p. 6.

BUFFELAN-LANORE Y., "Domicile, demeure et logement familial," *Répertoire de droit civil*, Dalloz, December 2019.

BUHMANN K., "Neglecting the Proactive Aspect of Human Rights Due Diligence? A Critical Appraisal of the EU's Non-Financial Reporting Directive as a Pillar One Avenue for Promoting Pillar Two Action," *Business and Human Rights Journal*, January 2018, vol. 3, no. 1, pp. 23-45, DOI:10.1017/bhj.2017.24.

BUISSON J., "Contrôle de l'éventuelle provocation policière : création d'un site pédo-pornographique un policier, même étranger," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 663.

BULEA C.-D., "Cooperarea judiciară în materie penală şi respectarea drepturilor omului. Probleme actuale. Probele electronice," *Caiete de drept penal*, 2021, vol. XVII, no. 1, p. 73.

BURDA E., TRELLOVA L., "Admissibility of an Agent Provocateur and an Advocate Acting as an Agent Law," *Balkan Social Science Review*, 2019, vol. 14, pp. 54-80.

BURETH O., "Responsabilité pénale des personnes morales et fusion-absorption : le grand chambardement ou comment créer une hydre !," *Petites affiches*, Lextenso, January 7, 2021, no. 5, p. 5.

BURNITIS C., "Facing the Future with FOSTA: Examining the Allow States and Victims to Fight Online Sex Trafficking Act of 2017," *University of Miami Race and Social Justice Law Review*, 2020, vol. 10, no. 2, pp. 138-166.

BURRELL J., “How the machine ‘thinks’: Understanding opacity in machine learning algorithms,” *Big Data & Society*, SAGE Publications Ltd, June 1, 2016, vol. 3, no. 1, pp. 1-12, DOI:10.1177/2053951715622512.

BUSCH C., “Regulating the Expanding Content Moderation Universe: A European Perspective on Infrastructure Moderation Special Issue: Governing the Digital Space,” *UCLA Journal of Law and Technology*, 2022, vol. 27, no. 2, pp. 32-79.

BYK C., “L’ère du numérique conduit-elle à l’émergence de nouveaux acteurs et formes de souveraineté ?,” *Cahiers Droit, Sciences & Technologies*, PUP, November 17, 2022, no. 15, pp. 171-192, DOI:10.4000/cdst.6859.

CAHN O., “Réflexions désabusées sur le chapitre I du titre I de la loi n° 2016-731 du 3 juin 2016,” *Actualité juridique Pénal*, Dalloz, 2016, p. 408.

CALDERARO A., BLUMFELDE S., “Artificial intelligence and EU security: the false promise of digital sovereignty,” *European Security*, Routledge, July 3, 2022, vol. 31, no. 3, pp. 415-434, DOI:10.1080/09662839.2022.2101885.

CARBONELL MATEU J.C., “Responsabilidad penal de las personas jurídicas: reflexiones en torno a su 'dogmática' y al sistema de la reforma de 2010,” *Cuadernos de política criminal*, Dykinson, 2010, no. 101, pp. 5-33.

CARNEY E., “Protecting Internet Freedom at the Expense of Facilitating Online Child Sex Trafficking: An Explanation as to Why CDA’s Section 230 Has No Place in a New NAFTA,” *Catholic University Law Review*, 2019, vol. 68, no. 2, pp. 352-378.

CARUANA R. et al., “Modern Slavery in Business: The Sad and Sorry State of a Non-Field,” *Business & Society*, SAGE Publications Inc, February 1, 2021, vol. 60, no. 2, pp. 251-287, DOI:10.1177/0007650320930417.

CASILLI A.A., “Digital Labor Studies Go Global: Toward a Digital Decolonial Turn,” *International Journal of Communication*, 2017, vol. 11, no. Special section ”Global Digital Culture”, pp. 3934-3954.

CASTETS-RENARD C., “Le renouveau de la responsabilité délictuelle des intermédiaires de l’internet,” *Recueil Dalloz*, 2012, p. 827.

CASTETS-RENARD C., “Régulation des algorithmes et gouvernance du machine learning : vers une transparence et 'explicabilité' des décisions algorithmiques ?,” *Revue Droit&Affaires*, Revue Paris II Assas, November 2018, no. 15, p. 32.

CASTETS-RENARD, C., “Quelle politique européenne de l’intelligence artificielle ?,” *Revue trimestrielle de droit européen*, 2021, p. 296.

CASTETS-RENARD C., NDIOR V., RASS-MASSON L., “Le marché unique numérique : quelles réalités matérielles et conceptuelles ?,” *Recueil Dalloz*, Dalloz, 2019, no. 17, p. 956.

CATELAN N., “Opération économique et responsabilité pénale des personnes morales : revirement de jurisprudence,” *Gazette du Palais*, Lextenso, March 16, 2021, no. 11, p. 51.

CHAFFAUT B.A.D., “Droit au déréférencement : mise en œuvre et zones d’ombre,” *Legipresse*, 2019, vol. N° 61, no. HS1, pp. 14-20.

CHAMBERLAIN J., “The Risk-Based Approach of the European Union’s Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective,” *European Journal of Risk Regulation*, Cambridge University Press, December 5, 2022, pp. 1-13, DOI:10.1017/err.2022.38.

CHAMBERLAIN L., “FOSTA: A Hostile Law with a Human Cost,” *Fordham Law Review*, 2019, vol. 87, no. 5, pp. 2170-2212.

CHAPMAN-SCHMIDT B., “‘Sex Trafficking’ as Epistemic Violence,” *Anti-Trafficking Review*, 2019, no. 12, pp. 172-187.

CHARPENET J., “Plateformes digitales et Etats : la corégulation par les données. Le cas des requêtes gouvernementales,” *Revue internationale de droit économique*, 2019, vol. 2019/2, no. XXXIII, pp. 362-381.

CHATZIS I., “Traite, esclavage et travail forcé au XXIe siècle : un état des lieux,” *Diplomatie*, December 2020, no. 106, p. 42.

CHEMAIN R., “La relation juridique des GAFA avec l’Union européenne,” *Revue de l’Union européenne*, Dalloz, 2023, no. 665, p. 90.

CHEN I., TORTOSA C., “The Use of Digital Evidence in Human Trafficking Investigations,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 122-124, DOI:10.14197/atr.201220149.

CHEN S., “Corporate Responsibilities in Internet-Enabled Social Networks,” *Journal of Business Ethics*, Springer, 2009, vol. 90, pp. 522-536.

CHO S.-Y., “Evaluating Policies Against Human Trafficking Worldwide: An Overview and Review of the 3P Index,” *Journal of Human Trafficking*, January 2, 2015, vol. 1, no. 1, pp. 83-99, DOI:10.1080/23322705.2015.1014660.

CHO S.-Y., DREHER A., NEUMAYER E., “Does Legalized Prostitution Increase Human Trafficking?,” *World Development*, January 2013, vol. 41, pp. 67-82, DOI:10.1016/j.worlddev.2012.05.023.

CHONE-GRIMALDI A.-S., “Digital Services Act - Vers un nouveau droit de la concurrence et de la régulation applicable au secteur numérique ?,” *La Semaine Juridique Edition Générale*, November 30, 2020, no. 49, p. 2179.

CHOUCRI N., CLARK D.D., “Who controls cyberspace?,” *Bulletin of the Atomic Scientists*, SAGE Publications, September 1, 2013, vol. 69, no. 5, pp. 20-31, DOI:10.1177/0096340213501370.

CHRIST K.L., BURRITT R.L., “Current perceptions on the problem of modern slavery in business,” *Business Strategy & Development*, June 2018, vol. 1, no. 2, pp. 103-114, DOI:10.1002/bsd2.15.

CHRISTAKIS T., “La communication aux autorités américaines de données sur la base du Cloud Act est-elle en conflit avec le règlement général sur la protection des données ?,” *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, no. 3, pp. 694-707.

CHRISTAKIS T., TERPAN F., “EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options,” *International Data Privacy Law*, 2021, p. 1, DOI:10.1093/idpl/ipaa022.

CHRISTODOULOU H., GAURIER L., MORNET A., “La proposition e-evidence: révélatrice des limites de l’émergence d’une procédure pénale européenne ou compromis nécessaire?,” *European Papers - A Journal on Law and Integration*, June 30, 2021, vol. 2021 6, no. 1, pp. 423-439, DOI:10.15166/2499-8249/476.

CHUANG J., “The United States as Global Sheriff: Using Unilateral Sanctions to Combat Human Trafficking,” *Michigan Journal of International Law*, 2006, vol. 27, no. 2, pp. 437-494, 58 pages.

CHUANG J., “Giving as Governance? Philanthrocapitalism and Modern-Day Slavery Abolitionism,” *UCLA law review*, August 1, 2015, vol. 62, pp. 1516-1556.

CITRON D., WITTES B., “The Problem Isn’t Just Backpage: Revising Section 230 Immunity,” *Georgetown Law Technology Review*, July 1, 2018, vol. 2, no. 2, p. 453.

CITRON D., WITTES B., “The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity,” *Fordham Law Review*, November 1, 2017, vol. 86, no. 2, p. 400.

CITRON D.K., “Technological Due Process,” *Washington University Law Review*, January 1, 2008, vol. 85, no. 6, pp. 1248-1313.

COFFEE JR. J.C., “No Soul to Damn: No Body to Kick: An Unscandalized Inquiry into the Problem of Corporate Punishment,” *Michigan Law Review*, 1981, vol. 79, no. 3, pp. 385-459.

COHEN J.E., “Law for the Platform Economy,” *University of California, Davis Law Review*, 2017, vol. 51, p. 132.

COHEN J.E., “Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt,” *Georgetown Law Faculty Publications and Other Works*, March 13, 2017, vol. 4, no. 1.

COHEN-ALMAGOR R., “Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications,” *Journal of Business Ethics*, March 2012, vol. 106, no. 3, pp. 353-365, DOI:10.1007/s10551-011-1001-z.

COLLET P., “Le renforcement progressif des garanties applicables à deux mesures intrusives : la géolocalisation et la sonorisation,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2021, p. 29.

COLLIOT-THELENE C., “La fin du monopole de la violence légitime ?,” *Revue d’études comparatives Est-Ouest*, Persée - Portail des revues scientifiques en SHS, 2003, vol. 34, no. 1, pp. 4-31, DOI:10.3406/receo.2003.1594.

COLLIOT-THELENE C., “Violence et contrainte,” *Lignes*, Éditions Hazan, 1995, vol. n° 25, no. 2, pp. 263-279.

COMBACAU J., “Pas une puissance, une liberté : la souveraineté internationale de l’Etat,” *Pouvoirs*, 1993, no. 67, pp. 47-58.

COMBE E., “Les plateformes : notion, enjeux et pistes d’évolution,” *L’émergence d’un droit des plateformes*, Editions Dalloz, 2021, p. 15.

COMERFORD T., “Pornography Isn’t the Problem: A Feminist Theoretical Perspective on the War against Pornhub Notes,” *Boston College Law Review*, 2022, vol. 63, no. 3, pp. 1177-1225.

CONAC P.-H., “Sustainable Corporate Governance in the EU: Reasonable Global Ambitions?,” *La Revue Européenne du Droit*, October 27, 2022, vol. 4, no. 1, pp. 111-118.

CONTE P., “Refus de remettre une convention secrète de déchiffrement d’un moyen de cryptologie. Notion de réquisition,” *Droit pénal*, LexisNexis, January 1, 2023, no. 1, p. 31.

CONTE P., “Groupe de sociétés : responsabilité pénale de la société-mère,” *Droit pénal*, LexisNexis, September 2021, no. 9, p. 25.

COOPER A., “Sexuality and the Internet: Surfing into the New Millennium,” *CyberPsychology & Behavior*, January 1998, vol. 1, no. 2, pp. 187-193, DOI:10.1089/cpb.1998.1.187.

CORENO E., “Finding the Line between Choice and Coercion: An Analysis of Massachusetts’s Attempt to Define Sex Trafficking,” *Northeastern University Law Review*, 2021, vol. 13, no. 1, pp. 124-174.

CORHAY M., “Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal,” *European Papers - A Journal on Law and Integration*, June 30, 2021, vol. 2021 6, no. 1, pp. 441-471, DOI:10.15166/2499-8249/477.

COWEN N., COLOSI R., “Sex work and online platforms: what should regulation do?,” *Journal of Entrepreneurship and Public Policy*, Emerald Publishing Limited, January 1, 2020, vol. 10, no. 2, pp. 284-303, DOI:10.1108/JEPP-03-2019-0009.

CRICHTON C., “Projet de règlement sur l’IA (I) : des concepts larges retenus par la Commission,” *Dalloz Actualité*, Dalloz, May 3, 2021.

CRUYSMANS E., “Airbnb, un service de la société de l’information,” *Les Pages : obligations, contrats et responsabilités*, 2020, vol. 2020, no. 71, p. 3.

CRUYSMANS E., “Oubli, anonymisation, déréférencement. Cachez-moi ces informations que je ne veux plus voir en ligne !,” *Bulletin social et juridique*, 2018, vol. 617, no. 1, pp. 7-10.

CRUYSMANS É., “Le droit à l’oubli devant la Cour européenne des droits de l’homme : l’intégration d’une composante temporelle dans un litige vie privée/liberté d’expression,”

Revue trimestrielle des droits de l'Homme, Anthemis, 2022, vol. 129, no. 1, pp. 161-182, DOI:10.3917/rtdh.129.0161.

CRUZ ÁNGELES J., "Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso," *Cuadernos de derecho transnacional*, September 29, 2022, vol. 14, no. 2, pp. 294-318, DOI:10.20318/cdt.2022.7186.

CSERNATONI R., "The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty," *European Security*, Routledge, July 3, 2022, vol. 31, no. 3, pp. 395-414, DOI:10.1080/09662839.2022.2103370.

CUOMO D., DOLCI N., "New tools, old abuse: Technology-Enabled Coercive Control (TECC)," *Geoforum*, November 1, 2021, vol. 126, pp. 224-232, DOI:10.1016/j.geoforum.2021.08.002.

D'AMBROSIO L., "Le devoir de vigilance : une innovation juridique entre continuités et ruptures," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 632-647.

D'AMBROSIO L., LAGERIE P.B. De, "La responsabilité des entreprises reformulée par la loi : un regard pluridisciplinaire," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 622-631.

DALTON R., "Abolishing child sex trafficking on the internet: Imposing criminal culpability on digital facilitators," *University of Memphis Law Review*, 2013, vol. 43, no. 4, pp. 1096-1144.

DANLOS B., "Le débat d'intérêt général dans la jurisprudence de la Cour EDH relative à la liberté d'expression," *LEGICOM*, October 4, 2017, vol. 58, no. 1, pp. 12-18.

DAOUD E., ANDRE A., "La responsabilité pénale des entreprises transnationales françaises : fiction ou réalité juridique ?," *Actualité juridique Pénal*, Dalloz, 2012, p. 15.

DARLEY M., "Le statut de la victime dans la lutte contre la traite des femmes," *Critique internationale*, 2006, vol. 30, no. 1, pp. 101-122.

DARLEY M., "Le proxénétisme en procès, réaffirmation d'un ordre sexuel national," *Sexualité, savoirs et pouvoirs*, Les Presses de l'Université de Montréal, Universanté, 2019, pp. 155-165.

DARLEY M., "Entre droit et culture, l'exploitation sexuelle en procès," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 93-122.

DASKAL J., "Borders and Bits," *Vanderbilt Law Review*, 2018, no. 71, p. 179.

DASKAL J., "Unpacking the CLOUD Act," *Eucrim*, 2018, no. 4, pp. 220-225, DOI:10.30709/eucrim-2018-022.

DAUM C.W., "Sex, Laws, and Cyberspace: Organized Interest Litigation Before the U.S. Supreme Court," *The Justice System Journal*, Taylor & Francis, Ltd., 2006, vol. 27, no. 3, pp. 302-322.

DAUPS T., "Pour une charte constitutionnelle de la robotique et des nouvelles technologies," *Petites affiches*, Lextenso, October 6, 2017, no. 200, p. 7.

DE COOMAN J., "Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act," *Market and Competition Law Review*, March 23, 2022, vol. 6, no. 1, pp. 49-88, DOI:10.34632/mclawreview.2022.11304.

DE LA CHAPELLE B., "Souveraineté et juridiction dans le cyberespace," *Hérodote*, La découverte, 2014, vol. 2014/1, no. 152-153, pp. 174-184.

DE MONTECLER M.-C., "Conservation des données : la guerre des juges n'aura pas lieu," *Dalloz Actualité*, Dalloz, April 26, 2021.

DE VRIES I., DETTMEIJER-VERMEULEN C., "Extremely wanted: human trafficking statistics—what to do with the hodgepodge of numbers?," *Forum on Crime and Society*, UNODC, 2015, vol. 8, pp. 15-36.

DE VRIES I., REID J.A., FARRELL A., "From Responding to Uncertainties and Ambiguities to More Constructive and Inclusive Debates on Commercial Sex and Sex Trafficking," *Victims &*

Offenders, Routledge, April 3, 2023, vol. 18, no. 3, pp. 586-606, DOI:10.1080/15564886.2022.2151539.

DECAUX E., "La responsabilité des sociétés transnationales en matière de droits de l'homme," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2005, p. 789.

DECIMA O., "Du piratage informatique aux perquisitions et saisies numériques," *Actualité juridique Pénal*, Dalloz, 2017, p. 315.

DECIMA O., "Terreur et métamorphose À propos de la loi n° 2016-731 du 3 juin 2016 sur la lutte contre le terrorisme," *Recueil Dalloz*, Dalloz, 2016, no. 31, p. 1826.

DEERING K.N. et al., "A Systematic Review of the Correlates of Violence Against Sex Workers," *American Journal of Public Health*, American Public Health Association, May 2014, vol. 104, no. 5, pp. 42-54, DOI:10.2105/AJPH.2014.301909.

DELALIEUX G., "La loi sur le devoir de vigilance des sociétés multinationales : parcours d'une loi improbable," *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 648-665.

DELATEUR M.J., "From Craigslist to Backpage.com: Conspiracy as a Strategy to Prosecute Third-Party Websites for Sex Trafficking," *Santa Clara Law Review*, 2016, vol. 56, no. 3, p. 530.

DELMAS-MARTY M., "Le droit pénal comme éthique de la mondialisation," *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2004, p. 1.

DELMAS-MARTY M., "Personnes morales étrangères et françaises (Questions de droit pénal international)," *Revue des sociétés*, Dalloz, 1993, p. 255.

DE MONTVALON P., "« Venir ici n'est pas gratuit ! » Négocier un passage aux frontières extérieures et intérieures de la France pour des prostituées nigérianes," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 17-46.

DESFORGES A., DETERVILLE E., "Lexique sur le cyberespace," *Hérodote*, La découverte, 2014, vol. 2014/1, no. 152-153, pp. 22-25.

DIAMANTIS M.E., "The Extended Corporate Mind: When Corporations Use AI to Break the Law," *North Carolina Law Review*, 2020 2019, vol. 98, no. 4, pp. 893-932.

DIAS OLIVA T., "Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression," *Human Rights Law Review*, December 9, 2020, vol. 20, no. 4, pp. 607-640, DOI:10.1093/hrlr/ngaa032.

DÍAZ Y GARCÍA CONLLEDO M., "El complicado régimen privilegiado del art. 30 del Código Penal Español en materia de codelincuencia y encubrimiento en los delitos cometidos utilizando medios o soportes de difusión mecánicos," *Nuevo Foro Penal*, Universidad EAFIT, 2013, vol. 9, no. 81, pp. 68-92, 68-92 pages, DOI:10.17230/nfp.9.81.2.

DIEZ VELASCO I., "La protección de personas víctimas de trata en el anteproyecto de Ley Orgánica Integral contra la Trata y la Explotación de Seres Humanos: el caso de la infancia y las personas solicitantes de asilo," *IgualdadES*, June 20, 2023, vol. 8, pp. 141-168, DOI:10.18042/cepc/IgdES.8.05.

DOEZEMA J., "Loose women or lost women? The re-emergence of the myth of white slavery in contemporary discourses of trafficking in women," *Gender Issues*, December 1999, vol. 18, no. 1, pp. 23-50, DOI:10.1007/s12147-999-0021-9.

DOEZEMA J., "Now You See Her, Now You Don't: Sex Workers at the UN Trafficking Protocol Negotiation," *Social & Legal Studies*, SAGE Publications Ltd, March 1, 2005, vol. 14, no. 1, pp. 61-89, DOI:10.1177/0964663905049526.

DÖLEMEYER A., LESER J., "Entre coopération et conflit," *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 45-65.

DONNAT F., "Droit à l'oubli," *La semaine juridique édition générale*, LexisNexis, October 7, 2019, no. 41, p. 1818.

DONOVAN E.M., “Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act: A Shield for Jane Doe,” *Connecticut Law Review*, 2020, vol. 52, no. 1, p. 83.

DOREY R., “La relation d’emprise,” *Troubles de la personnalité*, Dunod, Psychothérapies, 2013, pp. 88-112, DOI:10.3917/dunod.couta.2013.01.0088.

DOUPLITZKY K., “Le commerce du moi, modèle économique du profilage,” *Hermes, La Revue*, C.N.R.S. Editions, 2009, vol. 53, no. 1, pp. 112-117.

DREYER E., “Les OPJ peuvent filmer dans l’espace public sans limite ni contrôle judiciaire,” *La Semaine Juridique Edition Générale*, LexisNexis, July 10, 2023, no. 27, p. 834.

DREYER E., “Responsabilité pénale des personnes morales : à la recherche de l’organe et du représentant perdus,” *Gazette du Palais*, Lextenso, September 14, 2021, no. 31, p. 37.

DUBRAWSKI A. et al., “Leveraging Publicly Available Data to Discern Patterns of Human-Trafficking Activity,” *Journal of Human Trafficking*, January 2, 2015, vol. 1, no. 1, pp. 65-85, DOI:10.1080/23322705.2015.1015342.

DUCLERCQ J.-B., “Le droit public à l’ère des algorithmes,” *Revue du droit public*, Lextenso, September 1, 2017, no. 5, p. 1401.

DUMONT H., “Criminalité collective et principaux responsables : échec ou mutation du droit pénal ? Conclusion,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2012, vol. 1, no. 1, pp. 109-129, DOI:10.3917/rsc.1201.0109.

DUNIN-WASOWICZ J., BOURGIN A., BURNICHON N., “Entreprises et droits humains à l’aune de l’autonomie stratégique européenne,” *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, p. 15.

DURISIN E., VAN DER MEULEN E., “The Perfect Victim: ‘Young girls’, domestic trafficking, and anti-prostitution politics in Canada,” *Anti-Trafficking Review*, April 29, 2021, no. 16, pp. 145-149, DOI:10.14197/atr.201221169.

DUSHI D., “Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo,” *International Review of Law, Computers & Technology*, January 2, 2018, vol. 32, no. 1, pp. 80-98, DOI:10.1080/13600869.2018.1431871.

DYZENHAUS D., “Kelsen, Heller and Schmitt: Paradigms of Sovereignty Thought,” *Theoretical Inquiries in Law*, 2015, vol. 16, no. 2, pp. 336-366.

EABRASU M., “Les états de la définition wébérienne de l’État,” *Raisons politiques*, Presses de Sciences Po, May 4, 2012, vol. 45, no. 1, pp. 187-209.

ECKERT S., “The Business Transparency on Trafficking and Slavery Act: Fighting Forced Labor in Complex Global Supply Chains,” *Journal of International Business and Law*, 2013, vol. 12, no. 2, pp. 382-416.

EDWARDS L., VEALE M., “Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For,” *Duke Law & Technology Review*, December 4, 2017, vol. 16, no. 1, pp. 18-84.

ELKIN-KOREN N., “Contesting algorithms: Restoring the public interest in content filtering by artificial intelligence,” *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, pp. 1-13, DOI:10.1177/2053951720932296.

ELLIOTT J., MCCARTAN K., “The Reality of Trafficked People’s Access to Technology,” *The Journal of Criminal Law*, June 2013, vol. 77, no. 3, pp. 255-273, DOI:10.1350/jcla.2013.77.3.843.

EMERIC N., “Droit souple + droit fluide = droit liquide. Réflexion sur les mutations de la normativité juridique à l’ère des flux,” *Revue interdisciplinaire d’études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, no. 2, pp. 5-38, DOI:10.3917/riej.079.0005.

ESSER L., DETTMEIJER-VERMEULEN C., “The Prominent Role of National Judges in Interpreting the International Definition of Human Trafficking,” *Anti-Trafficking Review*, 2016, vol. 6, pp. 91-105.

EYSENBACH G., TILL J.E., “Ethical issues in qualitative research on internet communities,” *BMJ*, November 10, 2001, vol. 323, no. 7321, pp. 1102-1105, DOI:10.1136/bmj.323.7321.1103.

EZELL L., “Human Trafficking in Multinational Supply Chains: A Corporate Director’s Fiduciary Duty to Monitor and Eliminate Human Trafficking Violations,” *Vanderbilt Law Review*, 2016, vol. 69, no. 2, pp. 498-544.

FARLEY M., “'Bad for the Body, Bad for the Heart': Prostitution Harms Women Even if Legalized or Decriminalized,” *Violence Against Women*, SAGE Publications Inc, October 1, 2004, vol. 10, no. 10, pp. 1085-1125, DOI:10.1177/1077801204268607.

FARRELL A., OWENS C., MCDEVITT J., “New laws but few cases: understanding the challenges to the investigation and prosecution of human trafficking cases,” *Crime, Law and Social Change*, March 2014, vol. 61, no. 2, pp. 139-168, DOI:10.1007/s10611-013-9442-1.

FAVAREL-GARRIGUES G., MATHIEU L., “Proxénètes en procès,” *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 65-93.

FEENBERG A., “Technique et agency,” *Revue du MAUSS*, La Découverte, June 12, 2014, vol. n° 43, no. 1, pp. 169-180.

FEHRENBACHER A.E. et al., “Transgender People and Human Trafficking: Intersectional Exclusion of Transgender Migrants and People of Color from Anti-trafficking Protection in the United States,” *Journal of Human Trafficking*, Routledge, March 14, 2020, vol. 6, no. 2, pp. 182-194, DOI:10.1080/23322705.2020.1690116.

FERGUSON A., “Sex War: The Debate between Radical and Libertarian Feminists,” *Signs: Journal of Women in Culture and Society*, University of Chicago Press, 1984, vol. 10, no. 1, pp. 106-112, DOI:10.1086/494117.

FERNÁNDEZ MÁRQUEZ J., “Esclavitud, trata de personas y explotación: una perspectiva desde los derechos humanos,” *El Cotidiano*, Universidad Autónoma Metropolitana, Unidad Azcapotzalco, 2018, vol. 34, no. 209, pp. 47-56.

FERNÁNDEZ RODRÍGUEZ J.J., “Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente,” *Revista Española de Derecho Constitucional*, December 14, 2016, no. 108, pp. 93-122, DOI:10.18042/cepc/redc.108.03.

FERNÁNDEZ TERUELO J.G., “Responsabilidad penal de las personas jurídicas: el contenido de las obligaciones de supervisión, organización, vigilancia y control referidas en el art. 31 bis 1. b) del Código Penal español,” *Revista electrónica de ciencia penal y criminología*, Universidad de Granada, 2019, no. 21, p. 3.

FILIBERTI E., “Le droit comparé tient une place grandissante dans notre société,” *Petites affiches*, March 14, 2006, no. 52, p. 3.

FORGET C., “Les nouvelles méthodes d’enquête dans un contexte informatique : vers un encadrement (plus) strict ?,” *Revue du droit des technologies de l’information*, 2017, no. 66/67, p. 25.

FORRINGER-BEAL A., “Why the ‘Ideal Victim’ Persists: Queering representations of victimhood in human trafficking discourse,” *Anti-Trafficking Review*, September 27, 2022, no. 19, pp. 87-102, DOI:10.14197/atr.201222196.

FOUCAULT M., “Des espaces autres. Hétérotopies. Conférence au Cercle d’études architecturales,” *Architecture, Mouvement, Continuité*, 1984, no. 5, pp. 46-49.

FRALEY A., “Child Sex Tourism Legislation Under the PROTECT Act: Does It Really Protect?,” *St. John’s Law Review*, 2005, vol. 79, no. 2, p. 444.

FRANCILLON J., “Le droit pénal face à la cyberdélinquance et à la cybercriminalité,” *Revue Lamy Droit de l’immatériel*, April 1, 2012, no. 81.

FRANCILLON J., “Provocation à la commission d’actes de pédophilie organisée par un service de police étranger utilisant le réseau internet (suite),” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2008, p. 621.

FRANCILLON J., “Cyberdélinquance et provocations policières,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2014, p. 577.

FRANSSEN V., “The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level Reports: Practitioner’s Corner,” *European Data Protection Law Review*, 2017, vol. 3, no. 4, pp. 534-542.

FRASER C., “An analysis of the emerging role of social media in human trafficking: Examples from labour and human organ trading,” *International Journal of Development Issues*, July 4, 2016, vol. 15, no. 2, pp. 98-112, DOI:10.1108/IJDI-12-2015-0076.

FRASER N., GORDON L., “'Dependency' Demystified: Inscriptions of Power in a Keyword of the Welfare State,” *Social Politics: International Studies in Gender, State & Society*, March 1, 1994, vol. 1, no. 1, pp. 4-31, DOI:10.1093/sp/1.1.4.

FRISON-ROCHE M.-A., “Gouvernance d’internet: 'Nous sommes face à un enjeu de civilisation,'” *Petites affiches*, Lextenso, July 18, 2019, no. 143, p. 4.

FROSIO G.F., “Why keep a dog and bark yourself? From intermediary liability to responsibility,” *International Journal of Law and Information Technology*, March 1, 2018, vol. 26, no. 1, pp. 0-33, DOI:10.1093/ijlit/eax021.

FROSIO G.F., “The Death of ‘No Monitoring Obligations’: A Story of Untameable Monsters,” *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, November 30, 2017, vol. 8, no. 3.

FUCHS C., “Social Media and the Public Sphere,” *TripleC: Communication, Capitalism & Critique*, February 19, 2014, vol. 12, no. 1, pp. 57-101, DOI:10.31269/triplec.v12i1.552.

FUCHS C., “Towards an alternative concept of privacy,” *Journal of Information, Communication and Ethics in Society*, Emerald Group Publishing Limited, January 1, 2011, vol. 9, no. 4, pp. 219-237, DOI:10.1108/14779961111191039.

FUCINI S., “Vidéosurveillance sur la voie publique durant l’enquête : conditions d’autorisation,” *Dalloz Actualité*, Dalloz, January 6, 2021.

FUCINI S., “Vidéosurveillance sur la voie publique durant l’enquête : conditions de réalisation,” *Dalloz Actualité*, Dalloz, January 18, 2019.

GALLAGHER A.T., “Human Rights and Human Trafficking: Quagmire or Firm Ground? A Response to James Hathaway,” *Virginia Journal of International Law*, 2009, vol. 49, no. 4, pp. 789-848.

GALLAGHER A.T., “Improving the Effectiveness of the International Law of Human Trafficking: A Vision for the Future of the US Trafficking in Persons Reports,” *Human Rights Review*, Springer, 2011, vol. 12, no. 3, pp. 381-400, DOI:10.1007/s12142-010-0183-6.

GALLOIS A., “Fusion-absorption : revirement spectaculaire de la chambre criminelle de la Cour de cassation !,” *Gazette du Palais*, Lextenso, March 30, 2021, no. 13, p. 50.

GARCÍA SEDANO T., “La tercería locativa: obligaciones, retos y riesgos,” *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2022, no. 156, p. 4.

GARCÍA-MARTÍNEZ J.M., “Trata de Seres Humanos y Jurisdicción Universal,” *Revista Aranzadi de Derecho y Proceso Penal*, Autumn 2023, vol. 69.

GAUDEMET Y., “De la compliance à la vigilance : les entreprises au secours de l’État ?,” *La Semaine Juridique Edition Générale*, LexisNexis, May 29, 2023, no. 21, p. 649.

GAUTIER P.-Y., “La preuve hors la loi ou comment, grâce aux nouvelles technologies, progresse la 'vie privée' des salariés,” *Recueil Dalloz*, Dalloz, 2001, p. 3148.

GENÇ-GELGEÇ B., “Regulating Digital Platforms: Will the DSA Correct Its Predecessor’s Deficiencies?,” *Croatian Yearbook of European Law and Policy*, November 16, 2022, vol. 18, p. 25−60-25−60.

GERRARD Y., THORNHAM H., “Content moderation: Social media’s sexist assemblages,” *New Media & Society*, SAGE Publications, July 1, 2020, vol. 22, no. 7, pp. 1266-1286, DOI:10.1177/1461444820912540.

GERRY QC F., MURASZKIEWICZ J., VAVOULA N., “The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns,” *Computer Law & Security Review*, April 2016, vol. 32, no. 2, pp. 205-217, DOI:10.1016/j.clsr.2015.12.015.

GEZINSKI L.B., GONZALEZ-PONS K.M., “Sex Trafficking and Technology: A Systematic Review of Recruitment and Exploitation,” *Journal of Human Trafficking*, Routledge, February 15, 2022, vol. 0, no. 0, pp. 1-15, DOI:10.1080/23322705.2022.2034378.

GILBERT L., “Présentation : Regards sur les nouvelles technologies,” *Revue d’anthropologie du contemporain*, Altérités, 2008, vol. 5, no. 1, pp. 1-13.

GILLESPIE T., “Platforms Are Not Intermediaries,” *Georgetown Law Technology Review*, July 21, 2018, vol. 2, pp. 198-216.

GILLESPIE T., “Content moderation, AI, and the question of scale,” *Big Data & Society*, SAGE Publications Ltd, July 1, 2020, vol. 7, no. 2, pp. 1-5, DOI:10.1177/2053951720943234.

GIOMMONI L., IKWU R., “Identifying human trafficking indicators in the UK online sex market,” *Trends in Organized Crime*, September 17, 2021, DOI:10.1007/s12117-021-09431-0.

GODSEY N., “The Next Step: Why Non-Governmental Organizations Must Take a Growing Role in the New Global Anti-Trafficking Framework,” *Regent Journal of International Law*, 2012 2011, vol. 8, no. 1, pp. 26-56.

GOGORZA A., “L’accès aux données de connexion : les affres du pluralisme normatif,” *Droit pénal*, LexisNexis, October 2022, no. 10, p. 20.

GOLDMAN E., “The complicated story of FOSTA and section 320,” *First Amendment Law Review*, 2019, vol. 17, p. 279.

GOMEZ-JARA DIEZ C., “Corporate Culpability as a Limit to the Overcriminalization of Corporate Criminal Liability: The Interplay between Self-Regulation, Corporate Compliance, and Corporate Citizenship,” *New Criminal Law Review*, 2011, vol. 14, no. 1, pp. 78-96.

GORWA R., BINNS R., KATZENBACH C., “Algorithmic content moderation: Technical and political challenges in the automation of platform governance,” *Big Data & Society*, SAGE Publications Ltd, January 1, 2020, vol. 7, no. 1, pp. 1-15, DOI:10.1177/2053951719897945.

GOTLIEB A., DALFEN C., KATZ K., “The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles,” *American Journal of International Law*, Cambridge University Press, April 1974, vol. 68, no. 2, pp. 226-257, DOI:10.2307/2199651.

GRAW LEARY M., “Fighting Fire with Fire: Technology in Child Sex Trafficking,” *Duke Journal of Gender Law & Policy*, 2014, vol. 21, pp. 288-323.

GRAW LEARY M., “The Indecency and Injustice of Section 230 of the Communications Decency Act,” *Harvard Journal of Law & Public Policy*, 2018, vol. 41, no. 2, p. 552.

GREENBERG J.D., BROTMAN E.C., “Strict Vicarious Criminal Liability for Corporations and Corporate Executives: Stretching the Boundaries of Criminalization Symposium: Reducing Corporate Criminality: Evaluating Department of Justice Policy on the Prosecution of Business Organizations and Options for Reform,” *American Criminal Law Review*, 2014, vol. 51, no. 1, pp. 79-98.

GREIMAN V., BAIN C., “The Emergence of Cyber Activity as a Gateway to Human Trafficking,” *International Journal of Cyber Warfare and Terrorism*, 2012, vol. 12, no. 2, pp. 41-49.

GRIFFIN R., “Rethinking rights in social media governance: human rights, ideology and inequality,” *European Law Open*, Cambridge University Press, March 2023, vol. 2, no. 1, pp. 30-56, DOI:10.1017/elo.2023.7.

GRIFFITHS C., JACKSON A., “Intercepted Communications as Evidence: The Admissibility of Material Obtained from the Encrypted Messaging Service EncroChat: R v A, B, D & C [2021] EWCA Crim 128,” *Journal of Criminal Law*, 2022, vol. 86, no. 4, pp. 271-276, DOI:10.1177/00220183221113455.

GRIMMELMANN J., “The Virtues of Moderation,” *Yale Journal of Law and Technology*, 2015, vol. 17, no. 1, p. 42.

G’SELL F., “Remarques sur les aspects juridiques de la « souveraineté numérique »,” *La revue des juristes de Sciences Po*, 2020, no. 19, p. 52.

GUERRIER C., “« Loppsi 2 » et l’utilisation des nouvelles technologies,” *Revue Le Lamy Droit de l’immatériel*, October 1, 2010, no. 64.

GUILHAUMOU J., “Autour du concept d’agentivité,” *Rives méditerranéennes*, TELEMME (UMR 6570), February 29, 2012, no. 41, pp. 24-34, DOI:10.4000/rives.4108.

GUISASOLA LERMA C., “Prevención y represión penal del delito de trata: una aproximación al anteproyecto de Ley Orgánica integral contra la trata y la explotación,” *Revista Española de Empresas y Derechos Humanos*, July 2023, no. 1, pp. 37-62.

GUTIÉRREZ CASTILLO V.L., “Aproximación a la protección jurídica internacional del derecho de acceso y protección de datos en Europa,” *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, Facultad de Derecho, 2005, no. 3, pp. 31-40.

GUTIÉRREZ CASTILLO V.L., “El control europeo del ciberespacio ante el discurso de odio: análisis de las medidas de lucha y prevención,” *Araucaria: Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, Universidad de Sevilla, 2020, vol. 22, no. 45, pp. 291-310.

GUYOMAR M., “Souveraineté des États et responsabilité partagée dans l’application de la Convention européenne des droits de l’homme,” *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, p. 5.

HAAK D.M., “Re(de)fining Prostitution and Sex Work: Conceptual Clarity for Legal Thinking,” *Windsor Review of Legal and Social Issues*, February 13, 2019, vol. 40, pp. 67-112.

HALLEY J.E. et al., “From the International to the Local Feminist Legal Responses to Rape, Prostitution/Sex Work and Sex Trafficking: Four Studies in Contemporary Governance Feminism,” *Harvard Women’s Law Journal*, 2006, vol. 29, no. 2, p. 335.

HALVERSON H.C., “The Communications Decency Act: Immunity For Internet-Facilitated Commercial Sexual Exploitation,” *Dignity: A Journal on Sexual Exploitation and Violence*, February 2018, vol. 3, no. 1, p. 12, DOI:10.23860/dignity.2018.03.01.12.

HARBOTTLE QUIRÓS F., “El agente encubierto informático: Reflexiones a partir de la experiencia española,” *Revista Judicial, Poder Judicial de Costa Rica*, 2021, no. 131, pp. 123-140.

HARCOURT C., DONOVAN B., “The many faces of sex work,” *Sexually Transmitted Infections*, June 1, 2005, vol. 81, no. 3, pp. 201-206, DOI:10.1136/sti.2004.012468.

HARDY B., “Application dans l’espace de la directive 95/46/CE : la géographie du droit à l’oubli Commentaire de l’arrêt de la Cour de justice dans l’affaire Google Spain et Google (C-131/12),” *Revue trimestrielle de droit européen*, 2014, p. 879.

HARDY K., BARBAGALLO C., “Hustling the Platform: Capitalist Experiments and Resistance in the Digital Sex Industry,” *South Atlantic Quarterly*, Duke University Press, July 2021, vol. 120, no. 3, pp. 533-551, DOI:10.1215/00382876-9154898.

HARRÉ T., “Human Traffickers’ Fair Trial Rights and Transnational Criminal Law,” *Anti-Trafficking Review*, April 19, 2022, no. 18, pp. 159-173, DOI:10.14197/atr.2012221810.

HARRIS D., “Corporate Intent and the Concept of Agency,” *Stanford Journal of Law, Business & Finance*, 2022, vol. 27, no. 1, pp. 133-172.

HATCHUEL A., SEGRESTIN B., “Devoir de vigilance : la norme de gestion comme source de droit ?,” *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 666-682.

HAUSMAN J.-M., “La prostitution des personnes majeures dans la réforme du droit pénal sexuel belge : les premiers jalons d’un modèle néo-réglementariste,” *Actualité juridique Pénal*, Dalloz, January 2023, p. 23.

HAUTEREAU-BOUTONNET M., PARANCE B., “Prudence dans l’analyse du premier jugement sur le devoir de vigilance des entreprises ! - À propos du projet pétrolier en Ouganda et Tanzanie des filiales de TotalEnergies,” *La Semaine Juridique Edition Générale*, LexisNexis, March 27, 2023, no. 12, p. 373.

HE D., “Governing Hate Content Online: How the Rechtsstaat Shaped the Policy Discourse on the NetzDG in Germany,” *International Journal of Communication*, June 29, 2020, vol. 14, no. 0, p. 23.

HEIL E., NICHOLS A., “Hot spot trafficking: a theoretical discussion of the potential problems associated with targeted policing and the eradication of sex trafficking in the United States,” *Contemporary Justice Review*, Routledge, October 2, 2014, vol. 17, no. 4, pp. 421-433, DOI:10.1080/10282580.2014.980966.

HELDT A., “Reading between the lines and the numbers: an analysis of the first NetzDG reports,” *Internet Policy Review*, June 12, 2019, vol. 8, no. 2.

HELDT A., “Let’s Meet Halfway: Sharing New Responsibilities in a Digital Age,” *Journal of Information Policy*, Penn State University Press, 2019, vol. 9, pp. 335-369, DOI:10.5325/jinfopoli.9.2019.0336.

HENDERSON A.C., RHODES S.M., “'Got Sold a Dream and It Turned into a Nightmare': The Victim-Offender Overlap in Commercial Sexual Exploitation,” *Journal of Human Trafficking*, Routledge, January 2, 2022, vol. 8, no. 1, pp. 33-48, DOI:10.1080/23322705.2021.2019530.

HERRAN T., “La nouvelle compétence française en matière de terrorisme - Réflexions sur l’article 113-13 du Code pénal,” *Droit pénal*, April 2013, no. 4, p. étude 10.

HERT P.D., KOPCHEVA M., “International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case,” *Computer Law & Security Review*, Elsevier Limited, 2011, vol. 27, no. 3, pp. 291-297.

HORNING A., STALANS L., “Oblivious ‘Sex Traffickers’: Challenging stereotypes and the fairness of US trafficking laws,” *Anti-Trafficking Review*, April 19, 2022, no. 18, pp. 67-86, DOI:10.14197/atr.201222185.

HORTON B., “The Hydraulics of Intermediary Liability Regulation,” *Cleveland State Law Review*, 2022 2021, vol. 70, no. 2, pp. 201-272.

HOYER J., “Sex trafficking in the digital age: The role of virtual currency-specific legislation in keeping pace with technology,” *Wayne Law Review*, 2017, vol. 63, pp. 82-104.

HUBBARD P., “Cleansing the Metropolis: Sex Work and the Politics of Zero Tolerance,” *Urban Studies*, SAGE Publications Ltd, August 1, 2004, vol. 41, no. 9, pp. 1687-1702, DOI:10.1080/0042098042000243101.

HUBBARD P., MATTHEWS R., SCOULAR J., “Regulating sex work in the EU: prostitute women and the new spaces of exclusion,” *Gender, Place & Culture*, April 2008, vol. 15, no. 2, pp. 137-152, DOI:10.1080/09663690701863232.

HUET A., “Le droit pénal et internet,” *Petites affiches*, November 10, 1999, no. 224, p. 39.

HUGHES D.M., “Trafficking in Human Beings in the European Union: Gender, Sexual Exploitation, and Digital Communication Technologies,” *SAGE Open*, December 18, 2014, vol. 4, no. 4, p. 215824401455358, DOI:10.1177/2158244014553585.

IGLESIAS VILA M., “Subsidiarity, margin of appreciation and international adjudication within a cooperative conception of human rights,” *International Journal of Constitutional Law*, April 1, 2017, vol. 15, no. 2, pp. 393-413, DOI:10.1093/icon/mox035.

IOANNOU M., OOSTINGA M., “An empirical framework of control methods of victims of human trafficking for sexual exploitation,” *Global Crime*, January 2015, vol. 16, no. 1, pp. 34-39.

IRION K., “Government Cloud Computing and National Data Sovereignty,” *Policy & Internet*, 2012, vol. 4, no. 3-4, pp. 40-71, DOI:10.1002/poi3.10.

IRWIN M.A., “'White Slavery' As Metaphor Anatomy of a Moral Panic,” *Ex Post Facto: The History Journal*, 1996, vol. V.

IZORCHE M.-L., “Propositions méthodologiques pour la comparaison,” *Revue internationale de droit comparé*, 2001, vol. 53, no. 2, pp. 288-325, DOI:10.3406/ridc.2001.17977.

JACKSON C.A., HEINEMAN J., “Repeal FOSTA and Decriminalize Sex Work,” *Contexts*, August 2018, vol. 17, no. 3, pp. 74-75, DOI:10.1177/1536504218792534.

JACOB P., “La compétence des États à l’égard des données numériques - Du nuage au brouillard… en attendant l’éclaircie ?,” *Revue critique de droit international privé*, Dalloz, 2019, vol. 2019/3, no. 3, pp. 664-680.

JÄGERS N., RIJKEN C., “Prevention of Human Trafficking for Labor Exploitation: The Role of Corporations,” *Northwestern Journal of International Human Rights*, 2014, vol. 12, no. 1, pp. 46-73.

JAKSIC M., “« Tu peux être prostituée et victime de la traite »,” *Plein droit*, March 18, 2013, vol. 96, no. 1, pp. 18-22.

JAKSIC M., “Le mérite et le besoin,” *Terrains travaux*, September 17, 2013, vol. 22, no. 1, pp. 200-216.

JAKSIC M., “Figures de la victime de la traite des êtres humains : de la victime idéale à la victime coupable,” *Cahiers internationaux de sociologie*, July 4, 2008, vol. n° 124, no. 1, pp. 127-146.

JAKSIC M., RAGARU N., “Réparer l’exploitation sexuelle. Le dispositif d’indemnisation des victimes de traite en France,” *Cultures & Conflits*, November 8, 2021, vol. 122, no. 2, pp. 121-140.

JAMET J.-F., “L’Europe au défi de la souveraineté technologique,” *La revue des juristes de Sciences Po*, LexisNexis, March 2022, no. 22, p. 13.

JARRETT K., LIGHT B., “Puritanisme sexuel et capitalisme numérique,” *Revue Française de Socio-Économie*, La Découverte, 2020, vol. 25, no. 2, tran. VÖRÖS F., pp. 166-174, DOI:10.3917/rfse.025.0167.

JIANG M. et al., “Digital technology adoption for modern slavery risk mitigation in supply chains: An institutional perspective,” *Technological Forecasting and Social Change*, July 1, 2023, vol. 192, p. 122595, DOI:10.1016/j.techfore.2023.122595.

JIMENEZ G.A., “Corporate Criminal Liability: Toward a Compliance-Oriented Approach Notes,” *Indiana Journal of Global Legal Studies*, 2019, vol. 26, no. 1, pp. 353-380.

JIMENO BULNES M.J., “La responsabilidad penal de las personas jurídicas y los modelos de compliance: un supuesto de anticipación probatoria,” *Revista General de Derecho Penal*, Iustel, 2019, no. 32, p. 6.

JOHNSON D.R., POST D., “Law and Borders - The Rise of Law in Cyberspace,” *Stanford Law Review*, May 1996, vol. 48, no. 5, p. 1367.

JOLIN A., “On the Backs of Working Prostitutes: Feminist Theory and Prostitution Policy,” *Crime & Delinquency*, SAGE Publications Inc, January 1, 1994, vol. 40, no. 1, pp. 69-83, DOI:10.1177/0011128794040001005.

JOMNI A., “Le Conseil de l’Europe face aux défis de la lutte contre la cybercriminalité,” *Revue de la gendarmerie nationale*, December 2018, no. 263, p. 5.

JONES M., “Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw,” *Journal of law, technology & policy*, 2018, vol. 2, pp. 249-284, DOI:10.2139/ssrn.2981855.

JOVANOVIC M., “The Essence of Slavery: Exploitation in Human Rights Law,” *Human Rights Law Review*, December 9, 2020, vol. 20, no. 4, pp. 674-703, DOI:10.1093/hrlr/ngaa023.

KAESLING K., “Privatising Law Enforcement in Social Networks: A Comparative Model Analysis,” *Erasmus Law Review*, March 20, 2019, vol. 11, no. 3, pp. 151-164, DOI:10.5553/ELR.000115.

KANTOLA J., SQUIRES J., “From state feminism to market feminism?,” *International Political Science Review*, SAGE Publications Ltd, September 1, 2012, vol. 33, no. 4, pp. 382-400, DOI:10.1177/0192512111432513.

KAPUR R., “The Tragedy of Victimization Rhetoric: Resurrecting the 'Native' Subject in International/Post-Colonial Feminist Legal Politics,” *Harvard Human Rights Journal*, 2002, vol. 15, no. 1, pp. 1-37.

KASAKOWSKIJ T. et al., “Network enforcement as denunciation endorsement? A critical study on legal enforcement in social media,” *Telematics and Informatics*, March 2020, vol. 46, p. 101317, DOI:10.1016/j.tele.2019.101317.

KATZENBACH C., “'AI will fix this' – The Technical, Discursive, and Political Turn to AI in Governing Communication,” *Big Data & Society*, SAGE Publications Ltd, July 1, 2021, vol. 8, no. 2, pp. 1-8, DOI:10.1177/20539517211046182.

KEBIR M., “Compétence territoriale : accessibilité d’un site internet à l’origine d’un dommage,” *Dalloz Actualité*, Dalloz, November 6, 2017.

KEIGHLEY R., SANDERS T., “Prevention of modern slavery within sex work: Study protocol of a mixed methods project looking at the role of adult services websites,” *PLOS ONE*, May 18, 2023, vol. 18, no. 5, p. e0285829, DOI:10.1371/journal.pone.0285829.

KELLY L., “'You Can Find Anything You Want': A Critical Reflection on Research on Trafficking in Persons within and into Europe,” *International Migration*, 2005, vol. 43, no. 1/2, pp. 235-265.

KEMPADOO K., “The Modern-Day White (Wo)Man’s Burden: Trends in Anti-Trafficking and Anti-Slavery Campaigns,” *Journal of Human Trafficking*, Routledge, January 2, 2015, vol. 1, no. 1, pp. 8-20, DOI:10.1080/23322705.2015.1006120.

KERR P.L., “Push and Pull: The Intersections of Poverty, Health Disparities, and Human Trafficking,” *Public Health & Social Justice, Cancer InCytes Magazine*, 2014, vol. 3, no. 2, pp. 1-5.

KETTANI G., “Quand l’algorithme écrit le droit : les conséquences de la nouvelle normativité numérique,” *Dalloz IP/IT*, Dalloz, 2022, p. 552.

KINLEY D., TADAKI J., “From Talk to Walk: The Emergence of Human Rights Responsibilities for Corporations at International Law,” *Virginia Journal of International Law*, 2004, vol. 44, no. 4, pp. 931-1024.

KISS L. et al., “The use of Bayesian networks for realist evaluation of complex interventions: evidence for prevention of human trafficking,” *Journal of Computational Social Science*, May 2021, vol. 4, no. 1, pp. 25-48, DOI:10.1007/s42001-020-00067-8.

KJELLGREN R., “Good Tech, Bad Tech: Policing Sex Trafficking with Big Data,” *International Journal for Crime, Justice and Social Democracy*, March 1, 2022, vol. 11, no. 1, pp. 149-166, DOI:10.5204/ijcjsd.2139.

KLOESS J.A., BEECH A.R., HARKINS L., “Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics,” *Trauma, Violence, & Abuse*, April 2014, vol. 15, no. 2, pp. 125-139, DOI:10.1177/1524838013511543.

KLONICK K., “The new governors: the people, rules, and processes governing online speech,” *Harvard Law Review*, 2018, vol. 131, p. 1598.

KONRAD R., TRAPP A., PALMBACH T., “Overcoming Human Trafficking via Operations Research and Analytics: Opportunities for Methods, Models, and Applications,” *European Journal of Operational Research*, June 1, 2017, vol. 259, no. 2, pp. 733-745.

KORPISAARI P., “From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act,” *Journal of Media Law*, Routledge, November 24, 2022, vol. 0, no. 0, pp. 1-26, DOI:10.1080/17577632.2022.2148335.

KOSTA E., “The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection,” *SCRIPTed*, October 4, 2013, vol. 10, no. 3, pp. 339-363, DOI:10.2966/scrip.100313.339.

KRAGTEN-HEERDINK S.L.J., DETTMEIJER-VERMEULEN C.E., KORF D.J., “More Than Just 'Pushing and Pulling': Conceptualizing Identified Human Trafficking in the Netherlands,” *Crime & Delinquency*, December 1, 2018, vol. 64, no. 13, pp. 1765-1789, DOI:10.1177/0011128717728503.

KRIEG S.H., “Trafficking in Human Beings: The EU Approach between Border Control, Law Enforcement and Human Rights,” *European Law Journal*, 2009, vol. 15, no. 6, pp. 775-790, DOI:10.1111/j.1468-0386.2009.00490.x.

KRSMANOVIĆ E., “Child Trafficking vs. Child Sexual Exploitation: Critical reflection on the UK media reports,” *Anti-Trafficking Review*, April 29, 2021, no. 16, pp. 69-85, DOI:10.14197/atr.201221165.

KWET M., “Digital colonialism: US empire and the new imperialism in the Global South,” *Race & Class*, SAGE Publications Ltd, April 1, 2019, vol. 60, no. 4, pp. 3-26, DOI:10.1177/0306396818823172.

LAGERIE P.B. De et al., “La mise en œuvre du devoir de vigilance : une managérialisation de la loi ?,” *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 698-714.

LAGON M.P., “The Global Abolition of Human Trafficking: The Indispensible Role of the United States,” *Georgetown Journal of International Affairs*, 2011, vol. 12, no. 1, pp. 88-98.

LAIDLAW E.B., “Private Power, Public Interest: An Examination of Search Engine Accountability,” *International Journal of Law and Information Technology*, March 1, 2009, vol. 17, no. 1, pp. 113-145, DOI:10.1093/ijlit/ean018.

LAMPE A., “De la difficile qualification des sites collaboratifs aux limites du statut d’hébergeur prévu par la LCEN,” *Revue Lamy Droit de l’Immatériel*, June 1, 2008, no. 39.

LAND M.K., “Toward an International Law of the Internet,” *Harvard International Law Journal*, 2013, vol. 54, no. 2, pp. 393-458.

LANDAIS C., “Cyberdéfense : quelle stratégie pour la France ?,” *Cahiers français*, La documentation française, June 2020, no. 415, p. 68.

LANNIER S., “Using US Artificial Intelligence to Fight Human Trafficking in Europe. Potential Impacts on European Sovereignties,” *Eucrim*, 2023, vol. 01/2023, DOI:10.30709/eucrim-2023-002.

LARKIN J.E.D., “Criminal and Civil Liability for User Generated Content: Craigslist, a Case Study,” *Journal of Technology Law & Policy*, June 2010, vol. 15, no. 1, pp. 84-112.

LASSERRE CAPDEVILLE J., “La notion d’organe ou de représentant de la personne morale,” *Actualité juridique Pénal*, Dalloz, 2018, p. 550.

LAURENT X., “Captation de données numériques : une étape significative dans la consolidation du régime de l’article 706-102-1 du code de procédure pénale,” *Dalloz IP/IT*, Dalloz, 2022, p. 578.

LAVAUD-LEGENDRE B., “Des qualifications applicables à la prostitution des mineurs organisée en Plans,” *Actualité juridique Pénal*, Dalloz, January 2023, p. 17.

LAVAUD-LEGENDRE B., “La coopération répressive en matière de traite des êtres humains - Du droit à sa mise en oeuvre,” *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29.

LAZERGES C., “La dérive de la procédure pénale,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2003, p. 644.

LAZERGES C., “Le déclin du droit pénal : l’émergence d’une politique criminelle de l’ennemi,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 649.

LAZERGES C., “Des modèles de politique criminelle aux mouvements et systèmes de politique criminelle,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, vol. 3, no. 3, pp. 533-540, DOI:10.3917/rsc.2203.0533.

LE CLAINCHE J., “CJUE : le droit à l’oubli n’est pas inconditionnel,” *Revue Le Lamy Droit de l’immatériel*, August 1, 2014, no. 107.

LE COZ N., “Tu coopéreras sans retard et dans la plénitude de tes obligations Bilan sur les principales difficultés rencontrées dans la coopération internationale contre la traite des êtres humains,” *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29.

LE E., “La construction juridique de la prostitution. Trois récits différenciés,” *Cahiers du Genre*, December 15, 2014, vol. 57, no. 2, pp. 138-158.

LEBARON G., RÜHMKORF A., “Steering CSR Through Home State Regulation: A Comparison of the Impact of the UK Bribery Act and Modern Slavery Act on Global Supply Chain Governance,” *Global Policy*, 2017, vol. 8, no. S3, pp. 15-28, DOI:10.1111/1758-5899.12398.

LECOURT B., “Vers une directive sur le devoir de vigilance des sociétés - Résolution du Parlement européen du 10 mars 2021 contenant des recommandations à la Commission sur le devoir de vigilance et la responsabilité des entreprises, P9_TA-PROV(2021)0073, (2020/2129(INL),” *Revue des sociétés*, Dalloz, 2021, p. 335.

LEDERMAN E., “Corporate Criminal Liability: The Second Generation,” *Stetson Law Review*, 2017 2016, vol. 46, no. 1, pp. 71-88.

LEISEGANG D., “No country for free speech?: An old libel law and a new one aimed at social media are two threats to free expression in Germany,” *Index on Censorship*, SAGE Publications Ltd, July 1, 2017, vol. 46, no. 2, pp. 76-78, DOI:10.1177/0306422017716038.

LEPAGE A., “Provocation sur Internet - La distinction entre provocation à la preuve et provocation à la commission d’une infraction à l’épreuve d’Internet,” *Communication Commerce électronique*, September 2014, no. 9.

LEPAGE A., “Enquête sous pseudonyme sur les réseaux numériques,” *Communication Commerce électronique*, April 2018, no. 4, p. comm. 29.

LEPAGE A., “Un an de droit pénal du numérique (Octobre 2019 – Octobre 2020),” *Droit pénal*, LexisNexis, December 2012, no. 12, p. 11.

LESSIG L., “The Zones of Cyberspace,” *Stanford Law Review*, May 1996, vol. 48, no. 5, pp. 1403-1411.

LESSIG L., “Reading The Constitution in Cyberspace,” *Emory Law Journal*, 1996, vol. 45, no. 3.

LESSIG L., “The Law of the Horse: What Cyberlaw Might Teach,” *Harvard Law Review*, The Harvard Law Review Association, 1999, vol. 113, no. 2, pp. 501-549, DOI:10.2307/1342331.

LEVY A.F., “The virtues of unvirtuous spaces,” *Wake Forest Law Review*, 2017, vol. 52, p. 403.

LEWIS J.A., “Sovereignty and the Role of Government in Cyberspace,” *The Brown Journal of World Affairs*, Brown Journal of World Affairs, 2010, vol. 16, no. 2, pp. 55-65.

L’HOIRY X., MORETTI A., ANTONOPOULOS G.A., “Identifying sex trafficking in Adult Services Websites: an exploratory study with a British police force,” *Trends in Organized Crime*, May 5, 2021, DOI:10.1007/s12117-021-09414-1.

LIMONCELLI S.A., “The global development of contemporary anti-human trafficking advocacy,” *International Sociology*, SAGE Publications Ltd, November 1, 2017, vol. 32, no. 6, pp. 814-834, DOI:10.1177/0268580917729986.

LIMONCELLI S.A., “What in the World Are Anti-Trafficking NGOs Doing? Findings from a Global Study,” *Journal of Human Trafficking*, Routledge, October 1, 2016, vol. 2, no. 4, pp. 316-328, DOI:10.1080/23322705.2015.1135605.

LLANSÓ E.J., “No amount of 'AI' in content moderation will solve filtering’s prior-restraint problem,” *Big Data & Society*, SAGE Publications Ltd, January 1, 2020, vol. 7, no. 1, pp. 1-6, DOI:10.1177/2053951720920686.

LLORIA GARCÍA P., “El delito de trata de seres humanos y la necesidad de creación de una ley integral,” *Estudios Penales y Criminológicos*, June 22, 2019, vol. 39, p. 353, DOI:10.15304/epc.39.5965.

LLORIA GARCÍA P., “Algunas reflexiones sobre la perspectiva de género y el poder de castigar del Estado,” *Estudios Penales y Criminológicos*, June 15, 2020, vol. 40, DOI:10.15304/epc.40.6503.

LOBASZ J.K., “Beyond Border Security: Feminist Approaches to Human Trafficking,” *Security Studies*, Routledge, June 12, 2009, vol. 18, no. 2, pp. 319-344, DOI:10.1080/09636410902900020.

LÓPEZ-BARAJAS PEREA I., “Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley,” *Revista de Derecho Político*, Universidad Nacional de Educacion a Distancia (UNED), 2017, no. 98, pp. 91-119, 29 pages.

LUSKIN R., “Caring about Corporate 'Due Care': Why Criminal Respondeat Superior Liability Outreaches Its Justification,” *American Criminal Law Review*, 2020, vol. 57, no. 2, pp. 303-330.

LÜTZ F., “Gender equality and artificial intelligence in Europe. Addressing direct and indirect impacts of algorithms on gender-based discrimination,” *ERA Forum*, May 1, 2022, vol. 23, no. 1, pp. 33-52, DOI:10.1007/s12027-022-00709-6.

LUTZ H., SCHWIDDESSEN S., “The New German Hate Speech Law – Introduction and Frequently Asked Questions,” *Computer Law Review International*, Verlag Dr. Otto Schmidt, July 26, 2017, vol. 18, no. 4, pp. 103-111, DOI:10.9785/cri-2017-0403.

MACHAT S. et al., “Sex workers’ experiences and occupational conditions post-implementation of end-demand criminalization in Metro Vancouver, Canada,” *Canadian Journal of Public Health = Revue Canadienne De Sante Publique*, October 2019, vol. 110, no. 5, pp. 575-583, DOI:10.17269/s41997-019-00226-z.

MACHURA S. et al., “Recognizing Modern Slavery,” *Journal of Human Trafficking*, Routledge, July 3, 2019, vol. 5, no. 3, pp. 201-219, DOI:10.1080/23322705.2018.1471863.

MACKENZIE C., “Agency : un mot, un engagement,” *Rives méditerranéennes*, TELEMME (UMR 6570), February 29, 2012, no. 41, pp. 35-37, DOI:10.4000/rives.4139.

MAISTRE DU CHAMBON P., “La régularité des « provocations policières » : l’évolution de la jurisprudence,” *La Semaine Juridique Edition Générale*, LexisNexis, December 27, 1989, no. 51, p. doctr. 3422.

MAJIC S., “Same Same but Different? Gender, sex work, and respectability politics in the MyRedBook and Rentboy closures,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 82-98, DOI:10.14197/atr.201220146.

MALLET-POUJOL N., “Chronique - Droit de l’Internet,” *La semaine juridique Entreprise et affaires*, January 14, 2021, no. 2, p. 26.

MALPASS A. et al., “Overcoming Digital Exclusion during the COVID-19 Pandemic: Impact of Mobile Technology for Survivors of Modern Slavery and Human Trafficking – A Mixed Method Study of Survivors and Support Service Provider Views,” *Journal of Human Trafficking*, Routledge, March 29, 2022, vol. 0, no. 0, pp. 1-20, DOI:10.1080/23322705.2022.2050991.

MARAS M.-H., “Online Classified Advertisement Sites: Pimps and Facilitators of Prostitution and Sex Trafficking?,” *Journal of Internet Law*, November 1, 2017, vol. 21, no. 5, pp. 17-21.

MARECHAL J.-Y., “Le refus de communiquer le code de déverrouillage d’un téléphone portable utilisé pour commettre une infraction peut constituer un délit,” *La Semaine Juridique Edition Générale*, LexisNexis, November 14, 2022, no. 45, p. 1258.

MARIEZ J.-S., “Une nouvelle étape vers un accès transfrontalier aux preuves numériques : l’initiative européenne « e-evidence » ou la recherche d’un équilibre entre efficacité des enquêtes pénales, droit des personnes concernées et sécurité juridique pour les fournisseurs de services internet,” *Revue Lamy Droit de l’immatériel*, March 1, 2018, no. 146.

MARTELL C., “Customer Transparency Can Dampen the Growing Human Trafficking Problem,” *Journal of Business, Entrepreneurship and the Law*, 2021, vol. 14, no. 1, pp. 35-87.

MARTIN L. et al., “Learning each other’s language and building trust: Community-engaged transdisciplinary team building for research on human trafficking operations and disruption,” *International Journal of Qualitative Methods*, April 30, 2022, vol. 21, pp. 1-15, DOI:10.1177/16094069221101966.

MARTÍN-CASALS M., “An approach to some EU initiatives on the regulation of liability for damage caused by AI-Systems,” *Ius et Praxis*, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, August 2022, vol. 28, no. 2, pp. 3-24, DOI:10.4067/S0718-00122022000200003.

MASSANARI A., “#Gamergate and The Fappening: How Reddit’s algorithm, governance, and culture support toxic technocultures,” *New Media & Society*, 2017, vol. 19, no. 3, pp. 329-346, DOI:10.1177/1461444815608807.

MASSE M., “La souveraineté pénale,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 1999, p. 905.

MASSE M., “Des figures asymétriques de l’internationalisation du droit pénal,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2006, p. 755.

MATTAR M.Y., “Interpreting Judicial Interpretations of the Criminal Statutes of the Trafficking Victims Protection Act: Ten Years Later,” *American University Journal of Gender Social Policy and Law*, 2011, vol. 19, no. 4, pp. 1246-1304.

MATTHIAS A., “The responsibility gap: Ascribing responsibility for the actions of learning automata,” *Ethics and Information Technology*, September 1, 2004, vol. 6, no. 3, pp. 175-183, DOI:10.1007/s10676-004-3422-1.

MATULA C., “Any Safe Harbor in a Storm: SESTA-FOSTA and the Future of § 230 of the Communications Decency Act,” *Duke Law & Technology Review*, 2020, vol. 18, pp. 353-368.

MAXWELL W., “La CJUE dessine le noyau dur d’une future régulation des algorithmes,” *Légipresse*, 2020, p. 671.

MAYMIR S.V., “Anchoring the need to revise cross-border access to e-evidence,” *Internet Policy Review*, Alexander Von Humboldt Inst Internet & Soc, 2020, vol. 9, no. 3, DOI:10.14763/2020.3.1495.

MAZABRAUD B., “Foucault, le droit et les dispositifs de pouvoir,” *Cites*, October 11, 2010, vol. n° 42, no. 2, pp. 126-189.

MAZERES J.-A., “Normativité, vérité, gouvernementalité : figures du juridique chez Michel Foucault,” *Revue interdisciplinaire d’études juridiques*, Université Saint-Louis - Bruxelles, 2017, vol. 79, no. 2, pp. 55-75, DOI:10.3917/riej.079.0055.

MCCLINTOCK A., “Sex Workers and Sex Work: Introduction,” *Social Text*, Duke University Press, 1993, no. 37, pp. 1-10.

MCCREADY E., “Corporate Criminal Liability,” *American Criminal Law Review*, 2022, vol. 59, no. 3-Annual Survey of White Collar Crime, pp. 571-608.

MCKEE A., LUMBY C., “Pornhub, child sexual abuse materials and anti-pornography campaigning,” *Porn Studies*, Routledge, October 2, 2022, vol. 9, no. 4, pp. 464-476, DOI:10.1080/23268743.2022.2083662.

MCKNELLY M., “Untangling SESTA/FOSTA: How the Internet’s 'Knowledge' Threatens Anti-Sex Trafficking Law,” *Berkeley Technology Law Journal*, 2019, vol. 34, no. 4, pp. 1238-1266.

MCSWEEN M., “Investing in the Business against Human Trafficking: Embracing the Fourth P - Partnerships,” *Intercultural Human Rights Law Review*, 2011, vol. 6, pp. 283-324.

MENDEL J., SHARAPOV K., “Human Trafficking and Online Networks: Policy, Analysis, and Ignorance: Human Trafficking and Online Networks,” *Antipode*, June 2016, vol. 48, no. 3, pp. 665-684, DOI:10.1111/anti.12213.

MERABET S., “Le Digital Services Act : permanence des acteurs, renouvellement des qualifications,” *La Semaine Juridique Edition Générale*, LexisNexis, October 17, 2022, no. 41, p. 1175.

MERABET S., “Le Digital Services Act : guide d’utilisation de lutte contre les contenus illicites,” *La Semaine Juridique Edition Générale*, October 24, 2022, no. 42, p. 1210.

MERRY S.E., “Legal Pluralism,” *Law & Society Review*, 1988, vol. 22, no. 5, p. 869, DOI:10.2307/3053638.

MESA R., “Le transport de mineurs aux fins de mariages arrangés n’est pas constitutif du délit de traite des êtres humains,” *Actualité juridique Pénal*, Dalloz, 2023, p. 288.

MIA V., “The Failures of SESTA/FOSTA A Sex Worker Manifesto,” *Tsq-Transgender Studies Quarterly*, Duke University Press, May 1, 2020, vol. 7, no. 2, pp. 237-239, DOI:10.1215/23289252-8143393.

MICU B., “Reflection of the Principle of Loyalty in Matters regarding the Adduction of Evidence in the Romanian Criminal Proceedings,” *Lex ET Scientia International Journal*, 2015, vol. 22, no. 1, pp. 166-174.

MILIVOJEVIĆ S., MOORE H., SEGRAVE M., “Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 16-32, DOI:10.14197/atr.201220142.

MILLER WELBORN YOUNG A., “Willful Blindness: Applying a Drug Trafficking Theory of Liability to International Human Trafficking Prosecution,” *Berkeley Journal of International Law*, 2022, vol. 40, no. 1, pp. 143-170.

MINOW M., SPELMAN E.V., “In Context - Symposium on the Renaissance of Pragmatism in American Legal Thought,” *Southern California Law Review*, 1990 1989, vol. 63, no. 6, pp. 1597-1652.

MITCHELL K.J. et al., “Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization,” *Journal of Adolescent Health*, August 2010, vol. 47, no. 2, pp. 183-190, DOI:10.1016/j.jadohealth.2010.01.007.

MITSILEGAS V., “The privatisation of mutual trust in Europe’s area of criminal justice: The case of e-evidence,” *Maastricht Journal of European and Comparative Law*, SAGE Publications Ltd, June 1, 2018, vol. 25, no. 3, pp. 263-265, DOI:10.1177/1023263X18792240.

MÖKANDER J. et al., “Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation,” *Minds & Machines*, June 1, 2022, vol. 32, no. 2, pp. 241-268, DOI:10.1007/s11023-021-09577-4.

MOLINS F., “La protection des citoyens européens dans un monde ultra-connecté,” *Question d’Europe*, Fondation Robert Schuman, April 8, 2019, no. 510.

MONTJOYE Y.-A. De et al., “Unique in the shopping mall: On the reidentifiability of credit card metadata,” *Science*, January 30, 2015, vol. 347, no. 6221, pp. 536-539, DOI:10.1126/science.1256297.

MONTVALON P. De, “Sous condition « d’émancipation active » : le droit d’asile des prostituées nigérianes victimes de traite des êtres humains,” *Droit et société*, August 27, 2018, vol. 99, no. 2, pp. 374-392.

MOON L.E., “A New Role for Social Network Providers: NetzDG and the Communications Decency Act,” *Transnational Law & Contemporary Problems*, 2019, vol. 29, no. 1, pp. 611-633.

MORGAN E., “On FOSTA and the Failures of Punitive Speech Restrictions,” *Northwestern University Law Review*, 2020, vol. 115, no. 2, pp. 502-548.

MOUA L., “La lutte contre la traite dans les entreprises,” *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, pp. 244-253.

MUIR WATT H., “L’Alien Tort Statute devant la Cour Suprême des États-Unis. Territorialité, diplomatie judiciaire, ou économie politique ?,” *Revue critique de droit international privé*, Dalloz, 2013, vol. 2013/3, no. 3, pp. 594-605.

MUIR WATT H., “La portée territoriale du droit au déréférencement : un exercice de proportionnalité dans l’espace,” *Revue critique de droit international privé*, Dalloz, 2020, vol. 2020/2, no. 2, pp. 333-348.

MUSSO P., “Le Web : nouveau territoire et vieux concepts,” *Annales des Mines - Réalités industrielles*, ESKA, November 2010, vol. 2010/4, no. 4, pp. 74-83.

MUSTO J., “The Limits and Possibilities of Data-Driven Anti-trafficking Efforts,” *Georgia State University Law Review*, May 1, 2020, vol. 36, no. 4, p. 1147.

MUSTO J. et al., “Anti-Trafficking in the Time of FOSTA/SESTA: Networked Moral Gentrification and Sexual Humanitarian Creep,” *Social Sciences*, February 8, 2021, vol. 10, no. 2, p. 58, DOI:10.3390/socsci10020058.

MUSTO J., THAKOR M., GERASIMOV B., “Editorial: Between Hope and Hype: Critical evaluations of technology’s role in anti-trafficking,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 1-14, DOI:10.14197/atr.201220141.

MUSTO J.L., “What’s in a name?: Conflations and contradictions in contemporary U.S. discourses of human trafficking,” *Women’s Studies International Forum*, July 1, 2009, vol. 32, no. 4, pp. 281-287, DOI:10.1016/j.wsif.2009.05.016.

MUSTO J.L., BOYD d., “The Trafficking-Technology Nexus,” *Social Politics*, 2014, vol. 21, no. 3, pp. 461-483.

MYERS WEST S., “Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms,” *New Media & Society*, SAGE Publications, November 1, 2018, vol. 20, no. 11, pp. 4366-4383, DOI:10.1177/1461444818773059.

NAGAN W.P., HAMMER C., “The Changing Character of Sovereignty in International Law and International Relations,” *Columbia Journal of Transnational Law*, 2004, vol. 43, p. 141.

NAGLE L.E., “Selling Souls: The Effect of Globalization on Human Trafficking and Forced Servitude,” *Wisconsin International Law Journal*, 2008, vol. 26, no. 1, p. 131.

NDIOR V., “Le Conseil de surveillance de Facebook, « service après-vente » de la liberté d’expression ?,” *Recueil Dalloz*, Dalloz, 2020, no. 26, p. 1474.

NICAUD B., “Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE,” *Dalloz actualité*, Dalloz, September 5, 2022.

NICOLAS-GRECIANO M., STUCKENBERG C.-F., “Chronique de droit pénal constitutionnel allemand,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2022, p. 669.

NICOT M., “Femmes et filles, les premières victimes de la traite dans le monde,” *Diplomatie*, December 2020, no. 106, p. 54.

NOLAN J., “Hardening Soft Law: Are the emerging corporate social disclosure and due diligence laws capable of generating substantive compliance with human rights norms?,” *Revista de Direito Internacional*, October 26, 2018, vol. 15, no. 2, p. 59, DOI:10.5102/rdi.v15i2.5355.

NOLAN J., BOTT G., “Global supply chains and human rights: spotlight on forced labour and modern slavery practices,” *Australian Journal of Human Rights*, January 2, 2018, vol. 24, no. 1, pp. 43-69, DOI:10.1080/1323238X.2018.1441610.

NOVELLI C. et al., “Taking AI risks seriously: a new assessment model for the AI Act,” *AI & SOCIETY*, July 12, 2023, DOI:10.1007/s00146-023-01723-z.

NUOTIO K., “A legitimacy-based approach to EU criminal law: Maybe we are getting there, after all,” *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 1, 2020, vol. 11, no. 1, pp. 20-39, DOI:10.1177/2032284420903386.

O’BRIEN M.A., “Free Speech or Slavery Profiteering: Solutions for Policing Online Sex-Trafficking Advertisement,” *Vanderbilt Journal of Entertainment & Technology Law*, 2017, vol. 20, no. 1, pp. 288-318.

O’CONNELL DAVIDSON J., “Absolving the State: the Trafficking-Slavery Metaphor,” *Global Dialogue*, Summer/Autumn 2012, vol. 12, no. 2, pp. 31-41.

O’CONNELL DAVIDSON J., “New slavery, old binaries: human trafficking and the borders of ‘freedom’,” *Global Networks*, 2010, vol. 10, no. 2, pp. 244-261, DOI:10.1111/j.1471-0374.2010.00284.x.

O’CONNELL DAVIDSON J., “Will the Real Sex Slave Please Stand Up?,” *Feminist Review*, SAGE Publications, August 1, 2006, vol. 83, no. 1, pp. 3-22, DOI:10.1057/palgrave.fr.9400278.

O’CONNOR M., “Choice, agency consent and coercion: Complex issues in the lives of prostituted and trafficked women,” *Women’s Studies International Forum*, May 2017, vol. 62, pp. 8-16, DOI:10.1016/j.wsif.2017.02.005.

OLLARD R., “Un an de droit pénal du numérique (Octobre 2021 – Octobre 2022),” *Droit pénal*, LexisNexis, December 2022, no. 12, p. 12.

OMER C., “Intermediary Liability for Harmful Speech: lessons from abroad,” *Harvard Journal of Law & Technology*, 2014, vol. 28, no. 1, p. 289.

OOSTERHOUT J.H. Van, “The Role of Corporations in Shaping the Global Rules of the Game: In Search of New Foundations,” *Business Ethics Quarterly*, April 2010, vol. 20, no. 2, pp. 252-264, DOI:10.1017/S1052150X00002906.

ORAM S. et al., “Human Trafficking and Health: A Survey of Male and Female Survivors in England,” *American Journal of Public Health*, June 1, 2016, vol. 106, no. 6, pp. 1073-1078, DOI:10.2105/AJPH.2016.303095.

ORMEROD D., ROBERTS A., “The Trouble with Teixeira: Developing a Principled Approach to Entrapment,” *International Journal of Evidence & Proof*, 2002, vol. 6, no. 1, pp. 37-61.

ORTIZ FREULER J., “The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century,” *Global Media and China*, SAGE Publications Ltd, November 12, 2022, pp. 1-18, DOI:10.1177/20594364221139729.

ORTIZ PRADILLO J.C., “Big Data, vigilancias policiales y geolocalización: nuevas dimensiones de los derechos fundamentales en el proceso penal,” *Diario La Ley*, Wolters Kluwer, 2021, no. 9955, p. 1.

OTTISOVA L. et al., “Prevalence and risk of violence and the mental, physical and sexual health problems associated with human trafficking: an updated systematic review,” *Epidemiology and psychiatric sciences*, April 12, 2016, vol. 25, no. 4, pp. 317-341.

OUTSHOORN J., “Debating Prostitution in Parliament: A Feminist Analysis,” *European Journal of Women’s Studies*, SAGE Publications Ltd, November 1, 2001, vol. 8, no. 4, pp. 472-490, DOI:10.1177/135050680100800405.

PALACIO M., “Protection et surveillance augmentées Le nouveau paradigme sécurité et liberté,” *Cahiers de la sécurité et de la justice*, INHESJ, Deuxième trimestre 2019, no. 47, pp. 4-12.

PANSIER F.-J., “Présentation de la loi : de la LSQ à la LSI,” *Gazette du Palais*, Lextenso, March 27, 2003, no. 86, p. 2.

PARIZOT R., “Loi du 3 juin 2016 : aspects obscurs de droit pénal général (Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l’efficacité et les garanties de la procédure pénale),” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2016, p. 376.

PARKER G., PETROPOULOS G., VAN ALSTYNE M., “Platform mergers and antitrust,” *Industrial and Corporate Change*, October 1, 2021, vol. 30, no. 5, pp. 1307-1336, DOI:10.1093/icc/dtab048.

PASQUALE F., “Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power,” *Theoretical Inquiries in Law*, January 1, 2016, vol. 17, pp. 486-513.

PATES R., “Liberal Laws Juxtaposed with Rigid Control: an Analysis of the Logics of Governing Sex Work in Germany,” *Sexuality Research and Social Policy*, September 2012, vol. 9, no. 3, pp. 212-222, DOI:10.1007/s13178-012-0092-3.

PATI R., “Human Trafficking: An Issue of Human and National Security,” *University of Miami National Security and Armed Conflict Law Review*, 2013, vol. 4, p. 28.

PATI R., “States’ Positive Obligations with Respect to Human Trafficking: The European Court of Human Rights Breaks New Ground in Rantsev v. Cyprus and Russia,” *Boston University International Law Review*, 2011, vol. 29, pp. 79-142.

PEGUERA M., “The Platform Neutrality Conundrum and the Digital Services Act,” *International Review of Intellectual Property and Competition Law*, May 1, 2022, vol. 53, no. 5, pp. 681-684, DOI:10.1007/s40319-022-01205-7.

PENNEY J., “Chilling Effects: Online Surveillance and Wikipedia Use,” *Berkeley Technology Law Journal*, 2016, vol. 31, no. 1, p. 117, DOI:10.15779/Z38SS13.

PERALTA GUTIÉRREZ A., PARRA IGLESIAS F.J., “Incorporación de prueba penal obtenida en proceso judicial extranjero: casos EncroChat y Sky ECC,” *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2021, no. 149, p. 3.

PEREL M., ELKIN-KOREN N., “Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement,” *Florida Law Review*, 2017, vol. 69, p. 180.

PERER A.R., “Policing the Virtual Red Light District: A Legislative Solution to the Problems of Internet Prostitution and Sex Trafficking,” *Brooklyn Law Review*, 2012, vol. 77, no. 2, pp. 823-859.

PÉREZ GONZÁLEZ S., “Sobre la culpabilidad empresarial: notas para una coexistencia eficaz de los artículos 31 bis y 129 del Código Penal,” *Estudios Penales y Criminológicos*, April 21, 2020, vol. 40, DOI:10.15304/epc.40.6218.

PÉREZ RIVAS N., “La responsabilidad penal de los grupos de empresa: criterios sobre la atribución de responsabilidad penal a la empresa matriz por los delitos cometidos por sus filiales,” *La Ley Penal*, June 2023, no. 162.

PERRIER J.-B., “Le fair-play de la preuve pénale,” *Actualité juridique Pénal*, Dalloz, 2017, p. 436.

PETIT B., “Formes légales de travail et formes contemporaines d’esclavage,” *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, pp. 220-230.

PETIT-LECLAIR S., “Eurojust et la lutte contre la traite des êtres humains,” *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29, p. 21.

PETRICCA P., “Commercial Content Moderation: An opaque maze for freedom of expression and customers’ opinions,” *Rivista internazionale di Filosofia e Psicologia*, December 30, 2020, vol. 11, no. 3, pp. 307-326, DOI:10.4453/rifp.2020.0021.

PFERSMANN O., “Le droit comparé comme interprétation et comme théorie du droit,” *Revue internationale de droit comparé*, 2001, vol. 53, no. 2, pp. 274-288, DOI:10.3406/ridc.2001.17976.

PIERCE S.C., “Turning a Blind Eye: U.S. Corporate Involvement in Modern Day Slavery,” *Journal of Gender, Race & Justice*, 2011 2010, vol. 14, no. 2, pp. 577-600.

PILIPETS E., PAASONEN S., “Nipples, memes, and algorithmic failure: NSFW critique of Tumblr censorship,” *New Media & Society*, December 15, 2020, DOI:10.1177/1461444820979280.

PIOTROWICZ R.W., SORRENTINO L., “Human Trafficking and the Emergence of the Non-Punishment Principle,” *Human Rights Law Review*, December 2016, vol. 16, no. 4, pp. 669-699, DOI:10.1093/hrlr/ngw028.

PITTI G., “L’affaire de la sextape : on ne dribble pas le principe de loyauté des preuves !,” *Gazette du Palais*, September 19, 2017, no. 31, p. 18.

PLANITZER J., “Trafficking in human beings for the purpose of labour exploitation. Can obligatory reporting by corporations prevent trafficking?,” *Netherlands Quarterly of Human Rights*, 2016, vol. 34, no. 4, pp. 318-339.

PLANITZER J., KATONA N., “Criminal Liability of Corporations for Trafficking in Human Beings for Labour Exploitation,” *Global Policy*, November 2017, vol. 8, no. 4, pp. 505-511, DOI:10.1111/1758-5899.12510.

PODGOR E.S., “Corporate Criminal Liability: Introduction,” *Stetson Law Review*, 2012 2011, vol. 41, no. 1, pp. 1-6.

POELEMANS M., ORBEGOZO ORONOZ I., “Forces et limites de la coopération franco-espagnole,” *Cahiers de la sécurité et de la justice*, INHESJ, October 2014, no. 29.

POMARES CINTAS E., “La prostitución, rehén permanente del discurso de la trata de personas,” *RELIES: Revista del Laboratorio Iberoamericano para el Estudio Sociohistórico de las Sexualidades*, Universidad Pablo de Olavide, December 7, 2020, no. 4, pp. 173-192, DOI:10.46661/relies.5109.

POMART C., “Enfin une définition pour la notion de résidence habituelle,” *Revue Lamy Droit civil*, September 1, 2006, no. 30.

POST D.G., “Governing Cyberspace,” *Wayne Law Review*, 1996, vol. 43, no. 1, p. 155.

POST D.G., “Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace,” *Journal of Online Law*, 1995, pp. 1-11.

POST D.G., JOHNSON D.R., “Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems,” *Chicago-Kent Law Review*, 1998, vol. 73, no. 4, pp. 1054-1099.

PREVOST J.-B., “La fabrique des données : à propos du codage numérique du droit et de ses limites,” *Gazette du Palais*, January 22, 2019, no. 03, p. 81.

PRONIER J., “La clarification des règles encadrant le recours à un dispositif de captation des images et des paroles,” *Actualité juridique Pénal*, Dalloz, 2013, p. 227.

QUEMENER M., “Les dispositions liées au numérique de la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme,” *Dalloz IP/IT*, 2016, p. 431.

QUEMENER M., “Les spécificités juridiques de la preuve numérique,” *Actualité juridique Pénal*, Dalloz, 2014, p. 63.

QUEMENER M., “Les techniques spéciales d’enquête en matière de lutte contre la cybercriminalité,” *Actualité juridique Pénal*, Dalloz, 2015, p. 403.

RAETS S., JANSSENS J., “Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business,” *European Journal on Criminal Policy and Research*, October 26, 2019, DOI:10.1007/s10610-019-09429-z.

RAETS S., JANSSENS J., “Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business,” *European Journal on Criminal Policy & Research*, Springer Nature, June 2021, vol. 27, no. 2, pp. 215-238, DOI:10.1007/s10610-019-09429-z.

RAGARU N., “Du bon usage de la traite des êtres humains. Controverses autour d’un problème social et d’une qualification juridique,” *Genèses*, Belin, 2007, vol. 2007/1, no. 66, pp. 69-89.

RAHMAN M.A., “Human Trafficking in the era of Globalization: The case of Trafficking in the Global Market Economy,” *Journal of Global Studies Transcience*, 2011, vol. 2, no. 1, pp. 54-71.

RAPHAEL J., “Denial of Harm: Sex Trafficking, Backpage, and Free Speech Absolutism,” *Dignity: A Journal on Sexual Exploitation and Violence*, 2017, vol. 2, no. 1.

RAS I., GREGORIOU C., “The Quest to End Modern Slavery: Metaphors in corporate modern slavery statements,” *Anti-Trafficking Review*, September 26, 2019, no. 13, pp. 100-118, DOI:10.14197/atr.201219137.

RAYÓN BALLESTEROS M.C., “Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015,” *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario “Escorial-María Cristina,” 2019, no. 52, pp. 179-203.

RAYÓN BALLESTEROS M.C., “Cuestiones clave de las once primeras sentencias del Tribunal Supremo sobre la responsabilidad penal de la persona jurídica,” *Revista Aranzadi de Derecho y Proceso Penal*, June 2018, vol. 50.

RAYÓN BALLESTEROS M.C., HERNÁNDEZ J.A., “Cibercrimen: particularidades en su investigación y enjuiciamiento/Cybercrime: particularities in investigation and prosecution,” *Anuario Jurídico y Económico Escurialense*, Real Colegio Universitario “Escorial-María Cristina,” 2014, no. 47, pp. 209-233, 25 pages.

REIDENBERG J.R., “Lex Informatica: The Formulation of Information Policy Rules Through Technology,” *Texas Law Review*, 1998, vol. 76, no. 3, pp. 552-593.

RENDE TAYLOR L., SHIH E., “Worker feedback technologies and combatting modern slavery in global supply chains: examining the effectiveness of remediation-oriented and due-diligence-oriented technologies in identifying and addressing forced labour and human trafficking,” *Journal of the British Academy*, 2019, vol. 7, no. 1, pp. 131-165, DOI:10.5871/jba/007s1.131.

ROBERT J.-H., “Application de l’article 121-2 du Code pénal au cas où l’organe de la société prévenue est lui-même une société,” *La semaine du droit pénal et procédure pénale*, LexisNexis, September 12, 2022, no. 36, pp. 1623-1626.

ROBERTS H. et al., “Safeguarding European values with digital sovereignty: an analysis of statements and policies,” *Internet Policy Review*, Alexander Von Humboldt Inst Internet & Soc, 2021, vol. 10, no. 3, DOI:10.14763/2021.3.1575.

ROCHEFORT A., “Regulating Social Media Platforms: A Comparative Policy Analysis,” *Communication Law and Policy*, Routledge, April 2, 2020, vol. 25, no. 2, pp. 224-260, DOI:10.1080/10811680.2020.1735194.

RODOTA S., “Nouvelles technologies et droits de l’homme : faits, interprétations, perspectives,” *Mouvements*, La Découverte, June 8, 2010, vol. 62, no. 2, pp. 54-70.

RODRÍGUEZ RUIZ B., “Hacia un Estado post-patriarcal. Feminismo y ciudadanía,” *Revista de estudios políticos*, Centro de Estudios Políticos y Constitucionales (España), 2010, no. 149, pp. 87-122.

RODRÍGUEZ-LÓPEZ S., “Criminal Liability of Legal Persons for Human Trafficking Offences in International and European Law,” *Journal of Trafficking and Human Exploitation*, February 14, 2017, vol. 1, no. 1, pp. 95-114, DOI:10.7590/24522775114.

RODRÍGUEZ-LÓPEZ S., “(De)Constructing Stereotypes: Media Representations, Social Perceptions, and Legal Responses to Human Trafficking,” *Journal of Human Trafficking*, Routledge, January 2, 2018, vol. 4, no. 1, pp. 61-72, DOI:10.1080/23322705.2018.1423447.

ROJSZCZAK M., “e-Evidence Cooperation in Criminal Matters from an EU Perspective,” *Modern Law Review*, Wiley, July 2022, vol. 85, no. 4, pp. 997-1028, DOI:10.1111/1468-2230.12749.

ROSO CAÑADILLAS R., “Prevención: responsabilidad social y penal de las personas jurídicas,” *Revista General de Derecho Penal*, Iustel, 2020, no. 33, p. 14.

RUBERG B., “'Obscene, pornographic, or otherwise objectionable': Biased definitions of sexual content in video game live streaming,” *New Media & Society*, SAGE Publications, June 1, 2021, vol. 23, no. 6, pp. 1681-1699, DOI:10.1177/1461444820920759.

RUBIO MORENO F., “Caso EncroChat y la prueba resultante de las intervenciones masivas de comunicaciones encriptadas en procesos penales extranjeros,” *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2021, no. 153, p. 9.

RUIZ FABRI H., “Immatériel, territorialité et État,” *Archives de Philosophie du Droit*, Éditions Dalloz, 1999, vol. 43, pp. 187-212.

RUIZ HERRERA A.L., RUIZ GUEVARA S.M., LÓPEZ CANTERO E.J., “El papel de los medios de comunicación masiva en la comprensión del fenómeno de la trata de personas,” *Revista Criminalidad*, August 30, 2018, vol. 60, no. 2, pp. 25-39, DOI:10.47741/17943108.16.

RUSSO R., “Online Sex Trafficking Hysteria: Flawed Policies, Ignored Human Rights, and Censorship,” *Cleveland State Law Review*, March 13, 2020, vol. 68, no. 2, p. 314.

SACHOULIDOU A., “Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence,” *Artificial Intelligence and Law*, February 22, 2023, DOI:10.1007/s10506-023-09347-w.

SACHS T., CLERC C., “Controverse : le devoir de vigilance à la croisée des chemins ?,” *Revue de droit du travail*, Dalloz, 2022, p. 352.

SACHS T., TRICOT J., “La loi sur le devoir de vigilance : un modèle pour (re)penser la responsabilité des entreprises,” *Droit et société*, Lextenso, 2020, vol. 106, no. 3, pp. 682-698.

SAGITTAE G., “On the lawfulness of the EncroChat and Sky ECC-operations,” *New Journal of European Criminal Law*, SAGE Publications Ltd STM, March 14, 2023, p. 20322844231159576, DOI:10.1177/20322844231159576.

SAINT-PAU J.-C., “Les investigations numériques et le droit au respect de la vie privée,” *Actualité juridique Pénal*, Dalloz, 2017, p. 321.

SAINT-PAU J.-C., “Responsabilité pénale d’une personne morale absorbante en cas de fraude à la loi,” *La Semaine Juridique Edition Générale*, LexisNexis, July 18, 2022, no. 28, pp. 1416-1419.

SAIZ-ECHEZARRETA V., ALVARADO M.-C., GÓMEZ-LORENZINI P., “Advocacy of trafficking campaigns: A controversy story,” *Comunicar: Revista Científica de Comunicación y Educación*, April 1, 2018, vol. 26, no. 55, pp. 29-38, DOI:10.3916/C55-2018-03.

SAIZ-ECHEZARRETA V., ALVARADO M.-C., GÓMEZ-LORENZINI P., “Incidencia política de las campañas contra la trata: Un relato controvertido,” *Comunicar*, Grupo Comunicar, 2018, vol. 26, no. 55, pp. 29-38, 29-38 pages, DOI:http://dx.doi.org/10.3916/C55-2018-03.

SALAS D., “« Et la nuit noire de l’esclavage tomba sur moi… » Réflexions conclusives,” *Les Cahiers de la Justice*, Dalloz, 2020, vol. 2020/2, no. 2, pp. 288-295.

SALVADORI I., “Agentes artificiales, opacidad tecnológica y distribución de la responsabilidad penal,” *Cuadernos de política criminal*, Dykinson, 2021, no. 133, pp. 137-174.

SANCHEZ A., “FOSTA: A Necessary Step in Advancement of the Women’s Rights Movement,” *Touro Law Review*, 2020, vol. 36, no. 2, pp. 636-662.

SANCHÍS CRESPO C., “Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas,” *La ley penal: revista de derecho penal, procesal y penitenciario*, Wolters Kluwer, 2017, no. 125, p. 1.

SANDERS T. et al., “The Point of Counting: Mapping the Internet Based Sex Industry,” *Social Sciences*, Science Publishing Group, October 22, 2018, vol. 7, no. 5, p. 233, DOI:10.11648/j.ss.20180705.15.

ŞANDRU S., “About Data Protection and Data Retention in Romania,” *Masaryk University Journal of Law and Technology*, November 29, 2013, vol. 7, no. 2, pp. 379-399.

SARFATY G.A., “Can Big Data Revolutionize International Human Rights Law,” *University of Pennsylvania Journal of International Law*, 2017, vol. 39, no. 1, pp. 72-102.

SARKAR S., “Use of technology in human trafficking networks and sexual exploitation: A cross-sectional multi-country study,” *Transnational Social Review*, January 2, 2015, vol. 5, no. 1, pp. 54-68, DOI:10.1080/21931674.2014.991184.

SARKAR S., “Trans-border sex trafficking: identifying cases and victims in the UK,” *Migration and Development*, January 2, 2014, vol. 3, no. 1, pp. 95-107, DOI:10.1080/21632324.2013.869958.

SCHAUER F., “Fear, Risk and the First Amendment: Unraveling the Chilling Effect,” *Boston University Law Review*, January 1, 1978, vol. 58, pp. 684-732.

SCHERER A.G., PALAZZO G., “The New Political Role of Business in a Globalized World: A Review of a New Perspective on CSR and its Implications for the Firm, Governance, and Democracy: Political Role of Business in a Globalized World,” *Journal of Management Studies*, June 2011, vol. 48, no. 4, pp. 899-931, DOI:10.1111/j.1467-6486.2010.00950.x.

SCHLOENHARDT A., HUNT-WALSHE R., “The Role of Non-Governmental Organisations in Australia’s Anti-Trafficking in Persons Framework,” *University of Western Australia Law Review*, 2013 2012, vol. 36, no. 1, pp. 56-91.

SCHLOENHARDT A., MARKEY-TOWLER R., “Non-Criminalisation of Victims of Trafficking in Persons — Principles, Promises, and Perspectives,” *Groningen Journal of International Law*, July 15, 2016, vol. 4, no. 1, p. 10, DOI:10.21827/59db68fc35c13.

SCHWEMER S.F., MAHLER T., STYRI H., “Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?,” *Oslo Law Review*, Universitetsforlaget, 2021, vol. 8, no. 01, pp. 4-29, DOI:10.18261/ISSN.2387-3299-2021-01-01.

SCOULAR J. et al., “Beyond the Gaze and Well Beyond Wolfenden: The Practices and Rationalities of Regulating and Policing Sex Work in the Digital Age,” *Journal of Law and Society*, June 2019, vol. 46, no. 2, pp. 211-239, DOI:10.1111/jols.12155.

SEDDIKI N., “Repenser la responsabilité en affaires dans un monde globalisé,” *Paix et Securité Internationales*, 2020, no. 8, pp. 184-210.

SENECHAL J., “Vote des parlementaires européens sur l’AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s’inspirant du DSA, du Data Act et du RGPD ?,” *Dalloz actualité*, Dalloz, June 22, 2023.

SERRE C., EVRARD C., “Du rififi chez les grandes oreilles,” *Dalloz Actualité*, Dalloz, February 4, 2020.

SHAFFER G., POLLACK M., “Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance,” *Boston College Law Review*, September 1, 2011, vol. 52, no. 4, p. 1147.

SHARAPOV K., MENDEL J., “Trafficking in Human Beings: Made and Cut to Measure? Anti-trafficking Docufictions and the Production of Anti-trafficking Truths,” *Cultural Sociology*, SAGE Publications, December 1, 2018, vol. 12, no. 4, pp. 540-560, DOI:10.1177/1749975518788657.

SHARKEY T.C. et al., “Better together: A transdisciplinary approach to disrupt human trafficking,” *ISE Magazine*, 34-39, November 2021.

SHELLEY L., BAIN C., “Human Trafficking: Fighting the Illicit Economy with the Legitimate Economy,” *Social Inclusion*, February 23, 2015, vol. 3, no. 1, pp. 140-144, DOI:10.17645/si.v3i1.215.

SIERRA-RODRÍGUEZ A., ARROYO-MACHADO W., BARROSO-HURTADO D., “La trata de personas en Twitter: Finalidades, actores y temas en la escena hispanohablante,” *Comunicar: Revista Científica de Comunicación y Educación*, 2022, vol. 30, no. 71, pp. 79-91, DOI:10.3916/C71-2022-06.

SILLER N., “‘Modern slavery’: does international law distinguish between slavery, enslavement and trafficking?,” *Journal of international criminal justice*, Oxford University Press, May 1, 2016, vol. 14, no. 2, pp. 405-427, DOI:10.1093/jicj/mqv075.

SIRINELLI J., “La protection des données de connexion par la Cour de justice : cartographie d’une jurisprudence européenne inédite,” *Revue trimestrielle de droit européen*, 2021, p. 313.

SIRY L., “Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens,” *New Journal of European Criminal Law*, SAGE Publications Ltd STM, September 1, 2019, vol. 10, no. 3, pp. 227-250, DOI:10.1177/2032284419865608.

SKELDON R., “Trafficking: A Perspective from Asia,” *International Migration*, September 2000, vol. 38, no. 3, pp. 7-30, DOI:10.1111/1468-2435.00113.

SMITH M.V., “Applying the United Nations Trafficking Protocol in the Context of Climate Change. Comments,” *Chicago Journal of International Law*, 2021, vol. 22, no. 1, pp. 298-334.

SMYRNAIOS N., MARTY E., “Profession « nettoyeur du net »,” *Reseaux*, La Découverte, October 10, 2017, vol. n° 205, no. 5, pp. 56-90.

SNAJDR E., “Beneath the master narrative: human trafficking, myths of sexual slavery and ethnographic realities,” *Dialectical Anthropology*, June 1, 2013, vol. 37, no. 2, pp. 229-256, DOI:10.1007/s10624-013-9292-3.

SNYDER-HALL R.C., “Third-Wave Feminism and the Defense of 'Choice,'” *Perspectives on Politics*, March 2010, vol. 8, no. 1, pp. 255-261, DOI:10.1017/S1537592709992842.

SODERLUND G., “Running from the Rescuers: New U.S. Crusades Against Sex Trafficking and the Rhetoric of Abolition,” *NWSA Journal*, October 2005, vol. 17, no. 3, pp. 64-87, DOI:10.2979/NWS.2005.17.3.64.

SOLARI-MERLO M.N., “Análisis de los delitos informáticos. Una propuesta de clasificación,” *Revista Aranzadi de Derecho y Proceso Penal*, December 2020, vol. 60.

SOREL J.-M., “Le rôle de la soft law dans la gouvernance mondiale : vers une emprise hégémonique ?,” *Revue Européenne du Droit*, Groupe d’études géopolitiques, 2021, vol. 2, no. 1, pp. 46-50.

SOUTHERTON C. et al., “Restricted modes: Social media, content classification and LGBTQ sexual citizenship,” *New Media & Society*, SAGE Publications, May 1, 2021, vol. 23, no. 5, pp. 920-938, DOI:10.1177/1461444820904362.

SOUVIRA J.-M., “La traite des êtres humains et l’exploitation sexuelle,” *Cahiers de la sécurité et de la justice*, INHESJ, September 2009, no. 9, pp. 107-117.

SRIKANTIAH J., “Perfect victims and real survivors: the iconic victim in domestic human trafficking law,” *Boston University Law Review*, 2007, vol. 87, no. 1, pp. 157-211.

STASI M.L., “La exposición a la diversidad de contenidos en las redes sociales: Entre la regulación o la desagregación en la curación de contenidos,” *Teoría y derecho: revista de pensamiento jurídico*, Tirant lo Blanch, 2022, no. 32, pp. 130-165.

STASIAK F., “Groupe de sociétés - Groupe de sociétés et responsabilité pénale : de l’esquive à l’esquisse,” *Droit des sociétés*, LexisNexis, June 2017, no. 6, p. 16.

STEGEMAN H.M., “Regulating and representing camming: Strict limits on acceptable content on webcam sex platforms,” *New Media & Society*, SAGE Publications, November 27, 2021, p. 14614448211059116, DOI:10.1177/14614448211059117.

STEURER R., “The role of governments in corporate social responsibility: characterising public policies on CSR in Europe,” *Policy Sciences*, March 2010, vol. 43, no. 1, pp. 49-72, DOI:10.1007/s11077-009-9084-4.

STONE G.R., “Sex and the First Amendment: The Long and Winding History of Obscenity Law,” *First Amendment Law Review*, 2019, vol. 17, p. 140.

SUCH E. et al., “The Risks and Harms Associated with Modern Slavery during the COVID-19 Pandemic in the United Kingdom: A Multi-Method Study,” *Journal of Human Trafficking*, Routledge, April 8, 2023, vol. 0, no. 0, pp. 1-21, DOI:10.1080/23322705.2023.2194760.

SUZOR N., “Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms,” *Social Media + Society*, SAGE Publications Ltd, July 1, 2018, vol. 4, no. 3, pp. 1-11, DOI:10.1177/2056305118787812.

SWORDS J., LAING M., COOK I.R., “Platforms, sex work and their interconnectedness,” *Sexualities*, SAGE Publications Ltd, September 28, 2021, vol. 0, no. 0, p. 1, DOI:10.1177/13634607211023013.

TAYLOR M., HOLLAND G., QUAYLE E., “Typology of Paedophile Picture Collections,” *The Police Journal*, April 2001, vol. 74, no. 2, pp. 97-107, DOI:10.1177/0032258X0107400202.

TEUBNER G., “L’auto-constitutionnalisation des ETN ? Sur les rapports entre les codes de conduite « privés » et « publics » des entreprises,” *Revue interdisciplinaire d’études juridiques*, Université Saint-Louis - Bruxelles, 2015, vol. 75, no. 2015/2, pp. 0-25.

TEYSSEDRE J., “Le droit de l’Union européenne de la protection des données dans le prétoire du Conseil d’État : quels enjeux ?,” *Revue trimestrielle de droit européen*, 2021, p. 331.

THIAGO D.O., MARCELO A.D., GOMES A., “Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online,” *Sexuality & Culture*, Springer Nature B.V., 2021, vol. 25, no. 2, pp. 700-732, 700-732 pages, DOI:https://doi.org/10.1007/s12119-020-09790-w.

THIEULIN B., “Gouverner à l’heure de la révolution des pouvoirs,” *Pouvoirs*, January 11, 2018, vol. N° 164, no. 1, pp. 19-30.

THOMAS W.R., “How and Why Corporations Became (and Remain) Persons under the Criminal Law,” *Florida State University Law Review*, 2018 2017, vol. 45, no. 2, pp. 479-538.

TICHENOR E., “'I’ve Never Been So Exploited': The consequences of FOSTA-SESTA in Aotearoa New Zealand,” *Anti-Trafficking Review*, April 27, 2020, no. 14, pp. 99-115, DOI:10.14197/atr.201220147.

TIDBALL S., ZHENG M., CRESWELL J.W., “Buying Sex On-Line from Girls: NGO Representatives, Law Enforcement Officials, and Public Officials Speak out About Human Trafficking—A Qualitative Analysis,” *Gender Issues*, March 2016, vol. 33, no. 1, pp. 53-68, DOI:10.1007/s12147-015-9146-1.

TINOCO PASTRANA A., “Las órdenes europeas de entrega y conservación: La futura obtención transnacional de la prueba electrónica en los procesos penales en la Unión Europea,” *Cuadernos de política criminal*, Dykinson, 2021, no. 135, pp. 203-246.

TODRES J., “The Private Sector’s Pivotal Role in Combating Human Trafficking,” *California Law Review Circuit*, 2012, vol. 3, pp. 79-99.

TORRES ROSELL N., VILLACAMPA ESTIARTE C., “Protección jurídica y asistencia para víctimas de trata de seres humanos,” *Revista General de Derecho Penal*, Iustel, 2017, no. 27, p. 16.

TOSZA S., “All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order,” *New Journal of European Criminal Law*, SAGE Publications Ltd STM, June 1, 2020, vol. 11, no. 2, pp. 161-183, DOI:10.1177/2032284420919802.

TOUILLIER M., “Les droits de la défense dans les procédures d’exception : une évolution « vent dessus, vent dedans »,” *Actualité juridique Pénal*, Dalloz, 2016, p. 119.

TRIPP H., “All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims,” *Penn State Law Review*, 2019, vol. 124, no. 1, pp. 219-246.

TROPER M., “Le monopole de la contrainte légitime,” *Lignes*, Éditions Hazan, 1995, vol. n° 25, no. 2, pp. 34-47.

TURILLAZZI A. et al., “The digital services act: an analysis of its ethical, legal, and social implications,” *Law, Innovation and Technology*, Routledge, March 10, 2023, vol. 0, no. 0, pp. 1-24, DOI:10.1080/17579961.2023.2184136.

TURING A., “Computing machine and intelligence,” *Mind*, October 1, 1950, vol. LIX, no. 236, pp. 433-460, DOI:10.1093/mind/LIX.236.433.

TÜRK P., “Définition et enjeux de la souveraineté numérique,” *Cahiers français*, La documentation française, June 2020, no. 415, p. 18.

TURNER-MOSS E. et al., “Labour Exploitation and Health: A Case Series of Men and Women Seeking Post-Trafficking Services,” *Journal of Immigrant and Minority Health*, June 1, 2014, vol. 16, no. 3, pp. 473-480, DOI:10.1007/s10903-013-9832-6.

TUTTLE E., “Reexamining the Vicarious Criminal Liability of Corporations for the Willful Crimes of Their Employees,” *Cleveland State Law Review*, 2022 2021, vol. 70, no. 1, p. [i]-143.

TZVETKOVA M., “NGO responses to trafficking in women,” *Gender & Development*, Routledge, March 1, 2002, vol. 10, no. 1, pp. 59-68, DOI:10.1080/13552070215893.

VADILLO F., “Techniques d’enquête numérique judiciaire : les défis d’une survie dans la modernité,” *Enjeux numériques*, Annales des mines, September 2018, no. 3.

VAN BUREN H.J., SCHREMPF-STIRLING J., WESTERMANN-BEHAYLO M., “Business and Human Trafficking: A Social Connection and Political Responsibility Model,” *Business & Society*, February 2021, vol. 60, no. 2, pp. 341-375, DOI:10.1177/0007650319872509.

VAN DE KERCHOVE M., “Eclatement et recomposition du droit pénal,” *Revue de science criminelle et de droit pénal comparé*, Dalloz, 2000, p. 5.

VAN DER LEUN J., VAN SCHIJNDEL A., “Emerging from the shadows or pushed into the dark? The relation between the combat against trafficking in human beings and migration control,” *International Journal of Law, Crime and Justice*, March 2016, vol. 44, pp. 26-42, DOI:10.1016/j.ijlcj.2015.04.001.

VAN LOO R., “The Corporation as Courthouse,” *Yale Journal on Regulation*, January 1, 2016, vol. 33, p. 547.

VARGAS GALLEGO A.I., “Algunos apuntes sobre la interceptación de las comunicaciones telefónicas,” *Revista de Jurisprudencia El Derecho*, December 16, 2020, no. 8.

VARJU M., “The Protection of Technology Sovereignty in the EU: Policy, Powers and the Legal Reality,” *European law review*, Sweet & Maxwell, 2022, no. 4, pp. 568-583.

VELASCO NUÑEZ E., “Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías,” *Revista de Jurisprudencia*, February 1, 2011, no. 4, p. 1.

VELASCO NÚÑEZ E., “Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica,” *Diario La Ley*, November 4, 2013, no. 8183.

VERGES E., “La notion de criminalité organisée après la loi du 9 mai 2004,” *Actualité juridique Pénal*, Dalloz, 2004, p. 181.

VERGES E., “Loyauté et licéité, deux apports majeurs à la théorie de la preuve pénale,” *Recueil Dalloz*, 2014, p. 407.

VERGNE J.-P., DURAND R., “Cyberespace et organisations « virtuelles » : l’Etat souverain a-t-il encore un avenir ?,” *Regards croisés sur l’économie*, La Découverte, 2014, vol. 2014/1, no. 14, pp. 126-139.

VERHULST S.G., “Operationalizing digital self-determination,” *Data & Policy*, Cambridge University Press, January 2023, vol. 5, pp. 1-14, DOI:10.1017/dap.2023.11.

VERVAELE J., “Mesures de procédure spéciales et respect des droits de l’homme Rapport général,” *Utrecht Law Review*, October 2009, vol. 5, no. 2, pp. 110-152.

VIAUT L., “Droit et algorithmes : réflexion sur les nouveaux processus décisionnels,” *Petites affiches*, September 4, 2020, no. 177-178, p. 8.

VILJOEN S., “The Promise and Limits of Lawfulness: Inequality, Law, and the Techlash,” *Journal of Social Computing*, September 2021, vol. 2, no. 3, pp. 284-296, DOI:10.23919/JSC.2021.0025.

VILLACAMPA ESTIARTE C., “Acerca del Anteproyecto de Ley Orgánica Integral contra la Trata y la Explotación de Seres Humanos,” *Diario La Ley*, Wolters Kluwer, 2023, no. 10267, p. 1.

VILLACAMPA ESTIARTE C., “A vueltas con la prostitución callejera: ¿Hemos abandonado definitivamente el prohibicionismo suave?,” *Estudios penales y criminológicos*, Servicio de Publicaciones, 2015, no. 35, pp. 413-455.

VILLACAMPA ESTIARTE C., “Dificultades en la persecución penal de la trata de seres humanos para explotación laboral,” *Indret: Revista para el Análisis del Derecho*, Universitat Pompeu Fabra, 2022, no. 2, p. 6.

VILLACAMPA ESTIARTE C., “¿Es necesaria una ley integral contra la trata de seres humanos?,” *Revista General de Derecho Penal*, Iustel, 2020, no. 33, p. 16.

VILLACAMPA ESTIARTE C., “La moderna esclavitud y su relevancia jurídico-penal,” *Revista de Derecho Penal y Criminología*, Facultad de Derecho, 2013, no. 10, pp. 293-342.

VILLACAMPA ESTIARTE C., “Políticas De Criminalización De La Prostitución: Análisis Crítico De Su Fundamentación Y Resultados,” *Revista de Derecho Penal y Criminología*, Universidad Nacional de Educación a Distancia (UNED), 2012, no. 7, pp. 81-142, 62 pages.

VILLANUEVA FERNÁNDEZ A., FERNÁNDEZ-LLEBREZ GONZÁLEZ F., “La importancia de los datos de trata de seres humanos: una aproximación al sistema de recolección de datos de víctimas de trata en España,” *Revista Deusto de derechos humanos*, Instituto de Derechos Humanos Pedro Arrupe, 2019, no. 4, pp. 115-143.

VINCENT N.A., JANE E.A., “Beyond law Protecting victims through engineering and design,” *in* MARTELLOZZO E., JANE E.A. (eds.), *Cybercrime and its Victims*, Routledge, 1st ed., June 26, 2017, pp. 209-223, DOI:10.4324/9781315637198.

VIOLEAU O., “Les techniques d’investigations numériques : entre insécurité juridique et limites pratiques,” *Actualité juridique Pénal*, Dalloz, 2017, p. 324.

VIVANT M., “La responsabilité des intermédiaires de l’internet,” *La Semaine Juridique Edition Générale*, 1999, no. 45.

VLAMYNCK H., “Le point sur la captation de l’image et des paroles dans l’enquête de police,” *Actualité juridique Pénal*, Dalloz, 2011, p. 574.

VLAMYNCK H., “La loyauté de la preuve au stade de l’enquête policière,” *Actualité juridique Pénal*, Dalloz, 2014, p. 325.

VOLODKO A., COCKBAIN E., KLEINBERG B., “'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers,” *Trends in Organized Crime*, 2020, no. 23, pp. 7-35.

VUJANOVIC A.A. et al., “Applying Telemental Health Services for Adults Experiencing Trafficking,” *Public Health Rep*, SAGE Publications Inc, July 1, 2022, vol. 137, no. 1_suppl, pp. 17S-22S, DOI:10.1177/00333549221085243.

WACHTER S., MITTELSTADT B., FLORIDI L., “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,” *International Data Privacy Law*, May 2017, vol. 7, no. 2, pp. 76-99, DOI:10.1093/idpl/ipx005.

WALKOWITZ J.R., “The Politics of Prostitution,” *Signs*, University of Chicago Press, 1980, vol. 6, no. 1, pp. 123-135.

WARREN S.D., BRANDEIS L.D., “The Right to Privacy,” *Harvard Law Review*, The Harvard Law Review Association, 1890, vol. 4, no. 5, pp. 193-220, DOI:10.2307/1321160.

WATSON H., DONOVAN A., “Role of technology in human trafficking,” *TRACE*, October 2015.

WEITZER R., “Flawed Theory and Method in Studies of Prostitution,” *Violence Against Women*, July 2005, vol. 11, no. 7, pp. 933-949, DOI:10.1177/1077801205276986.

WEITZER R., “Sex Trafficking and the Sex Industry: The Need for Evidence-Based Theory and Legislation,” *Journal of Criminal Law and Criminology*, 2013, vol. 101, no. 4, p. 1336.

WHEATON E.M., SCHAUER E.J., GALLI T.V., “Economics of Human Trafficking,” *International Migration*, July 19, 2010, vol. 48, no. 4, pp. 114-141, DOI:10.1111/j.1468-2435.2009.00592.x.

WHITE A., GUIKEMA S., CARR B., “Why are You Here? Modeling Illicit Massage Business Location Characteristics with Machine Learning,” *Journal of Human Trafficking*, Routledge, October 4, 2021, vol. 0, no. 0, pp. 1-21, DOI:10.1080/23322705.2021.1982238.

WIESNER L., “Good Intentions and Unintended Consequences: SESTA/FOSTA’s First Two Years,” *Temple Law Review*, 2021 2020, vol. 93, p. 151.

WOLFE N., “Coyote Publishing, Inc. v. Miller: Blurring the Standards of Commercial and Noncommercial Speech,” *Golden Gate University Law Review*, January 3, 2012, vol. 42, no. 1.

YOUNG I.M., “Responsibility and Global Justice: A Social Connection Model,” *Social Philosophy and Policy*, Cambridge University Press, January 2006, vol. 23, no. 1, pp. 102-130, DOI:10.1017/S0265052506060043.

YOUNG I.M., “Mothers, Citizenship, and Independence: A Critique of Pure Family Values,” *Ethics*, University of Chicago Press, 1995, vol. 105, no. 3, pp. 535-556.

ZENG H.S., DANAHER B., SMITH M.D., “Internet Governance Through Site Shutdowns: The Impact of Shutting Down Two Major Commercial Sex Advertising Sites,” *Management Science*, August 16, 2022, p. 4498, DOI:10.1287/mnsc.2022.4498.

ZHANG S.X., “Measuring labor trafficking: a research note,” *Crime, Law and Social Change*, November 1, 2012, vol. 58, no. 4, pp. 469-482, DOI:10.1007/s10611-012-9393-y.

ZHANG T. et al., “A qualitative assessment of hotel employee engagement in anti-human-trafficking initiatives,” *International Journal of Hospitality Management*, April 1, 2022, vol. 102, p. 103148, DOI:10.1016/j.ijhm.2022.103148.

ZHIDKOVA T., “Globalization and the Emergence of Violent Non-state Actors: The Case of Human Trafficking,” *New Global Studies*, De Gruyter, April 1, 2015, vol. 9, no. 1, pp. 1-25, DOI:10.1515/ngs-2014-0014.

ZINITI C., “Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It,” *Berkeley Technology Law Journal*, 2008, vol. 23, no. 1, pp. 582-616.

ZUIDERVEEN BORGESIUS F.J., “Strengthening legal protection against discrimination by algorithms and artificial intelligence,” *The International Journal of Human Rights*, Routledge, November 25, 2020, vol. 24, no. 10, pp. 1572-1593, DOI:10.1080/13642987.2020.1743976.

ZURTH P., “The German NetzDG as Role Model or Cautionary Tale? – Implications for the Debate on Social Media Liability,” *Fordham Intellectual Property, Media & Entertainment Law Journal*, 2021, vol. 31, no. 4, p. 1084, DOI:10.2139/ssrn.3668804.

I. SSRN articles

CHRISTAKIS T., *Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)*, SSRN Scholarly Paper, ID 3086820, CEIS & The Chertoff Group White Paper, Lawful Access to Data: The US v. Microsoft Case, Sovereignty in the Cyber-Space and European Data Protection, November 29, 2017.

CHRISTAKIS T., *“European Digital Sovereignty”: Successfully Navigating Between the “Brussels Effect” and Europe’s Quest for Strategic Autonomy*, SSRN Scholarly Paper, ID 3748098, Social Science Research Network, December 7, 2020, DOI:10.2139/ssrn.3748098.

GOLDMAN E., *The United States’ Approach to “Platform” Regulation*, SSRN Scholarly Paper, ID 4404374, Defeating Disinformation UnConference, 2023.

GRIFFIN R., *New School Speech Regulation and Online Hate Speech: A Case Study of Germany’s NetzDG*, SSRN Scholarly Paper, ID 3920386, Social Science Research Network, September 9, 2021, DOI:10.2139/ssrn.3920386.

LODDER A.R., MORAIS CARVALHO J., *Online Platforms: Towards An Information Tsunami with New Requirements on Moderation, Ranking, and Traceability*, SSRN Scholarly Paper, Social Science Research Network, ID 4050115, March 4, 2022, DOI:10.2139/ssrn.4050115.

SCHULZ W., *Regulating Intermediaries to Protect Privacy Online – The Case of the German NetzDG*, SSRN Scholarly Paper, ID 3216572, Social Science Research Network, July 19, 2018.

TOSZA S., *Mutual Recognition by Private Actors in Criminal Justice? Service Providers As Gatekeepers of Data and Human Rights Obligations*, SSRN Scholarly Paper, ID 3517878, Rochester, NY, Social Science Research Network, September 19, 2019, DOI:10.2139/ssrn.3517878.

WALDMAN A.E., *Disorderly Content*, SSRN Scholarly Paper, ID 3906001, Rochester, NY, Social Science Research Network, August 16, 2021, DOI:10.2139/ssrn.3906001.

II. ArXiv articles

BARAKAT H.L., REDMILES E.M., "Community Under Surveillance: Impacts of Marginalization on an Online Labor Forum," SocArXiv, September 24, 2021, DOI:10.31235/osf.io/74zw2.

KEJRIWAL M. et al., "FlagIt: A System for Minimally Supervised Human Trafficking Indicator Mining," *ArXiv:1712.03086 [cs]*, December 5, 2017, online http://arxiv.org/abs/1712.03086 (retrieved on April 10, 2021), DOI:arXiv:1712.03086 [cs].

KONRAD R. et al., *Perspectives on How To Conduct Responsible Anti-Human Trafficking Research in Operations and Analytics*, arXiv:2006.16445, ArXiv, December 21, 2022, online http://arxiv.org/abs/2006.16445 (retrieved on February 10, 2023).

WANG L. et al., "Sex Trafficking Detection with Ordinal Regression Neural Networks," *ArXiv:1908.05434 [cs, stat]*, January 11, 2020, online http://arxiv.org/abs/1908.05434 (retrieved on May 20, 2021).

III. JurisClasseur (France)

CASTETS-RENARD C., "Fascicule 1245 : Régulation des plateformes en ligne," *JurisClasseur Europe Traité*, December 1, 2021.

MARECHAL J.-Y., "Art. 121-2 - Fasc. 20 : Responsabilité pénale des personnes morales," *JurisClasseur Pénal Code*, LexisNexis, May 27, 2022.

MEINDL T., "Fascicule 20 : Procédure applicable à la criminalité et la délinquance organisées – Poursuite. Instruction. Jugement. Assistants spécialisés – Dispositions dérogatoires de procédure – Articles 706-73 à 706-106," *JurisClasseur Procédure pénale*, LexisNexis, January 31, 2020.

QUEMENER M., "Fascicule 20 : La preuve numérique dans un cadre pénal - Articles 427 à 457," *JurisClasseur Procédure pénale*, LexisNexis, April 18, 2019.

QUEMENER M., "Fascicule 1110 : Infiltrations numériques," *JurisClasseur Communication*, LexisNexis, July 3, 2019.

QUEMENER M., "Fascicule 982 : Géolocalisation dans le cadre pénal - Articles 689 à 693," *JurisClasseur Communication*, LexisNexis, July 3, 2019.

RALSER E., "Fascicule unique : Domicile et résidence dans les rapports internationaux - Articles 102 à 111," *JurisClasseur Civil Code*, LexisNexis, December 27, 2017.

STELLA E., "Synthèse - Activités internet," *JurisClasseur Communication*, LexisNexis, September 24, 2020.

VIDAL J., "Fascicule 82-20 : Droit pénal. – Responsabilités," *JurisClasseur Travail Traité*, LexisNexis, July 16, 2021.

§3. Thesis and dissertations

BAL L., *Le mythe de la souveraineté en droit international : la souveraineté des Etats à l'épreuve des mutations de l'ordre juridique international*, Thesis, Université de Strasbourg, February 3, 2012.

BARRAUD B., *Le renouvellement des sources du droit - Illustrations en droit de la communication par internet*, Thesis, Université d'Aix Marseille, July 1, 2016.

BOOS R., *La lutte contre la cybercriminalité au regard de l'action des États*, Thesis, Université de Lorraine, 2016.

HERRAN T., *Essai d'une théorie générale de l'entraide policière internationale*, Thesis, Université de Pau et des Pays de l'Adour, 2012.

HULTGREN M., *An exploratory study of the indicators of trafficking in online female escort ads*, Thesis, San Diego State University, 2015.

KENNEDY E., *Predictive Patterns of Sex Trafficking Online*, Thesis, Carnegie Mellon University, 2012.

LANNIER S., *Le blanchiment d'argent dans le cadre de la traite d'êtres humains en sa forme d'exploitation sexuelle : une approche comparative*, Master Dissertation, Université de Bordeaux and Vietnam National University, 2019.

LAVORGNA A., *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*, Thesis, University of Trento, December 2013.

LESER J., *Feeling Blue: Affective Rationalities in Vice Squad Policing*, Thesis, Universität Leipzig, 2019.

MORIN M.-E., *Le système pénal de l'Union européenne*, Thesis, Université d'Aix-Marseille, November 28, 2017.

MORNET A., *Les fichiers pénaux de l'Union européenne : Contribution à l'étude de la protection des données à caractère personnel*, Thesis, Université Toulouse 1, December 4, 2020.

MORTIER P., *Les métamorphoses de la souveraineté*, Thesis, Université d'Angers, January 1, 2011.

NETTER E., *Numérique et grandes notions du droit privé*, Thesis, Université de Picardie - Jules Verne, November 20, 2017.

PARK J., *The public-private partnerships' impact on transparency and effectiveness in the EU internet content regulation : the case of "Network Enforcement Act (NetzDG)" in Germany*, Thesis, Universitätsverlag Potsdam, 2020.

ROUSSEL B., *Les investigations numériques en procédure pénale*, Thesis, Université de Bordeaux, July 7, 2020.

SCHLANGEN E.A., *The Application of Coercive Control Theory to Youth Sex Trafficking*, Master thesis, Northern Arizona University, 2022.

SEILER B., *Analyse de la traite d'êtres humains sur Internet : le cas de la prostitution en Suisse romande*, Mémoire de maîtrise, Université de Lausanne, July 2017.

SIMON P., *La compétence d'incrimination de l'Union européenne*, Thesis, Université Paris Est, Université du Luxembourg, Droit de l'Union européenne Thèses, 2019.

SIMONSON E., *Semi-Supervised Classification of Social Media Posts: Identifying Sex-Industry Posts to Enable Better Support for Those Experiencing Sex-Trafficking*, Master thesis, Massachusetts Institute of Technology, April 7, 2021, DOI:10.48550/arXiv.2104.03233.

TADROUS S., *La place de la victime dans le procès pénal*, Thesis, Université Montpellier I, December 1, 2014.

VAN RIJ J.J.M., *The trafficking and sexual exploitation of native Hungarian speaking women in the Netherlands. A case study into the nature of forced prostitution and the modus operandi of organised crime groups involved in human trafficking in Europe*, Thesis, Inholland University of Applied Sciences, June 2014.

VIUHKO M., *Restricted agency, control and exploitation - Understanding the agency of trafficked persons in the 21sst century Finland*, Thesis, University of Helsinki, 2019.

§4. Research reports

BANK M. et al., *The lobby network: big tech's web of influence in the EU*, Corporate Europe Observatory, LobbyControl e.V., August 2021.

BLUNT D., WOLF A., LAUREN N., *Erased The Impact of FOSTA-SESTA*, Hacking//Hustling, 2020.

BLUNT D. et al., *Posting into the Void: studying the impact of shadowbanning on sex workers and activists*, Hacking//Hustling, 2020.

BOGUCKI A. et al., *The AI Act and emerging EU digital acquis. Overlaps, gaps and inconsistencies*, CEPS In-Depth Analysis, Centre for European Policy Studies, September 14, 2022.

BOIZARD M. et al., *Le droit à l'oubli [Rapport de recherche]*, report, no. 11-25, Mission de recherche Droit et Justice, February 2015.

BOYD d. et al., *Human Trafficking and Technology: A framework for understanding the role of technology in the commercial sexual exploitation of children in the US*, Microsoft Research Connections, December 2011.

CALLANAN C. et al., *Rapport Filtrage d'Internet Equilibrer les réponses à la cybercriminalité dans une société démocratique*, Open Society Institute, October 2009.

CARRERA S., STEFAN M., *Access to Electronic Data for Criminal Investigations Purposes in the EU*, CEPS Paper in Liberty and Security in Europe, no. 2020-01, Centre for European Policy Studies, February 2020.

CARTWRIGHT B. et al., *Deploying artificial intelligence to detect and respond to the use of digital technology by perpetrators of human trafficking*, International CyberCrime Research Centre - Simon Fraser University, April 2022.

CASTAÑO REYERO M.J. et al., *Cultura de datos en la trata de seres humanos: informe técnico de investigación*, Universidad Pontificia Comillas, 1st edition, February 17, 2022, DOI:10.14422/iuem.20220218.

COCKAYNE J., *Innovation for inclusion: using digital technology to increase financial agency and prevent modern slavery*, Secretariat Briefing Paper 3, Financial Sector Commission Secretariat, UN University, Liechtenstein Initiative for a Financial Sector Commission on Modern Slavery and Human Trafficking, 2019.

CORNILS M., *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries*, Algorithm Watch, May 26, 2020.

CROM J.-P.L., *Histoire du droit du travail dans les colonies françaises (1848-1960)*, Rapport de recherche, halshs-01592836, Mission de recherche Droit et Justice, January 11, 2017.

DANK M. et al., *Estimating the Size and Structure of the Underground Commercial Sex Economy in Eight Major US Cities*, Research Report, The Urban Institute, March 2014.

DE VRIES K. et al., *The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?)*, CEPS Liberty and Security in Europe, Centre for European Policy Studies, May 2010.

DI NICOLA A., BARATTO G., MARTINI E., *Surf and sound - The role of the internet in people smuggling and human trafficking*, Faculty of Law, University of Trento, ECrime Research Reports, March 2017.

CHAWKI M., WAHAB M., *Technology Is a Double-Edged Sword: Illegal Human Trafficking in the Information Age*, DROIT-TIC.fr, 2004.

ENGLER A., RENDA A., *Reconciling the AI Value Chain with the EU's Artificial Intelligence Act*, CEPS In-Depth Analysis, Centre for European Policy Studies, September 30, 2022.

FARMS G., *25 Keys to Unlock the Financial Chains of Human Trafficking & Modern Slavery*, UN University, Workshop Breaking the Financial Chains: Disrupting Financial Flows associated with Slavery, Human Trafficking, Forced Labour and Child Labour, March 31, 2017.

GOLDMAN E., *Balancing Section 230 and Anti-Sex Trafficking Initiatives - Hearing on "Latest Developments in Combating Online Sex Trafficking" - Written Remarks*, Legal Studies Research Papers Series, no. 2017-17, Santa Clara University School of Law, November 30, 2017.

GUBEREK T., SILVA R., *"Human Rights and Technology": Mapping the Landscape to Support Grantmaking*, PRIMA, Ford Foundation, August 2014.

GUILLOU S., *La souveraineté numérique française passera par l'investissement dans les technologies numériques*, Sciences Po Paris, Chaire Digital, Gouvernance, et Souveraineté, 2020.

KENNEDY M., *Counter-Trafficking Top 40 Tech Against Child Trafficking*, Center for Mind and Culture, May 2019.

LAKE Q. et al., *Corporate leadership on modern slavery: How have companies responded to the Modern Slavery Act one year on?*, Hult International Business School & Ethical Trading Initiative, 2016.

LATONERO M., *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Center on Communication Leadership & Policy, University of Southern California, November 2012.

LATONERO M. et al., *Human Trafficking Online The Role of Social Networking Sites and Online Classifieds*, Center on Communication Leadership & Policy, University of Southern California, September 2011.

LATONERO M., WEX B., AHYAUDIN S., *Technology and Labor Trafficking Project Framing Document*, USC Annenberg - Center on communication leadership & policy, June 2014.

LATONERO M. et al., *Technology and Labor Trafficking in a Network Society - General Overview, Emerging Innovations, and Philippines Case Study*, USC Annenberg - USC University of Southern California, February 2015.

LAVAUD-LEGENDRE B., *Approche globale et traite des êtres humains - De l'« injonction à la coopération » au travail ensemble*, CNRS, July 1, 2018, online https://halshs.archives-ouvertes.fr/halshs-02177213 (retrieved on October 29, 2021).

LAVAUD-LEGENDRE B., "La traite des êtres humains comme objet de politique publique," May 2014, online https://hal.archives-ouvertes.fr/hal-01188870 (retrieved on October 29, 2021).

LAVAUD-LEGENDRE B., *Guide d'identification et d'orientation des victimes de traite des êtres humains*, COMPTRASEC, June 2016.

LAVAUD-LEGENDRE B., PLESSARD C., ENCRENAZ G., *Prostitution de mineures – Quelles réalités sociales et juridiques ?*, Rapport de recherche, Université de Bordeaux, CNRS - COMPTRASEC UMR 5114, October 30, 2020.

LEBARON G. et al., *Confronting root causes: forced labour in global supply chains*, Open Democracy, Beyond Trafficking and Slavery Series, 2018.

MALTZAHN K., *Digital dangers Information & communication technologies and trafficking in women*, APC-200608-WNSP-I-EN-P-0024, Association for progressive communications, Issue Papers, August 2006.

MENECEUR Y., *Analyse des principaux cadres supranationaux de régulation de l'intelligence artificielle : de l'éthique à la conformité*, Projet d'étude, May 27, 2021, online https://lestempselectriques.net/index.php/2021/05/27/analyse-des-principaux-cadres-supranationaux-de-regulation-de-lintelligence-artificielle-de-lethique-a-la-conformite/ (retrieved on May 28, 2021).

MITCHELL K., BOYD d., *Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement*, Crimes against Children Research Center, University of New Hampshire, November 2014.

ROE-SEPOWITZ D. et al., *Online Advertisement Truth Set Sex Trafficking Matrix: A tool to Detect Minors in Online Advertisements*, Research Brief, Arizona State University School of Social Work, Office of sex trafficking intervention Research, November 2018.

SHENTOV O., RUSEV A., ANTONOPOULOS G.A., *Financing of Organised Crime: Human Trafficking in Focus*, Sofia, Center for the Study of Democracy, EU, 2018.

STEFAN M., GONZÁLEZ FUSTER G., *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters - State of the art and latest developments in the EU and the US*, CEPS Paper in Liberty and Security in Europe, no. 2018-07, Centre for European Policy Studies, November 30, 2018.

TAYLOR R., MARIA L., LATONERO M., *Updated Guide to Ethics and Human Rights in Anti-Trafficking: Ethical Standards for Working with Migrant Workers and Trafficked Persons in the Digital Age*, Issara Institute - Bangkok, 2018.

TRUONG T.-D., *Human trafficking and organised crime*, Institute of Social Studies, Working paper series no. 339, 2001.

VAN DIJK J. et al., *Counting what counts: tools for the validation and utilization of EU statistics on human trafficking*, HOME/2011/ISEC/AG/THB/4000001960, INTERVICT/Universitat Autònoma de Barcelona, TrafStat project, January 1, 2014.

VÄYRYNEN R., *Illegal Immigration, Human Trafficking, and Organized Crime*, no. DP2003-72, World Institute for Development Economic Research, WIDER Working Paper Series, 2003.

VEALE M., *Algorithms in the Criminal Justice System*, The Law Society Commission on the Use of Algorithms in the justice System, The Law Society of England and Wales, July 2019.

WOOLLEY S., GURSKY J., *Countering disinformation and protecting democratic communication on encrypted messaging applications*, Brookings institution, June 11, 2021.

ZIMMERMAN C. et al., *Stolen smiles: a summary report on the physical and psychological health consequences of women and adolescents trafficked in Europe*, London School of Hygiene & Tropical Medicine, 2006.

ZIMMERMAN C. et al., *The Health Risks and Consequences of Trafficking in Women and Adolescents Findings from a European Study*, London School of Hygiene & Tropical Medicine, 2003.

§5. Lectures

DELMAS-MARTY M., *Une boussole des possibles: Gouvernance mondiale et humanismes juridiques - Leçon de clôture prononcée le 11 mai 2011*, Collège de France, 2020.

FOUCAULT M. et al., *Sécurité, territoire, population: cours au Collège de France, 1977-1978*, Seuil : Gallimard, Hautes études, 2004.

POLITIS N.-S., "Le problème des limitations de la souveraineté et la théorie de l'abus des droits dans les rapports internationaux (Volume 6)," *Collected Courses of the Hague Academy of International Law*, Brill, January 1, 1925.

SASSEN S., *Losing control: sovereignty in an age of globalization*, Columbia University Press, University Seminars: Leonard Hastings Schoff Memorial Lectures, 1996.

SUPIOT A., *La gouvernance par les nombres: cours au Collège de France (2012-2014)*, Fayard, 2020.

WEBER M., *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004, tran. LIVINGSTONE R..

WEBER M., *Le savant et le politique (1919)*, Union Générale d'Éditions, Le Monde en 10-18, 1963.

I. Conference lectures and presentations

ANCEL M., "Le droit pénal comparé en tant que moyen de recherche dans le domaine de la politique criminelle," *in* MAX-PLANCK-INSTITUT FÜR AUSLÄNDISCHES UND INTERNATIONALES STRAFRECHT INTERNATIONALES KOLLOQUIUM FREIBURG IM BREISGAU) (ed.), *Comparison as a method of criminal law and criminology*, Duncker & Humblot, Strafrecht und Kriminologie ; Bd 6, 1980, p. 73.

BARWULOR C. et al., "'Disadvantaged in the American-dominated Internet': Sex, Work, and Technology," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Yokohama Japan, ACM, May 6, 2021, pp. 1-16, DOI:10.1145/3411764.3445378.

BENSOUSSAN A., LEPAGE A., QUEMENER M., "Loyauté de la preuve et nouvelles technologies : entre exigences processuelles et efficacité répressive," *in* GUINCHARD S. et al. (eds.), *Les transformations de la justice pénale: cycle de conférences 2013 à la Cour de cassation*, 2014.

BOYD d., MARWICK A., "Social Steganography: Privacy in Networked Publics," *International Communication Association*, Boston, MA, May 28, 2011.

CHARPENTIER J., "Le phénomène étatique à travers les grandes mutations politiques contemporaines," *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 11.

CHEN C., DELL N., ROESNER F., "Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors," *Proceedings of the 28th USENIX Security Symposium*, Santa Clara, CA, USA, August 16, 2016, p. 89.

GERRY Q.C. F., SHAW P., "Emerging and Future Technology Trends in the Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants," *First International Conference on Transdisciplinary AI*, Laguna Hills, CA, USA, IEEE, September 2019, pp. 1-9, DOI:10.1109/TransAI46475.2019.00009.

GOULD A.J., "From Pseudoscience to Protoscience: Estimating Human Trafficking and Modern Forms of Slavery," *Second Annual Interdisciplinary Conference on Human Trafficking*, University of Nebraska, 2010.

HULTGREN M. et al., "Using Knowledge Management to Assist in Identifying Human Sex Trafficking," *49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA, IEEE, January 2016, pp. 4344-4353, online http://ieeexplore.ieee.org/document/7427725/ (retrieved on December 26, 2020), DOI:10.1109/HICSS.2016.539.

IBANEZ M., SUTHERS D., "Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources," *47th Hawaii International Conference on System Sciences*, Waikoloa, HI, IEEE, January 2014, pp. 1556-1565, online http://ieeexplore.ieee.org/document/6758797/ (retrieved on October 9, 2020), DOI:10.1109/HICSS.2014.200.

IBANEZ M., SUTHERS D., "Detecting Covert Sex Trafficking Networks in Virtual Markets," *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining: ASONAM 2016 : San Francisco, CA, USA, August 18-21, 2016*, Institute of Electrical and Electronics Engineers, 2016, online http://ieeexplore.ieee.org/servlet/opac?punumber=7736513 (retrieved on October 9, 2020).

JEAN J.-P., "La mémoire du crime dans les deux lois de déclaration relative au génocide des Arméniens et à l'esclavage," *in* INSTITUT DE SCIENCES CRIMINELLES DE POITIERS, DANTI-JUAN M. (eds.), *La mémoire et le crime: dix-huitièmes Journées d'étude de l'Institut de sciences*

criminelles de Poitiers, vendredi 18 et samedi 19 juin 2010, Éditions Cujas, Travaux de l'institut de sciences criminelles de Poitiers no. 27, 2011, p. 175.

KAPOOR R., KEJRIWAL M., SZEKELY P., "Using contexts and constraints for improved geotagging of human trafficking webpages," *Proceedings of the Fourth International ACM Workshop on Managing and Mining Enriched Geo-Spatial Data - GeoRich '17*, Chicago, Illinois, ACM Press, 2017, pp. 1-6, online http://dl.acm.org/citation.cfm?doid=3080546.3080547 (retrieved on January 16, 2021), DOI:10.1145/3080546.3080547.

KEJRIWAL M., SZEKELY P., "Information Extraction in Illicit Web Domains," *Proceedings of the 26th International Conference on World Wide Web*, Perth Australia, International World Wide Web Conferences Steering Committee, April 3, 2017, pp. 997-1006, online https://dl.acm.org/doi/10.1145/3038912.3052642 (retrieved on January 16, 2021), DOI:10.1145/3038912.3052642.

KEJRIWAL M., SZEKELY P., "An Investigative Search Engine for the Human Trafficking Domain," *in* D'AMATO C. et al. (eds.), *The Semantic Web – ISWC 2017: 16th International Semantic Web Conference, Vienna, Austria, October 21-25, 2017, Proceedings, Part II*, Springer International Publishing, Lecture Notes in Computer Science, 2017, vol. 10588, p. 247, DOI:10.1007/978-3-319-68204-4.

KEJRIWAL M., SZEKELY P., "Knowledge Graphs for Social Good: An Entity-centric Search Engine for the Human Trafficking Domain," *IEEE Transactions on Big Data*, 2019, vol. 14, no. 8, pp. 1-15, DOI:10.1109/TBDATA.2017.2763164.

KEJRIWAL M., SZEKELY P., KNOBLOCK C., "Investigative Knowledge Discovery for Combating Illicit Activities," *IEEE Intelligent Systems*, January 2018, vol. 33, no. 1, pp. 53-63, DOI:10.1109/MIS.2018.111144556.

LALONDE L., "L'interdisciplinarité comme « contextes », quels usages de l'Autre ?," *in* JOURNEE D'ETUDE SUR LA METHODOLOGIE ET L'EPISTEMOLOGIE JURIDIQUES, AZZARIA G. (eds.), *Les cadres théoriques et le droit: actes de la 2e Journée d'étude sur la méthodologie et l'épistémologie juridiques*, Éditions Yvon Blais, 2013, p. 375.

LI L. et al., "Detection and Characterization of Human Trafficking Networks Using Unsupervised Scalable Text Template Matching," *IEEE International Conference on Big Data*, December 2018, pp. 3111-3120, https://ieeexplore.ieee.org/document/8622189, DOI:10.1109/BigData.2018.8622189.

MATTMANN C.A. et al., "Multimedia Metadata-based Forensics in Human Trafficking Web Data," *WSDM'16 workshop proceedings*, San Francisco, USA, Interfacultary Research Institutes, Institute for Logic, Language and Computation (ILLC)IEEE, February 22, 2016.

MAX-PLANCK-INSTITUT FÜR AUSLÄNDISCHES UND INTERNATIONALES STRAFRECHT INTERNATIONALES KOLLOQUIUM FREIBURG IM BREISGAU), *Die Vergleichung als Methode der Strafrechtswissenschaft und der Kriminologie = La comparaison en tant que méthode scientifique en droit pénal et en criminologie = Comparison as a method of criminal law and criminology*, Duncker & Humblot, Strafrecht und Kriminologie ; Bd 6, 1980.

MCALISTER R., "Webscraping as an Investigation Tool to Identify Potential Human Trafficking Operations in Romania," *Proceedings of the ACM Web Science Conference on ZZZ - WebSci '15*, Oxford, United Kingdom, ACM Press, 2015, pp. 1-2, online http://dl.acm.org/citation.cfm?doid=2786451.2786510 (retrieved on November 28, 2020), DOI:10.1145/2786451.2786510.

MOUTON J.-D., "L'état selon le droit international - diversité et unité," *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 79.

QUENEUDEC J.-P., "Conclusions," *in* SOCIETE FRANÇAISE POUR LE DROIT INTERNATIONAL (ed.), *L'Etat souverain à l'aube du XXIe siècle: colloque de Nancy*, A. Pedone, 1994, p. 307.

RABBANY R., BAYANI D., DUBRAWSKI A., “Active Search of Connections for Case Building and Combating Human Trafficking,” *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, London United Kingdom, ACM, July 19, 2018, pp. 2120-2129, online https://dl.acm.org/doi/10.1145/3219819.3220103 (retrieved on May 1, 2021), DOI:10.1145/3219819.3220103.

RENSHAW C., “The Globalisation Paradox and the Implementation of International Human Rights: the Function of Transnational Networks in Combating Human Trafficking in the ASEAN Region,” *Law and Society Association Australia and New Zealand (LSAANZ) Conference 2008 ‘W(h)ither Human Rights’*, University of Sydney, December 10, 2008, online https://ses.library.usyd.edu.au/handle/2123/4045 (retrieved on June 8, 2021).

ROKSANDIĆ S., PROTRKA N., ENGELHART M., “Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?,” *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022, pp. 1225-1232, DOI:10.23919/MIPRO55190.2022.9803606.

SILVA D.R. et al., “Data integration from open internet sources and network detection to combat underage sex trafficking,” *Proceedings of the 15th Annual International Conference on Digital Government Research - dg.o ’14*, Aguascalientes, Mexico, ACM Press, 2014, pp. 86-90, online http://dl.acm.org/citation.cfm?doid=2612733.2612746 (retrieved on January 16, 2021), DOI:10.1145/2612733.2612746.

STANOJOSKA A., PETREVSKI B., “Theory of push and pull factors: a new way of explaining the old,” *Conference: Archibald Reiss Days*, Belgrade, Serbia, March 1, 2012.

STYLIANOU A. et al., “TraffickCam: Crowdsourced and Computer Vision Based Approaches to Fighting Sex Trafficking,” *2017 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, Washington, DC, USA, IEEE, October 2017, pp. 1-8, online https://ieeexplore.ieee.org/document/8457947/ (retrieved on December 26, 2020), DOI:10.1109/AIPR.2017.8457947.

STYLIANOU A. et al., “Hotels-50K: A Global Hotel Recognition Dataset,” *Proceedings of the AAAI Conference on Artificial Intelligence*, July 2019, vol. 33, pp. 726-733, https://ojs.aaai.org/index.php/AAAI/article/view/3863, DOI:10.1609/aaai.v33i01.3301726.

SZEKELY P. et al., “Building and Using a Knowledge Graph to Combat Human Trafficking,” *in* ARENAS M. et al. (eds.), *The Semantic Web - ISWC 2015: 14th International Semantic Web Conference, Bethlehem, PA, USA, October 11-15, 2015, Proceedings, Part II*, Springer International Publishing, Lecture Notes in Computer Science, 2015, vol. 9367, pp. 205-211, DOI:10.1007/978-3-319-25010-6.

TONG E. et al., “Combating Human Trafficking with Multimodal Deep Models,” *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, Vancouver, Canada, Association for Computational Linguistics, July 2017, pp. 1547-1556, online https://aclanthology.org/P17-1142 (retrieved on February 10, 2023), DOI:10.18653/v1/P17-1142.

WANG H. et al., “Data integration from open internet sources to combat sex trafficking of minors,” *Proceedings of the 13th Annual International Conference on Digital Government Research - dg.o ’12*, College Park, Maryland, ACM Press, 2012, p. 245, online http://dl.acm.org/citation.cfm?doid=2307729.2307769 (retrieved on December 29, 2020), DOI:10.1145/2307729.2307769.

WEINBERG N. et al., “AI against Modern Slavery: Digital Insights into Modern Slavery Reporting -Challenges and Opportunities,” *Proceedings of the AAAI Fall Symposium on AI for Social Good Virtual Symposium*, November 13, 2020.

WESTLAKE B., BOUCHARD M., FRANK R., “Comparing Methods for Detecting Child Exploitation Content Online,” *2012 European Intelligence and Security Informatics Conference*, Odense, Denmark, IEEE, August 2012, pp. 156-163, online

http://ieeexplore.ieee.org/document/6298826/ (retrieved on February 9, 2021), DOI:10.1109/EISIC.2012.25.

§6. Main legislation

I. National legislation

A. France

Code civil.

Code de commerce.

Code de procédure pénale.

Code pénal.

Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

B. Spain

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Ley 35/1995, de 11 de diciembre, de ayudas y asistencia a las víctimas de delitos violentos y contra la libertad sexual.

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género.

Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por Ley Orgánica 2/2009.

4Ley 4/2015, de 27 de abril, del Estatuto de la víctima del delito.

1. In negotiation

MINISTERIO DE JUSTICIA et al., Anteproyecto de Ley Orgánica integral contra la trata y la explotación de seres humanos, 2022.

C. Romania

Codul de Procedură Penală (Legea nr. 135/2010).

Codul Penal (Legea nr. 286/2009).

Legea nr. 302 privind cooperarea judiciară internațională în materie penală, June 26, 2004.

Legea nr. 51/1995 pentru organizarea și exercitarea profesiei de avocat, June 7, 1995.

Lege nr. 678/2001 privind prevenirea și combaterea traficului de persoane, November 21, 2001.

Lege nr. 682/2002 privind protecția martorilor, December 19, 2002.

Lege nr. 211/2004 privind unele măsuri pentru asigurarea informării, sprijinirii și protecției victimelor infracțiunilor, May 27, 2004.

Lege nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, November 17, 2004.

Lege nr. 298/2008 privind reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum și pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, November 18, 2008.

Lege nr. 82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, June 13, 2012.

Lege nr. 235/2015 pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, October 12, 2015.

Lege nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, December 28, 2018.

Ordonanţa de urgenţă nr. 194/2002 privind regimul străinilor în România, December 12, 2002.

Ordonanță de Urgență nr. 78/2016 pentru organizarea și funcționarea Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, precum și pentru modificarea și completarea unor acte normative, November 16, 2016.

D. United States

Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, October 3, 2019.

Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), 2017.

Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018.

Victims of Trafficking and Violence Protection Act, 2000.

US Code.

California Transparency in Supply Chains Act, 2010.

E. Others

BELGIUM, Code d'instruction criminelle.

BELGIUM, Code pénal.

BELGIUM, Loi portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, December 25, 2016.

BELGIUM, Loi modifiant le Code pénal en ce qui concerne le droit pénal sexuel, March 30, 2022.

GERMANY, NetzDG - Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken - Network Enforcement Act, June 3, 2021.

HOUSE OF COMMONS, Police, Crime, Sentencing and Courts Bill (Amendment Paper), United Kingdom, June 16, 2021.

UNITED KINGDOM, Modern Slavery Act 2015.

II. Supranational legislation

A. United Nations

Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, 2000.

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, 2000.

United Nations Convention against Transnational Organized Crime, 2000.

B. Council of Europe

European Convention on Human Rights, 1950.

European Convention on Mutual Assistance in Criminal Matters, 1959.

Convention on Action against Trafficking in Human Beings, 2005.

Convention 108+ for the protection of individuals with regard to the processing of personal data, 2018.

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 2021.

C. European Union

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, 2000.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

Directive 2002/58/CE of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Council Directive 2004/81/EC of 29 April 2004 on the residence permit issued to third-country nationals who are victims of trafficking in human beings or who have been the subject of an action to facilitate illegal immigration, who cooperate with the competent authorities.

Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

Treaty on the Functioning of the European Union, 2012.

Charter of Fundamental Rights of the European Union, 2012.

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings

1. In negotiation

COUNCIL OF THE EU, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - General approach, December 6, 2022, 2021/0106(COD).

EUROPEAN COMMISSION, Proposal for a Directive of the European Parliament and of the Council amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, December 19, 2022, COM(2022) 732 final.

EUROPEAN COMMISSION, Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), January 10, 2017, COM(2017) 10 final.

EUROPEAN COMMISSION, Draft Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, December 13, 2022.

EUROPEAN COMMISSION, Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, April 21, 2021, COM/2021/206 final.

EUROPEAN COMMISSION, Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, 2022.

EUROPEAN COMMISSION, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), September 28, 2022, COM(2022) 496 final.

EUROPEAN COMMISSION, Proposal for a Regulation of the European Parliament and of the Council on prohibiting products made with forced labour on the Union market, September 14, 2022, COM(2022) 453 final.

EUROPEAN PARLIAMENT, Amendments on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, June 14, 2023, P9_TA(2023)0236.

EUROPEAN PARLIAMENT, Amendments on the proposal for a directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937, June 1, 2023, P9_TA(2023)0209.

§7. Case law

I. National case law

A. France

1. Conseil Constitutionnel

Conseil constitutionnel, *Loi relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, March 23, 2017, 2017-750 DC.

Conseil constitutionnel, *M. Malek B. [Pénalisation du refus de remettre aux autorités judiciaires la convention secrète de déchiffrement d'un moyen de cryptologie]*, March 30, 2018, 2018-696 QPC.

Conseil constitutionnel, *Loi de programmation 2018-2022 et de réforme pour la justice*, March 21, 2019, 2019-778 DC.

Conseil constitutionnel, *M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]*, December 3, 2021, 2021-952 QPC.

Conseil constitutionnel, *M. Saïd Z.*, April 8, 2022, 2022-987 QPC.

2. Cour de Cassation

Cour de Cassation, Assemblée plénière, December 9, 2019, no. 18-86767.

Cour de Cassation, Assemblée plénière, November 7, 2022, 21-83.146.

Cour de Cassation, Chambre civile 1, February 23, 1965, no. 62-13427.

Cour de Cassation, Chambre civile 1, February 11, 1997, no. 95-11674.

Cour de Cassation, Chambre civile 1, December 9, 2003, no. 01-03225.

Cour de Cassation, Chambre civile 1, December 14, 2005, 05-10.951.

Cour de Cassation, Chambre civile 1, January 22, 2014, no. 10-15890.

Cour de Cassation, Chambre civile 1, January 22, 2014, no. 11-24019.

Cour de Cassation, Chambre civile 1, January 22, 2014, no. 11-26822.

Cour de Cassation, Chambre civile 1, October 18, 2017, no. 16-10428.

Cour de Cassation, Chambre civile 1, June 15, 2022, 18-24.850.

Cour de Cassation, Chambre commerciale, January 11, 2005, no. 02-18381.

Cour de Cassation, Chambre commerciale, March 20, 2007, no. 04-19679.

Cour de Cassation, Chambre commerciale, March 9, 2010, no. 08-16752.

Cour de Cassation, Chambre commerciale, July 13, 2010, no. 06-20230.

Cour de Cassation, Chambre commerciale, March 29, 2011, no. 10-12272.

Cour de Cassation, Chambre commerciale, September 20, 2011, no. 10-16569.

Cour de Cassation, Chambre commerciale, March 20, 2012, no. 11-10600.

Cour de Cassation, Chambre commerciale, May 3, 2012, no. 11-10507.

Cour de Cassation, Chambre commerciale, May 3, 2012, no. 11-10508.

Cour de Cassation, Chambre commerciale, February 12, 2013, no. 11-25914.

Cour de Cassation, Chambre commerciale, July 5, 2017, 14-16.737.

Cour de Cassation, Chambre criminelle, July 17, 1990, no. 90-82614.

Cour de Cassation, Chambre criminelle, November 26, 1990, no. 90-84590.

Cour de Cassation, Chambre criminelle, December 9, 1991, no. 88-80786, 90-84994.

Cour de Cassation, Chambre criminelle, February 27, 1996, no. 95-81366.

Cour de Cassation, Chambre criminelle, March 27, 1996, no. 95-82016.

Cour de Cassation, Chambre criminelle, October 9, 1996, no. 95-81232.

Cour de Cassation, Chambre criminelle, December 16, 1997, no. 96-85589.

Cour de Cassation, Chambre criminelle, December 1, 1998, no. 97-80560.

Cour de Cassation, Chambre criminelle, January 19, 1999, no. 98-83787.
Cour de Cassation, Chambre criminelle, September 15, 1999, no. 98-87624.
Cour de Cassation, Chambre criminelle, October 25, 2000, no. 00-80829.
Cour de Cassation, Chambre criminelle, June 26, 2001, 00-83.466.
Cour de Cassation, Chambre criminelle, December 17, 2003, 00-87.872.
Cour de Cassation, Chambre criminelle, April 6, 2004, 02-88.007.
Cour de Cassation, Chambre criminelle, February 7, 2006, 05-80.083.
Cour de Cassation, Chambre criminelle, February 7, 2006, no. 05-81888.
Cour de Cassation, Chambre criminelle, June 20, 2006, no. 05-85255.
Cour de Cassation, Chambre criminelle, February 7, 2007, no. 06-87753.
Cour de Cassation, Chambre criminelle, March 21, 2007, no. 06-89444.
Cour de Cassation, Chambre criminelle, April 24, 2007, no. 06-87656.
Cour de Cassation, Chambre criminelle, January 15, 2008, no. 07-86944.
Cour de Cassation, Chambre criminelle, June 4, 2008, no. 08-81045.
Cour de Cassation, Chambre criminelle, June 25, 2008, no. 07-80261.
Cour de Cassation, Chambre criminelle, September 9, 2008, no. 07-87281.
Cour de Cassation, Chambre criminelle, October 13, 2009, no. 09-80857.
Cour de Cassation, Chambre criminelle, December 8, 2009, no. 09-82120 and 09-82135.
Cour de Cassation, Chambre criminelle, February 23, 2010, no. 09-81819.
Cour de Cassation, Chambre criminelle, December 14, 2010, no. 10-80088.
Cour de Cassation, Chambre criminelle, October 11, 2011, no. 10-87212.
Cour de Cassation, Chambre criminelle, November 22, 2011, no. 11-84308.
Cour de Cassation, Chambre criminelle, November 29, 2011, no. 09-88250.
Cour de Cassation, Chambre criminelle, May 15, 2012, no. 11-83301.
Cour de Cassation, Chambre criminelle, June 12, 2012, no. 11-83657.
Cour de Cassation, Chambre criminelle, June 18, 2013, no. 12-85917.
Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81945.
Cour de Cassation, Chambre criminelle, October 22, 2013, no. 13-81949.
Cour de Cassation, Chambre criminelle, November 6, 2013, no. 12-87130.
Cour de Cassation, Chambre criminelle, January 14, 2014, no. 13-84909.
Cour de Cassation, Chambre criminelle, April 30, 2014, no. 13-88162.
Cour de Cassation, Chambre criminelle, January 6, 2015, no. 14-85448.
Cour de Cassation, Chambre criminelle, February 9, 2016, no. 15-85070.
Cour de Cassation, Chambre criminelle, June 22, 2016, no. 16-81834.
Cour de Cassation, Chambre criminelle, July 12, 2016, no. 15-86645.
Cour de Cassation, Chambre criminelle, June 28, 2017, no. 16-85291.
Cour de Cassation, Chambre criminelle, July 11, 2017, no. 17-80313.
Cour de Cassation, Chambre criminelle, January 9, 2018, no. 17-82946.
Cour de Cassation, Chambre criminelle, April 10, 2018, no. 17-85607.

Cour de Cassation, Chambre criminelle, May 24, 2018, no. 16-86.851.

Cour de Cassation, Chambre criminelle, June 20, 2018, no. 17-86651.

Cour de Cassation, Chambre criminelle, June 20, 2018, no. 17-86657.

Cour de Cassation, Chambre criminelle, December 11, 2018, no. 18-82365.

Cour de Cassation, Chambre criminelle, May 7, 2019, no. 18-85596.

Cour de Cassation, Chambre criminelle, January 29, 2020, no. 17-83577.

Cour de Cassation, Chambre criminelle, October 13, 2020, no. 20-80150.

Cour de Cassation, Chambre criminelle, November 25, 2020, no. 18-86955.

Cour de Cassation, Chambre criminelle, December 8, 2020, no. 20-83885.

Cour de Cassation, Chambre criminelle, June 16, 2021, no. 20-83098.

Cour de Cassation, Chambre criminelle, April 6, 2022, no. 21-84092.

Cour de cassation, Chambre criminelle, May 18, 2022, no. 21-82283.

Cour de cassation, Chambre criminelle, June 9, 2022, no. 22-90006.

Cour de cassation, Chambre criminelle, June 21, 2022, no. 20-86857.

Cour de Cassation, Chambre criminelle, July 12, 2022, no. 20-86652.

Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-83710.

Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-83820.

Cour de Cassation, Chambre criminelle, July 12, 2022, no. 21-84096.

Cour de Cassation, Chambre criminelle, October 11, 2022, no. 21-85148.

Cour de cassation, Chambre criminelle, October 12, 2022, no. 21-81648.

Cour de Cassation, Chambre criminelle, May 10, 2023, no. 22-86186.

Cour de cassation, Chambre criminelle, May 11, 2023, no. 22-85425.

3. Conseil d'Etat

Conseil d'État, 10ème - 9ème chambres réunies, March 27, 2020, no. 399922.

Conseil d'Etat, *French Data Network et autres*, April 21, 2021, no. 397844, 397851, 393099, 394922, 424717, 424718.

4. Others authorities

Tribunal de grande Instance de Paris, *Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" v. Yahoo ! Inc. et Yahoo France*, May 22, 2000, Ordonnance de référé.

Cour d'appel de Paris, 11ème chambre, *Timothy K. et Yahoo! Inc v. Ministère public, Association Amicale des déportés d'Auschwitz et des Camps de Haute Silésie, et MRAP*, March 17, 2004.

CNIL, *Délibération portant avis sur un projet de décret modifiant le décret n°2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale (demande d'avis n°18004354)*, September 26, 2019, no. 2019-119.

B. Romania

1. Curtea Constituţională

Curtea Constituţională, *Decizia referitoare la excepţia de neconstituţionalitate a prevederilor Legii nr.298/2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, precum şi pentru modificarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice*, October 8, 2009, no. 1298/2008.

Curtea Constituţională, *Decizia referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr.82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice și ale art.152 din Codul de procedură penală*, July 8, 2014, no. 440/014.

Curtea Constituţională, *Decizia referitoare la excepția de neconstituționalitate a dispozițiilor art. 145 din Codul de procedură penală*, April 6, 2017, no. 244/2017.

2. Înalta Curte de Casaţie şi Justiţie

Înalta Curte de Casaţie şi Justiţie - Secţia Penală, February 18, 2010, no. 626/2010.

3. Others authorities

Curtea de Apel Bucureşti Secţia I Penală, November 5, 2013, no. 11308/302/201.

Curtea de Apel Craiova, Secția penală, April 6, 2015, no. 483/2015.

Tribunalul Constanţa, October 21, 2015, no. 366/2015.

C. Spain

1. Tribunal Constitucional

Tribunal Constitucional, November 29, 1984, no. 114/1984.

Tribunal Constitucional, July 20, 1993, no. 254/1993.

Tribunal Constitucional, November 30, 2000, no. 292/2000.

Tribunal Constitucional, July 18, 2005, no. 205/2005.

Tribunal Constitucional, October 9, 2006, no. 281/2006.

Tribunal Constitucional, September 22, 2014, no. 145/2014.

2. Tribunal Supremo

Tribunal Supremo. Sala Primera, de lo Civil, de Diciembre de 2009, no. 773/2009.

Tribunal Supremo. Sala Primera, de lo Civil, May 18, 2010, no. 316/2010.

Tribunal Supremo. Sala Segunda, de lo Penal, May 20, 1996, no. 274/1996.

Tribunal Supremo. Sala Segunda, de lo Penal, February 3, 2006, no. 104/2006.

Tribunal Supremo. Sala Segunda, de lo Penal, June 22, 2007, no. 562/2007.

Tribunal Supremo. Sala Segunda, de lo Penal, July 5, 2007, no. 767/2007.

Tribunal Supremo. Sala Segunda, de lo Penal, May 9, 2008, no. 236/2008.

Tribunal Supremo. Sala Segunda, de lo Penal, May 28, 2008, no. 292/2008.

Tribunal Supremo. Sala Segunda, de lo Penal, July 14, 2010, no. 752/2010.

Tribunal Supremo. Sala Segunda, de lo Penal, de Abril de 2013, no. 342/2013.

Tribunal Supremo. Sala Segunda, de lo Penal, January 22, 2014, no. 7/2014.

Tribunal Supremo. Sala Segunda, de lo Penal, November 26, 2014, no. 850/2014.

Tribunal Supremo. Sala Segunda, de lo Penal, February 29, 2016, no. 154/2016.

Tribunal Supremo. Sala Segunda, de lo Penal, March 16, 2016, no. 221/2016.

Tribunal Supremo. Sala Segunda, de lo Penal, April 20, 2016, no. 329/2016.

Tribunal Supremo. Sala Segunda, de lo Penal, June 13, 2016, no. 516/2016.

Tribunal Supremo. Sala Segunda, de lo Penal, July 7, 2016, no. 610/2016.

Tribunal Supremo. Sala Segunda, de lo Penal, July 26, 2016, no. 1847/2015.

Tribunal Supremo. Sala Segunda, de lo Penal, February 23, 2017, no. 121/2017.

Tribunal Supremo. Sala Segunda, de lo Penal, February 7, 2019, no. 65/2019.

Tribunal Supremo. Sala Segunda, de lo Penal, November 13, 2019, no. 554/2019.

D. United States

1. US Supreme Court

US Supreme Court, *New York Central & Hudson River Railroad Co. v. US*, February 23, 1909, 212 U.S. 481.

US Supreme Court, *Giboney v. Empire Storage & Ice Co.*, April 4, 1949, 336 U.S. 490.

US Supreme Court, *Wieman v. Updegraff*, December 15, 1952, 344 U.S. 183.

US Supreme Court, *National Labor Relations Board v. Deena Artware, Inc.*, February 23, 1960, 361 U.S. 398.

US Supreme Court, *Gibson v. Florida Legislative Investigation Committee*, March 25, 1963, 372 U.S. 539.

US Supreme Court, *Brandenburg v. Ohio*, June 9, 1969, 395 U.S. 444.

US Supreme Court, *Miller v. California*, June 21, 1973, 413 U.S. 15.

US Supreme Court, *Paris Adult Theatre I v. Slaton*, June 21, 1973, 413 U.S. 49.

US Supreme Court, *Central Hudson Gas & Electric Corp. v. Public Service Commission*, June 20, 1980, 447 U.S. 557.

US Supreme Court, *US v. Bestfoods*, June 8, 1998, 524 U.S. 51.

US Supreme Court, *Sosa v. Alvarez-Machain et al.*, June 29, 2004, no. 03–339.

US Supreme Court, *Waddington v. Sarausad*, January 21, 2009, 479 F. 3d 671.

US Supreme Court, *Morrisson and others v. National Australia Bank Ltd. and others*, June 24, 2010, no. 08–1191, *547 F. 3d 167*.

US Supreme Court, *Kiobel v. Royal Dutch Petroleum Co. et al.*, April 17, 2013, no. 10–1491.

US Supreme Court, *Manhattan Community Access Corp. v. Halleck*, June 17, 2019, no. 17-1702, *587 U.S.*

US Supreme Court, *Doe v. Facebook, Inc.*, March 7, 2022, no. 21-459.

US Supreme Court, *Gonzalez, et al. petitioners v. Google LLC*, May 18, 2023, no. 21–1333.

US Supreme Court, *Twitter, Inc. v. Taamneh et al.*, May 18, 2023, no. 21–1496.

2. Others courts

US Court of Appeals, Seventh Circuit, *US v. Parfait Powder Puff*, November 4, 1947, 163 F.2d 1008.

US District Court, E.D. Pennsylvania, *US v. Johns-Manville Corporation*, April 16, 1964, 231 F. Supp. 690.

US District Court, E.D. Wisconsin, *Handlos v. Litton Industries, Inc.*, May 7, 1971, 326 F. Supp. 965.

US Court of Appeals, Ninth Circuit, *US v. Hilton Hotels Corp.*, September 26, 1972, 467 F.2d 1000.

US Court of Appeals, Ninth Circuit, *US v. Polizzi*, July 18, 1974, 500 F.2d 856.

US Court of Appeals, First Circuit, *US v. Bank of New England, N.A.*, June 10, 1987, 821 F.2d 844.

US Court of Appeals, Fifth Circuit, *US v. Alamo Bank of Texas*, September 14, 1989, 880 F.2d 828.

US District Court, Southern District of New York, *Cubby, Inc. v. CompuServe Inc.*, October 29, 1991, *776 F. Supp. 135*.

New York Supreme Court, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, May 24, 1995.

US District Court, E.D. Virginia, Alexandria Division, *Zeran v. America Online, Inc.*, March 21, 1997, *958 F. Supp. 1124*.

Court of Appeal of California, Fourth District, Division Two, *Wooten v. Superior Court*, October 30, 2001, *113 Cal. Rptr. 2d 195*.

US Court of Appeals, Ninth Circuit, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, June 27, 2005, *125 S. Ct. 2764*.

US Court of Appeals, Ninth Circuit, *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, April 3, 2008, no. 04-56916, 04-57173, *521 F.3d 1157*.

US Court of Appeals, Ninth Circuit, *Barnes v. Yahoo!, Inc.*, June 22, 2009, no. 05-36189, *570 F.3d 1096 (2009)*.

US Court of Appeals, Tenth Circuit, *Federal Trade Commi. v. Accusearch Inc.*, June 29, 2009, no. 08-800, *570 F.3d 1187*.

US District Court, N.D. Illinois, *Dart v. Craigslist, Inc.*, October 20, 2009, 09 C 1385, *665 F. Supp. 2d 961*.

US Court of Appeals, Ninth Circuit, *Coyote Publishing Inc. v. Miller*, March 11, 2010, no. 07-16633, *598 F.3d 592*.

US District Court Eastern District of Missouri Eastern Division, *M.A. ex rel P.K. v. Village Voice Media Holdings, LLC*, August 15, 2011, 4:10cv1740 TCM, *809 F. Supp. 2d 1041*.

US District Court, M.D. Tennessee, Nashville Division, *Backpage.Com, LLC v. Cooper*, January 3, 2013, 3:12-cv-00654, *939 F. Supp. 2d 805*.

US District Court Western District of Washington at Tacoma, *J.S. v. Vill. Voice Media Holdings, LLC*, March 5, 2013, 3:12-cv-06031-BHS.

US District Court Northern District of California, *USA v. Omuro and others*, June 24, 2014, 3:14-cr-00336.

Supreme Court of the State of Washington, *J.S. v. Vill. Voice Media Holdings, LLC*, September 3, 2015, no. 90510-0, *184 Wash.2d 95*.

US Court of Appeals, Seventh Circuit, *Backpage.com, LLC v. Dart*, November 30, 2015, no. 15–3047, *807 F.3d 229*.

US District Court Eastern District of New York, *United States v. Easy Rent Systems, Inc.*, January 28, 2016, 16-CR-45.

US Court of Appeals, Sixth Circuit, *United States v. Afyare*, March 2, 2016, no. 13-5924, *632 F. App'x 272*.

US Court of Appeals, First Circuit, *Doe No. 1 v. Backpage.com, LLC*, March 14, 2016, no. 15-1724, *817 F.3d 12, 17*.

Superior Court of the State of California, County of Sacramento, *People of the State of California v. Carl Ferrer*, November 16, 2016, no. 16FE019224, WL 7884408.

US District Court District of Massachusetts, *Doe No. 1 v. Backpage.com, LLC*, March 29, 2018, 17-11069-LTS.

US District Court Middle District of Florida Orlando Division, *Florida Abolitionist v. Backpage.com LLC*, March 31, 2018, 6:17-cv-218-Orl-28TBS.

US District Court, District of Arizona, *Miscellaneous Relief, US v. Lacey and others*, April 9, 2018, 2:18-cr-00422-SPL.

US District Court for the District of Columbia, *Woodhull Freedom Found. v. US*, September 24, 2018, 18-cv-01552 (RJL), *334 F. Supp. 3d 185*.

US Court of Appeals, Second Circuit, *Herrick v. Grindr LLC*, March 27, 2019, no. 18-396.

US Court of Appeals, District of Columbia, *Woodhull Freedom Found. v. United States*, January 24, 2020, no. 18-5298, *948 F.3d 363*.

US District Court, Southern District of California, *Doe v. KIK Interactive, Inc.*, August 31, 2020, 20-60702-CIV-SINGHAL, *482 F. Supp. 3d 1242*.

US District Court for the Southern District of Texas Houston Division, *A.B. v. Salesforce*, March 22, 2021, 4:30-CV-01254.

Supreme Court of Texas, *In re Facebook, Inc.*, June 25, 2021, no. 20-0434, *625 S.W.3d 80*.

Washington State Court of Appeals Division Two, *State Of Washington v. Darcus D. Allen*, July 27, 2021, 54007-0-II.

US District Court, Northern District of California, *Doe v. Twitter, Inc.*, August 19, 2021, 21-cv-00485-JCS, *555 F. Supp. 3d 889*.

US District Court, Central District of California, *Doe v. Mindgeek US Inc.*, November 2, 2021, 8:21-cv-00338-CJC-ADS.

California Court of Appeals, First District, Second Division, *Does v. Salesforce.com*, December 30, 2021, no. A159566.

US District Court, Northern District of Alabama, *Doe v. MG Freesites, Ltd.*, February 9, 2022, 7:21-cv-00220-LSC.

US District Court, District of Columbia, *Woodhull Freedom Found. v. United States*, March 29, 2022, 18-1552 (RJL).

US District Court, Western District of Washington, *M.L. v. Craigslist, Inc.*, April 25, 2022, C19-6153 BHS-TLF.

US District Court, Northern District of Illinois, *G.G. v. Salesforce.com*, May 16, 2022, 20-cv-02335.

US Court of Appeals, District of Columbia, *Woodhull Freedom Found. v. US (Opening Brief)*, June 9, 2022, no. 22-5105.

US District Court, District of Oregon, *A.M v. Omegle.com*, July 13, 2022, 3:21-cv-01674-MO.

US Court of Appeals, Ninth Circuit, *Plaintiff-Appellee, v. Lacey, Larkin, Spear, Brunst, Padilla, Vaught*, September 21, 2022, no. 22-10000.

US Court of Appeals, Ninth Circuit, *Does 1-6 v. Reddit, Inc.*, October 24, 2022, no. 21-56293, *2022 WL 13743458*.

US Court of Appeals, Ninth Circuit, *Doe v. Twitter, Inc.*, May 3, 2023, no. 22-15103, *3:21-cv-00485-JCS*.

US Court of Appeals, Ninth Circuit, *J.B. v. Craigslist, Inc.*, May 3, 2023, no. 22-15290, *4:19-cv-07848-HSG*.

US Court of Appeals, Ninth Circuit, *Vargas v. Facebook, Inc.*, June 23, 2023, no. 21-16499, *3:19-cv-05081-WHO*.

E. Belgium

Cour de cassation (Belgium), *YAHOO ! Inc.*, December 1, 2015, P.13.2082.N.

Cour de cassation (Belgium), *Skype*, February 19, 2019, P.17.1229.N.

F. Germany

Bundesverfassungsgericht, December 15, 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

II. Supranational case law

A. European Court of Human Rights

ECHR, *Handyside v. the United Kingdom*, December 7, 1976, no. 5493/72.

ECHR, *Klass and others v. Germany*,September 6, 1978, no. 5029/71.

ECHR, *Sunday Times v. the United Kingdom (no. 1)*, April 26, 1979, no. 6538/74.

ECHR, *Malone v. the United Kingdom*, August 2, 1984, no. 8691/79.

ECHR, *Leander v. Sweden*, March 26, 1987, no. 9248/81.

ECHR, *Müller and Others v. Switzerland*, May 24, 1988, no. 10737/84.

ECHR, *Schenk v. Switzerland*, July 12, 1988, no. 10862/84.

ECHR, *Soering v. the United Kingdom*, July 7, 1989, no. 14038/88.

ECHR, *Kruslin v. France*, April 24, 1990, no. 11801/85.

ECHR, *Huvig v. France*, April 24, 1990, no. 11105/84.

ECHR, *Autronic Ag v. Switzerland*, May 22, 1990, no. 12726/87.

ECHR, *Lüdi v. Switzerland*, June 15, 1992, no. 12433/86.

ECHR, *Otto-Preminger-Institut v. Austria*, September 20, 1994, no. 13470/87.

ECHR, *Loizidou v. Turkey (preliminary objections)*, March 23, 1995, no. 15318/89.

ECHR, *Goodwin v. the United Kingdom*, March 27, 1996, no. 17488/90.

ECHR, *Wingrove v. the United Kingdom*, November 25, 1996, no. 17419/90.

ECHR, *Kopp v. Switzerland*, March 25, 1998, no. 13/1997/797/1000.

ECHR, *Vasilescu v. Romania*, May 22, 1998, no. 53/1997/837/1043.

ECHR, *Teixeira de Castro v. Portugal*, June 9, 1998, no. 44/1997/828/1034.

ECHR, *Valenzuela Contreras v. Spain*, July 30, 1998, no. 58/1997/842/1048.

ECHR, *Lambert v. France*, August 24, 1998, no. 88/1997/872/1084.

ECHR, *A. v. the United Kingdom*, September 23, 1998, no. 100/1997/884/1096.

ECHR, Smith and Grady v. the United Kingdom, September 27, 1999, 33985/96, 33986/96.

ECHR, *Nilsen and Johnsen v. Norway*, November 25, 1999, no. 23118/93.

ECHR, *Fuentes Bobo v. Spain*, February 29, 2000, no. 39293/98.

ECHR, *Ozgur Gundem v. Turkey*, March 16, 2000, no. 23144/93.

ECHR, *Z. and Others v. the United Kingdom*, May 10, 2001, no. 29392/95.

ECHR, *Association Ekin v. France*, July 17, 2001, no. 39288/98.

ECHR, *P.G. and J.H. v. the United Kingdom*, September 25, 2001, no. 44787/98.

ECHR, *Allan v. the United Kingdom*, November 5, 2002, no. 48539/99.

ECHR, *Peck v. the United Kingdom*, January 28, 2003, no. 44647/98.

ECHR, *Prado Bugallo v. Spain*, February 18, 2003, no. 58496/00.

ECHR, *Sequeira v. Portugal*, May 6, 2003, no. 73557/01.

ECHR, *Edwards and Lewis v. the United Kingdom*, July 22, 2003, 39647/98 and 40461/98

ECHR, *M.C. v. Bulgary*, December 4, 2003, no. 39272/98.

ECHR, *Eurofinacom v. France*, September 7, 2004, no. 58753/00.

ECHR, *Aalmoes and Others v. the Netherlands*, November 25, 2004, no. 16269/02.

ECHR, *Matheron v. France*, March 29, 2005, no. 57752/00.

ECHR, *Appleby and Others v. the United Kingdom*, May 6, 2005, no. 44306/98.

ECHR, *Vetter v. France*, May 31, 2005, no. 59842/00.

ECHR, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Irlande*, June 30, 2005, no. 45036/98.

ECHR, *Siliadin v. France*, July 26, 2005, no. 73316/01.

ECHR, *Shannon v. the United Kingdom*, October 4, 2005, no. 6563/03.

ECHR, *Perrin v. the United Kingdom*, October 18, 2005, no. 5446/03.

ECHR, *Vanyan v. Russia*, December 15, 2005, no. 53203/99.

ECHR, *Wisse v. France*, December 20, 2005, no. 71611/01.

ECHR, *V.D. and C.G. v. France*, June 22, 2006, no. 68238/01.

ECHR, *Weber and Saravia v. Germany*, June 29, 2006, no. 54934/00.

ECHR, *Khudobin v. Russia*, October 26, 2006, no. 59696/00.

ECHR, *Copland v. the United Kingdom*, April 3, 2007, no. 62617/00.

ECHR, *Dumitri Popescu v. Romania*, April 26, 2007, no. 71525/01.

ECHR, *Paeffgen Gmbh v. Germany*, September 18, 2007, 25379/04, 21688/05, 21722/05, 21770/05.

ECHR, *Ramanauskas v. Lithuania (1)*, February 5, 2008, no. 74420/01.

ECHR, *Milinienė v. Lithuania*, June 24, 2008, no. 74355/01.

ECHR, *Liberty and others v. the United Kingdom*, July 1, 2008, no. 58243/00.

ECHR, *Malininas v. Lithuania*, July 1, 2008, no. 10071/04.

ECHR, *S. and Marper v. the United Kingdom*, December 4, 2008, 30562/04 et 30566/04.

ECHR, *Women on Waves and Others v. Portugal*, February 3, 2009, no. 31276/05.

ECHR, *Iordachi and others v. Moldova*, February 10, 2009, no. 25198/02.

ECHR, *Constantin and Stoian v. Romania*, September 29, 2009, 23782/06 and 46629/06.

ECHR, *Burak Hun v. Turkey*, December 15, 2009, no. 17570/04.

ECHR, *Rantsev v. Cyprus and Russia*, January 7, 2010, no. 25965/04.

ECHR, *Akdaş v. Turkey*, February 16, 2010, no. 41056/04.

ECHR, *Medvedyev and Others v. France*, March 29, 2010, no. 3394/03.

ECHR, *Fatullayev v. Azerbaijan*, April 22, 2010, no. 40984/07.

ECHR, *Kennedy v. the United Kingdom*, May 18, 2010, no. 26839/05.

ECHR, *Cox v. Turkey*, May 20, 2010, no. 2933/03.

ECHR, *Uzun v. Germany*, September 2, 2010, no. 35623/05.

ECHR, *Dink v. Turkey*, September 14, 2010, 2668/07, 6102/08, 30079/08, 7072/09, 7124/09.

ECHR, *Bannikova v. Russia*, November 4, 2010, no. 18757/06.

ECHR, *Moulin v. France*, November 23, 2010, no. 37104/06.

ECHR, *Aleksey Ovchinnikov v. Russia*, December 16, 2010, no. 24061/04.

ECHR, *Mosley v. the United Kingdom*, May 10, 2011, no. 48009/08.

ECHR, *Karttunen v. Finland*, May 10, 2011, no. 1685/10.

ECHR, *Amann v. Switzerland*, October 18, 2011, no. 27798/95.

ECHR, *Axel Springer Ag v. Germany*, February 7, 2012, no. 39954/08.

ECHR, *Vejdeland and Others v. Sweden*, February 9, 2012, no. 1813/07.

ECHR, *Mouvement raëlien suisse v. Switzerland*, July 13, 2012, no. 16354/06.

ECHR, *M. and Others v. Italy and Bulgaria*, July 31, 2012, no. 40020/03.

ECHR, *Michaud v. France*, December 6, 2012, no. 12323/11.

ECHR, *Ahmet Yildrim v. Turkey*, December 18, 2012, no. 3111/10.

ECHR, *Ashby Donald and Others v. France*, January 10, 2013, no. 36769/08.

ECHR, *Neij and Sunder Kolmisoppi v. Sweden (The Pirate Bay)*, February 19, 2013, no. 40397/12.

ECHR, *Animal Defenders International v. the United Kingdom*, April 22, 2013, no. 48876/08.

ECHR, *Sepil v. Turkey*, November 12, 2013, no. 17711/07.

ECHR, *Sandu v. the Republic of Moldova*, February 11, 2014, no. 16463/08.

ECHR, *Akdeniz and Others v. Turkey*, March 11, 2014, no. 20877/10.

ECHR, *Nosko and Nefedov v. Russia*, October 30, 2014, 5753/09 and 11789/10.

ECHR, *Morice v. France*, April 23, 2015, no. 29369/10.

ECHR, *Delfi AS v. Estonie*, June 16, 2015, no. 64569/09.

ECHR, *Cengiz and Others v. Turkey*, December 1, 2015, 48226/10 and 14027/11.

ECHR, *Roman Zakharov v. Russia*, December 4, 2015, no. 47143/06.

ECHR, *Szabó and Vissy v. Hungary*, January 12, 2016, no. 37138/14.

ECHR, *L.E. v. Greece*, January 21, 2016, no. 71545/12.

ECHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, February 2, 2016, no. 22947/13.

ECHR, *Avotiņš v. Latvia*, May 23, 2016, no. 17502/07.

ECHR, *J. and others v. Austria*, January 17, 2017, no. 58216/12.

ECHR, *Pihl v. Sweden*, February 7, 2017, no. 74742/14.

ECHR, *Modestou v. Greece*, March 16, 2017, no. 51693/13.

ECHR, *Chowdury and Others v. Greece*, March 30, 2017, no. 21884/15.

ECHR, *Matanović v. Croatia*, April 4, 2017, no. 2742/12.

ECHR, *Bože v. Latvia*, May 18, 2017, no. 40927/05.

ECHR, *Trabajo Rueda v. Spain*, May 30, 2017, no. 32600/12.

ECHR, *Bayev and Others v. Russia*, June 20, 2017, no. 67667/09.

ECHR, *Bărbulescu v. Romania*, September 5, 2017, no. 61496/08.

ECHR, *Ben Faiza v. France*, February 8, 2018, no. 31446/12.

ECHR, *Ramanauskas v. Lithuania (2)*, February 20, 2018, no. 55146/14.

ECHR, Benedik v. Slovenia, April 24, 2018, no. 62357/14.

ECHR, *Tchokhonelidze v. Georgia*, June 28, 2018, 5753/09 and 11789/10.

ECHR, *Mariya Alekhina and Others v. Russia*, July 17, 2018, no. 38004/12.

ECHR, *Big Brother Watch and others v. the United Kingdom (1)*, September 13, 2018, 58170/13, 62322/14 and 24960/15.

ECHR, *Selahattin Demirtas v. Turkey (3)*, July 9, 2019, no. 8732/11.

ECHR, *Ringler v. Austria*, May 12, 2020, no. 2309/10.

ECHR, *Engels v. Russia*, June 23, 2020, no. 61919/16.

ECHR, *Bulgakov v. Russia*, June 23, 2020, no. 20159/15.

ECHR, *Vladimir Kharitonov v. Russia*, June 23, 2020, no. 10795/14.

ECHR, *Ooo Flavus and others v. Russia*, June 23, 2020, 12468/15, 23489/15 and 19074/16.

ECHR, *S.M. v. Croatia*, June 25, 2020, no. 60561/14.

ECHR, *V.C.L. and A.N. v. the United Kingdom*, February 16, 2021, 77587/12 and 74603/12.

ECHR, *Bivolaru and Moldovan v. France*, March 25, 2021, 40324/16 and 12623/17.

ECHR, *Centrum För Rättvisa v. Sweden (2)*, May 25, 2021, no. 35252/08.

ECHR, *Big Brother Watch and others v. the United Kingdom (2*), May 25, 2021, 58170/13, 62322/14 and 24960/15.

ECHR, *Hurbain v. Belgium*, June 22, 2021, no. 57292/16.

ECHR, *Zoletic and Others v. Azerbaijan*, October 7, 2021, no. 20116/12.

ECHR, *A.L. and E.J. v. France [Encrochat]*, pending, 44715/20 and 47930/21.

B. Court of Justice of the European Union

ECJ, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration*, February 5, 1963, no. 26-62.

ECJ, *Anciens Etablissements D. Angenieux fils aîné and Caisse primaire centrale d'assurance maladie de la région parisienne v. Willy Hakenberg*, July 12, 1973, C-13/37.

ECJ, *Yvonne van Duyn v Home Office*, December 4, 1974, no. 41-74.

ECJ, *Handelskwekerij G. J. Bier B.V. v Mines de Potasse d'Alsace S.A. (preliminary ruling requested by the Gerechtshof of The Hague)*, November 30, 1976, C-21/76.

ECJ, *Silvani Di Paolo v. Office National de l'Emploi*, February 17, 1977, C-76/76.

ECJ, *Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein*, February 20, 1979, C-120/78.

ECJ, *Criminal proceedings against Tullio Ratti*, April 5, 1979, no. 148/78.

ECJ, *Rezguia Adoui v Belgian State and City of Liège; Dominique Cornuaille v Belgian State*, May 18, 1982, no. 115 and 116/81.

ECJ, *Foto-Frost v. Hauptzollamt Lübeck-Ost*, October 22, 1987, C-314/85.

ECJ, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL, Chequepoint International Ltd and Presse Alliance SA*, March 7, 1995, C-68/93.

ECJ, *Aldona Malgorzata Jany e.a. and Staatssecretaris van Justitie*, November 20, 2001, C-268/99.

ECJ, *Bodil Lindqvist*, November 6, 2003, C-101/01.

ECJ, *Ireland v. European Parliament and Council of the European Union*, February 10, 2009,

C-301/06.

CJEU, *Google France SARL and Google Inc. v. Louis Vuitton Malletier SA (C-236/08), Google France SARL v. Viaticum SA and Luteciel SARL (C-237/08), Google France SARL v. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin and Tiger SARL (C-238/08)*, March 23, 2010, C-236/08 to C-238/08.

CJEU, *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08), and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)*, December 7, 2010, C-585/08 and C-144/09.

CJEU, *L'Oréal SA and others v. eBay International AG*, July 12, 2011, C-324/09.

CJEU, *eDate Advertising GmbH v. X; and Olivier Martinez, Robert Martinez v. MGN Limited*, October 25, 2011, C-509/09 and C-161/10.

CJEU, *Proceedings relating to the execution of European arrest warrants issued against Ciprian Vasile Radu*, January 29, 2013, C-396/11.

CJEU, *Stefano Melloni v. Ministerio Fiscal*, February 26, 2013, C-399/11.

CJEU, *Peter Pinckney v. KDG Mediatech AG*, October 3, 2013, C-170/12.

CJEU, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH et Wega Filmproduktionsgesellschaft mbH*, March 27, 2014, C-314/12.

CJEU, *Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a. (C-594/12) v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána and Ireland*, April 8, 2014, C-293/12 and C-594/12.

CJEU, *Google Spain SL and Google Inc. v. AEPD and Mario Costeja González*, May 13, 2014, C-131/12.

CJEU, *Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis*, September 11, 2014, C-291/13.

CJEU, *Pez Hejduk v EnergieAgentur.NRW GmbH*, January 22, 2015, C-441/13.

CJEU, *Minister for Justice and Equality v. Francis Lanigan*, July 16, 2015, C-237/15 PPU.

CJEU, *Maximillian Schrems v. Data Protection Commissioner (Schrems I)*, October 6, 2015, C-362/14.

CJEU, *Pál Aranyosi and Robert Căldăraru v. Generalstaatsanwaltschaft Bremen*, April 5, 2016, C-404/15 and C-659/15 PPU.

CJEU, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, September 15, 2016, C-484/14.

CJEU, *Patrick Breyer v. Bundesrepublik Deutschland*, October 19, 2016, C-582/14.

CJEU, *Concurrence SARL v Samsung Electronics France SAS, Amazon Services Europe Sàrl*, December 21, 2016, C-618/15.

CJEU, *Tele2 Sverige AB v. Post-och telestyrelsen*, December 21, 2016, C-203/15 and C-698/15.

CJEU, *Stichting Brein v. Ziggo BV, XS4ALL Internet BV*, June 14, 2017, C-610/15.

CJEU, *Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data*, July 26, 2017, Opinion 1/15.

CJEU, *Envisaged agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, July 26, 2017, Opinion 1/15.

CJEU, *Asociación Profesional Elite Taxi v. Uber Systems Spain SL*, December 20, 2017, C-434/15.

CJEU, *Uber France SAS*, April 10, 2018, C-320/16.

CJEU, *Coöperatieve Vereniging SNB-REACT U.A. v. Deepak Mehta*, August 7, 2018, C-521/17.

CJEU, *Ministerio Fiscal*, October 2, 2018, C-207/16.

CJEU, *Minister for Justice and Equality v. OG and PI*, May 27, 2019, C-508/18 and C-82/19 PPU.

CJEU, *Minister for Justice and Equality v. PF*, May 27, 2019, C-509/18.

CJEU, *GC, AF, BH and ED v. CNIL*, September 24, 2019, C-136/17.

CJEU, *Google LLC v. CNIL*, September 24, 2019, C-507/17.

CJEU, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd*, October 3, 2019, C-18/18.

CJEU, *JR and YC*, December 12, 2019, C-566/19 PPU and C-626/19 PPU.

CJEU, *Airbnb Ireland UC*, December 19, 2019, C-390/18.

CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*, July 16, 2020, C-311/18.

CJEU, *Criminal proceedings against A and Others*, December 8, 2020, C-584/19.

CJEU, *European Commission v. Kingdom of Spain*, February 25, 2021, C-658/19.

CJEU, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs v. Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées ; and Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministres*, October 6, 2020, C-511/18, C-512/18, C-520/18.

CJEU, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, October 6, 2020, C-623/17.

CJEU, *Frank Peterson v. Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH (C-682/18), and Elsevier Inc. v. Cyando AG (C-683/18)*, June 22, 2021, C-682/18 and C-683/18.

CJEU, *Gtflix Tv v. DR*, December 21, 2021, C-251/20.

CJEU, *G.D. v. Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, April 5, 2022, C-140/20.

CJEU, *TU and RE v. Google LLC*, December 8, 2022, C-460/20.

CJEU, *Staatsanwaltschaft Berlin [Encrochat]*, pending, C-670/22.

C. Others

Permanent Court of International Justice, *Wimbledon*, August 17, 1923, E. b Docket III.

Permanent Court of International Justice, *Lotus*, September 7, 1927, no. 9.

Trial Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*, February 22, 2001, IT-96-23-T&IT-96-23/1-T.

Appels Chamber, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, *Prosecutor v. Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic*, June 12, 2002, IT-96-23 & IT-96-23/1-A.

Inter-American Court of Human Rights, *Hacienda Brasil Verde Workers v. the Federative Republic of Brazil*, October 20, 2016.

§8. Grey literature

I. National grey literature

A. France

BOUCHOUX C. et al., *Rapport d'information sur les femmes et les mineur-e-s victimes de la traite des êtres humains*, no. 448, Sénat, March 9, 2016.

CNCDH, "Avis sur le 2nd plan d'action national contre la traite des êtres humains (2019-2021)," December 1, 2019.

CNCDH, "Avis sur la traite des êtres humains à des fins d'exploitation économique," October 15, 2020.

CNCDH, "Avis - Evaluation du plan d'action national contre la traite des êtres humains (2019-2021)," January 12, 2023, A-2023-1.

CNNUM, "Ambition numérique Pour une politique française et européenne de la transition numérique - Rapport remis au Premier Ministère," June 2015.

COMMISSION NATIONALE DE LUTTE CONTRE LE TRAVAIL ILLEGAL, "Plan national de lutte contre le travail illégal (2023-2027)," Direction Générale du Travail, May 22, 2023.

COUR DE CASSATION, *Le juge et la mondialisation: dans la jurisprudence de la Cour de cassation - Etude annuelle 2017*, La Documentation Française, 2018.

CONSEIL D'ÉTAT (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 1.

CONSEIL D'ÉTAT (ed.), *Droit comparé et territorialité du droit - un cycle de conférences du Conseil d'État*, La Documentation Française, 2017, vol. 2.

CONSEIL D'ETAT, "Etude - Internet et les réseaux numériques," République française, November 30, 1997.

DEFENSEUR DES DROITS, CNIL, "Algorithmes : prévenir l'automatisation des discriminations," 2020.

DURANTON N., *Rapport d'information sur les actes du colloque « Droits de l'Homme et démocratie à l'ère numérique », organisé le 14 novembre 2019, dans le cadre de la présidence française du Comité des ministres du Conseil de l'Europe*, Sénat Session ordinaire 2019-2020, 2019.

DUTHILLEUL A., DE JOUVENEL M., *Evaluation de la mise en oeuvre de la loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre*, 2019/12/CGE/SG, Conseil Général de l'économie, de l'industrie, de l'énergie et des technologies, January 2020.

GAUVAIN R. et al., *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, Rapport au Premier Ministre, June 26, 2019.

GEOFFROY G., *Rapport d'information sur la prostitution en France*, no. 3334, Assemblée Nationale, April 13, 2011.

GOUVERNEMENT, *Lancement du premier plan national de lutte contre la prostitution des mineurs*, November 15, 2021.

GROUPE DE DIAGNOSTIC STRATEGIQUE, *Vers une police 3.0 : enjeux et perspectives à l'horizon 2025*, no. 3, INHESJ, 27e Session nationale « Sécurité et Justice » - 2015/2016, June 2016.

GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Protéger les Internautes - Rapport sur la cybercriminalité*, February 2014.

GROUPE DE TRAVAIL SUR LA PROSTITUTION DES MINEURS, *Rapport sur la prostitution des mineurs*, June 28, 2021.

INSPECTION GENERALE DES AFFAIRES SOCIALES, INSPECTION GENERALE DE L'ADMINISTRATION, INSPECTION GENERALE DE LA JUSTICE, "Evaluation de la loi du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées," December 2019.

MINISTERE DE LA JUSTICE, Circulaire de lutte contre le proxénétisme, December 18, 2001.

MINISTERE DE LA JUSTICE, Circulaire de présentation des dispositions de droit pénal de la loi n° 2003-239 du 18 mars pour la sécurité intérieure et de la loi n° 2003-88 du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xénophobe, February 3, 2003.

MINISTERE DE LA JUSTICE, Circulaire de présentation de la loi n°2014-372 relative à la géolocalisation, April 1, 2014.

MINISTERE DE LA JUSTICE, Circulaire de politique pénale en matière de lutte contre la traite des êtres humains, January 22, 2015.

MISSION INTERMINISTERIELLE POUR LA PROTECTION DES FEMMES CONTRE LES VIOLENCES ET LA LUTTE CONTRE LA TRAITE DES ETRES HUMAINS, SECRETARIAT D'ETAT CHARGE DE L'EGALITE ENTRE LES FEMMES ET LES HOMMES ET DE LA LUTTE CONTRE LES DISCRIMINATIONS, "2nd plan d'action national contre la traite des êtres humains 2019-2021," 2019.

MISSION MINISTERIELLE PROJETS ANNUELS DE PERFORMANCE, "Budget général - Annexe au projet de loi de finances pour 2021 - Justice," 2020.

SAINT-MARTIN L., HETZEL P., *Rapport général au nom de la commission des finances, de l'économie générale et du contrôle budgétaire sur le projet de loi de finances pour 2022 (n° 4482) - Annexe n° 18 Justice*, no. 4482, Assemblée Nationale, October 7, 2021.

SERVICE STATISTIQUE MINISTERIEL DE LA SECURITE INTERIEURE, "La traite et l'exploitation des êtres humains depuis 2016 : une approche par les données administratives," *Interstats*, October 2021, no. 36, p. 1.

SERVICE STATISTIQUE MINISTERIEL DE LA SECURITE INTERIEURE, "La traite et l'exploitation des êtres humains depuis 2016 : une approche par les données administratives," *Interstats*, October 2022, no. 49, p. 1.

SOURD A., BENADDOU L., VIGNOLLES L., *La traite des êtres humains en France Le profil des victimes suivies par les associations en 2021*, Service statistique ministériel de la sécurité intérieure, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, 2022.

SOURD A., VACHER A., *La traite des êtres humains en France Profil des victimes suivies par les associations en 2018*, Troisième enquête annuelle, Observatoire national de la délinquance et des réponses pénales, Mission interministérielle pour la protection des femmes contre les violences et la lutte contre la traite des êtres humains, 2019.

THIEULIN B., *Towards a European digital sovereignty policy*, Opinion of the Economic, Social and Environmental Council, March 13, 2019.

WARSMANN J.-L., *Rapport d'information sur la mise en application de la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*, no. 2378, Assemblée nationale, June 15, 2005.

1. Non-governmental organizations

AMICALE DU NID, *Rapport d'activité 2018*, June 2019.

AMICALE DU NID, *Rapport d'activité 2020*, June 2021.

ASSOCIATION ALC, "Identifier, accueillir et accompagner les victimes de la traite des êtres humains - Guide pratique," Dispositif National Ac.Sé, République française, February 2014.

RENAUD J. et al., *Loi sur le devoir de vigilance des sociétés mères et entreprises donneuses d'ordre - Année 1 : les entreprises doivent mieux faire*, Forum Citoyen pour la RSE, February 2019.

B. Romania

AGENŢIA NAŢIONALĂ ÎMPOTRIVA TRAFICULUI DE PERSOANE, "ANITP şi OLX, impreună pentru siguranţa ta," *ANITP*, October 31, 2018, online https://anitp.mai.gov.ro/4999-2/ (retrieved on July 5, 2022).

AGENŢIA NAŢIONALĂ ÎMPOTRIVA TRAFICULUI DE PERSOANE, "National Identification and Referral Mechanism of Victims of Trafficking in Persons," 2019.

AGENTIA NATIONALA ÎMPOTRIVA TRAFICULUI DE PERSOANE, "Raport anual privind fenomenul traficului de persoane in 2019," 2020.

AGENTIA NATIONALA ÎMPOTRIVA TRAFICULUI DE PERSOANE, "Raport Anual privind fenomenul traficului de persoane în anul 2021," 2022.

GUVERNUL, "Strategie naţională împotriva traficului de persoane pentru perioada 2018-2022," October 31, 2018.

C. Spain

CENTRO DE INTELIGENCIA CONTRA EL TERRORISMO Y EL CRIMEN ORGANIZADO, "Plan estratégico nacional contra la trata y la explotación de seres humanos 2021-2023," Secretaría de Estado de seguridad, Ministerio del Interior, January 2022.

DELEGACIÓN DEL GOBIERNO CONTRA LA VIOLENCIA DE GÉNERO, "Protocolos de Coordinación Interinstitucional," *Ministerio de Igualdad*, no date, online https://violenciagenero.igualdad.gob.es/otrasFormas/trata/normativaProtocolo/marco/home.htm (retrieved on December 2, 2021).

DIRECCIÓN GENERAL DE LA MUJER, "Protocolo para la protección de las víctimas de trata de seres humanos en la comunidad de Madrid," Comunidad de Madrid, November 2017.

DOLZ LAGO M.J., "Apuntes sobre las penas con dimensión laboral en el régimen español de responsabilidad penal de las personas jurídicas," *in* FISCALÍA GENERAL DEL ESTADO (ed.), *La responsabilidad penal de las personas jurídicas: homenaje al Excmo. Sr. D. José Manuel Maza Martín*, Ministerio de Justicia, 2018, p. 79.

FISCALÍA GENERAL DEL ESTADO, Circular 1/2011 relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010, *FIS-C-2011-00001*, June 1, 2011.

FISCALÍA GENERAL DEL ESTADO, Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, *FIS-C-2016-00001*, January 22, 2016.

FISCALÍA GENERAL DEL ESTADO, Circular 1/2019 sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal, March 6, 2019.

FISCALÍA GENERAL DEL ESTADO, Circular 2/2019 sobre interceptación de comunicaciones telefónicas y telemáticas, March 6, 2019.

FISCALÍA GENERAL DEL ESTADO, Circular 3/2019 sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, March 6, 2019.

FISCALÍA GENERAL DEL ESTADO, Circular 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, March 6, 2019.

MARCHENA GÓMEZ M., "La contribución del magistrado José Manuel Maza a la consolidación de un modelo de autorresponsabilidad penal de las personas jurídicas," *in* FISCALÍA GENERAL DEL ESTADO (ed.), *La responsabilidad penal de las personas jurídicas: homenaje al Excmo. Sr. D. José Manuel Maza Martín*, Ministerio de Justicia, 2018, p. 241.

MINISTERIO DE JUSTICIA et al., "Framework protocol for protection of victims of human trafficking," October 28, 2011.

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD, "Plan integral de lucha contra la trata de mujeres y niñas con fines de explotación sexual 2015-2018," 2014.

REGIDORIA D'IGUALTAT I POLÍTIQUES INCLUSIVES, "Protocolo de intervención con víctimas de trata para la explotación sexual en la ciudad de València," Ajuntament de València, April 2017.

UNIDAD DE EXTRANJERÍA, "Diligencias de seguimiento del delito de trata de seres humanos año 2020," Fiscalía General del Estado, 2021.

D. United States

BIGIO J., VOGELSTEIN R.B., *Ending Human Trafficking in the Twenty-First Century*, no. 91, Council on Foreign Relations,, Council Special Report, June 2021.

BOUCHÉ V., *An Empirical Analysis of the Intersection of Organized Crime and Human Trafficking In the United States*, National criminal justice reference service - Office of Justice Programs, July 2017.

DARPA, "Memex," no date, online https://www.darpa.mil/about-us/timeline/memex (retrieved on April 27, 2021).

DEPARTMENT OF JUSTICE, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment - Press Release Number: 18 - 427," *The United States Department of Justice*, April 9, 2018, online https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads (retrieved on May 23, 2022).

DEPARTMENT OF JUSTICE, "National Strategy to Combat Human Trafficking," January 2017.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2013.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2017.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2018.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2019.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2021.

DEPARTMENT OF STATE, "Trafficking in persons report," June 2023.

DEPARTMENT OF JUSTICE, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, "The crime of human trafficking - A Law Enforcement Guide to Identification and Investigation," January 1, 2007.

KHODARKOVSKY J., RUSSO A.N., BRITSCH L.E., "Prosecuting sex trafficking cases in the wake of the Backpage takedown and the world of cryptocurrency," *Department of Justice journal of federal law and practice USA*, 2021, vol. 69, no. 3, pp. 101-126.

OFFICE TO MONITOR AND COMBAT TRAFFICKING IN PERSONS, "Trafficking in Persons Report: France," *US Department of State*, 2023, online https://www.state.gov/reports/2023-trafficking-in-persons-report/france/ (retrieved on July 6, 2023).

PELLERIN C., "DARPA Program Helps to Fight Human Trafficking," *U.S. Department of Defense*, 2017, online https://www.defense.gov/News/News-Stories/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ (retrieved on January 14, 2022).

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, *Backpage.com's knowing facilitation of online sex trafficking*, Committee on Homeland Security and Governmental Affairs, January 10, 2017.

THE WHITE HOUSE, "The National Action Plan To Combat Human Trafficking," December 2021.

US GOVERNMENT ACCOUNTABILITY OFFICE, *Virtual currencies. Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, December 2021, GAO-22-105462.

US GOVERNMENT ACCOUNTABILITY OFFICE, *Sex trafficking - Online Platforms and Federal Prosecutions*, June 2021.

1. Non-governmental organizations

CONSUMER WATCHDOG et al., *How Google's backing of Backpage protects child sex trafficking*, May 17, 2017.

GLAAD, *Social media safety index*, 2021.

FEEHS K., CURRIER WHEELER A., *2019 Federal Human Trafficking Report*, Human Trafficking Institute, 2020.

LANE L., GRAY A., RODOLPH A., *2021 Federal Human Trafficking Report*, Human Trafficking Institute, 2022.

LANE L. et al., *2022 Federal Human Trafficking Report*, Human Trafficking Institute, 2023.

E. Germany

BUNDESKRIMINALAMT, *Human trafficking and exploitation National Situation Report 2020*, 2020.

PEARSON E., "Organ Trafficking – Challenges and Perspectives," *in* SECTOR PROJECT AGAINST TRAFFICKING IN WOMEN (ed.), *Challenging Trafficking in Persons - Theoretical Debate & Practical Approaches*, Federal Ministry for Economic Cooperation and Developement, Allemagne, Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH, 2005.

PRASAD N., ROHNER B., "Undocumented Migration, Labour Exploitation and Trafficking," *in* SECTOR PROJECT AGAINST TRAFFICKING IN WOMEN (ed.), *Challenging Trafficking in Persons - Theoretical Debate & Practical Approaches*, Federal Ministry for Economic Cooperation and Developement (Germany), Deutsche Gesellschaft für Technische Zusammenarbeit (GTZ) GmbH, 2005, pp. 39-43.

1. Non-governmental organizations

CZARNECKI D., *Trafficking in human beings 2.0 - Digitalisation of trafficking in human beings in Germany - Developments and Courses of Action*, KOK, German NGO Network against Trafficking in Human Beings, 2023.

F. United Kindgom

HM GOVERNMENT et al., *2021 UK Annual Report on Modern Slavery*, October 2021.

1. Modern slavery statements

GOOGLE, "2021 Statement Against Modern Slavery," June 2022.

MASTERCARD, "Modern Day Slavery & Human Trafficking Statement," *Mastercard*, 2021, online https://www.mastercard.us/en-us/vision/who-we-are/careers/mastercard-modern-slavery-and-human-trafficking-statement.html (retrieved on July 8, 2022).

G. Others

CONSEIL FEDERAL, *Prostitution et traite d'êtres humains à des fins d'exploitation sexuelle Rapport*, Switzerland, June 5, 2015.

ORFANA I., *Guidelines for development of a transnational referral mechanism for trafficked persons in Europe: TRM-EU*, Department of Equal Opportunities, Presidency of the Council of Ministers, Italy, ICMPD, 2010.

II. Supranational grey literature

A. Council of Europe

AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE, "Feasibility Study," December 17, 2020, CAHAI(2020)23.

CAPLAN A. et al., *Trafficking in organs, tissues and cells and trafficking in human beings for the purpose of the removal of organs*, Council of Europe and UN, 2009.

COMMITTEE OF EXPERTS ON INTERNET INTERMEDIARIES, "Algorithms and human rights Study on the human rights dimensions of automated data processing techniques and possible regulatory implications," 2017.

COMMITTEE OF MINISTERS, "Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society," May 13, 2005, CM(2005)56 final.

COMMITTEE OF MINISTERS, "Recommendation No. R (87) 15 regulating the use of personal data in the police sector," September 17, 1987.

COMMITTEE OF MINISTERS, "Recommendation No. R (88) 18 Concerning Liability of Enterprises Having Legal Personality for Offences Committed in the Exercise of their Activities," October 20, 1988.

COMMITTEE OF MINISTERS, "Recommendation no. R (91)11 concerning sexual exploitation, pornography and prostitution of, and trafficking in, children and young adults," September 9, 1991.

COMMITTEE OF MINISTERS, "Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology," September 11, 1995.

COMMITTEE OF MINISTERS, "Recommendation No. R (97) 20 to member states on 'hate speech,'" October 30, 1997.

COMMITTEE OF MINISTERS, "Recommendation No. R (2000) 11 to member states on action against trafficking in human beings for the purpose of sexual exploitation," May 19, 2000.

COMMITTEE OF MINISTERS, "Recommendation Rec(2001)11 concerning guiding principles on the fight against organised crime," September 19, 2001.

COMMITTEE OF MINISTERS, "Recommendation Rec(2005)10 on 'special investigation techniques' in relation to serious crimes including acts of terrorism," April 20, 2005.

COMMITTEE OF MINISTERS, "Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems," April 8, 2020.

COMMITTEE OF MINISTERS, "Recommendation CM/Rec(2022)21 to member States on preventing and combating trafficking in human beings for the purpose of labour exploitation," September 27, 2022.

COUNCIL OF EUROPE, "Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters," April 20, 1959.

COUNCIL OF EUROPE, "Explanatory Report to the Council of Europe Convention on Cybercrime," 2001.

COUNCIL OF EUROPE, "Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques : Vers un protocole à la Convention de Budapest," September 5, 2019.

CYBERCRIME CONVENTION COMMITTEE, "Transborder access to data and jurisdiction: Options for further action by the T-CY," Conseil de l'Europe, December 3, 2014, T-CY (2014)16.

CYBERCRIME CONVENTION COMMITTEE, "T-CY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention)," March 1, 2017, T-CY(2015)16.

CYBERCRIME CONVENTION COMMITTEE, "Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime Workplan and working methods," November 29, 2017, T-CY (2017)20.

CYBERCRIME CONVENTION COMMITTEE, "The Budapest Convention on Cybercrime: benefits and impact in practice," July 13, 2020, T-CY (2020)16.

CYBERCRIME CONVENTION COMMITTEE, “Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Draft Protocol version 3,” May 28, 2021.

CYBERCRIME CONVENTION COMMITTEE, “Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence,” 2021.

CYBERCRIME CONVENTION COMMITTEE, “Assessment Report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime,” January 25, 2013, T-CY (2012)10 REV.

CYBERCRIME CONVENTION COMMITTEE, “T-CY Guidance Note #13 The scope of procedural powers and of international co-operation provisions of the Budapest Convention,” Council of Europe, June 27, 2023, T-CY(2023)6.

CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE, “Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines Revised study and guidelines,” 2020.

CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE, “Data retention in the States Parties to the Budapest Convention on Cybercrime Survey report 2020,” 2020.

CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE, CYBERCRIME@EAP III PROJECT, “Study on Strategy of Cooperation with Multinational Service Providers,” August 30, 2017, 2016/DGI/JP/3608.

ECONOMIC CRIME DIVISION, DIRECTORATE GENERAL OF HUMAN RIGHTS AND LEGAL AFFAIRS, “Guidelines for the cooperation between law enforcement and internet service providers against cybercrime,” April 2, 2008.

EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE, “European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment,” December 4, 2018.

GRETA, “8th general report on GRETA’s activities covering the period from 1 January to 31 December 2018,” 2019.

GRETA, “9th general report on GRETA’s activities covering the period from 1 January to 31 December 2019,” 2020.

GRETA, “11th general report on GRETA’s activities covering the period from 1 January to 31 December 2021,” 2022.

GRETA, “Evaluation Report - France - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings,” February 18, 2022.

GRETA, “Evaluation Report - Spain - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings,” June 12, 2023.

GRETA, “Evaluation Report - Romania - Third evaluation round - Access to justice and effective remedies for victims of trafficking in human beings,” June 3, 2021.

GRETA, “Guidance note on preventing and combatting trafficking in human beings for the purpose of labour exploitation,” December 2020, GRETA(2020)12.

GRETA, “Human trafficking for the purpose of labour explotation - Thematic Chapter of the 7th General Report on GRETA’s Activities (covering the period from 1 January to 31 December 2017),” October 2019.

GRETA, “Online and technology-facilitated trafficking in human beings. Full report,” March 2022.

GRETA, “Online and technology-facilitated trafficking in human beings. Summary and recommendations,”March 2022.

GRETA, “Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties. Fourth evaluation round. Thematic focus: Addressing vulnerabilities to trafficking in human beings,” June 30, 2023.

GRETA, “Questionnaire for the evaluation of the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the Parties. Third evaluation round. Thematic focus: Access to justice and effective remedies for victims of trafficking in human beings,” 2018.

GRETA, “Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by France - Second evaluation round,” 2017.

GRETA, “Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Spain - Second evaluation round,” 2018.

GRETA, “Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Romania - Second evaluation round,” 2016.

GRETA, “Table ronde sur la traite des êtres humains à l’ère du numérique,” *Coe.int*, December 18, 2019, online https://www.coe.int/fr/web/anti-human-trafficking/news/-/asset_publisher/fX6ZWufj34JY/content/round-table-on-action-against-trafficking-in-human-beings-in-the-digital-age (retrieved on September 20, 2021).

GROUP OF EXPERTS ON ACTION AGAINST VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE, “General Recommendation No. 1 on the digital dimension of violence against women,” October 20, 2021.

GROUP OF SPECIALISTS ON THE IMPACT OF THE USE OF NEW INFORMATION TECHNOLOGIES ON TRAFFICKING IN HUMAN BEINGS FOR THE PURPOSE OF SEXUAL EXPLOITATION, “Final Report,” Committee for Equality between Women and Men, September 16, 2003, EG-S-NT (2002) 9 rev.

HUGHES D., GROUP OF SPECIALISTS ON THE IMPACT OF THE USE OF NEW INFORMATION TECHNOLOGIES ON TRAFFICKING IN HUMAN BEINGS FOR THE PURPOSE OF SEXUAL EXPLOITATION, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation A Study of the Users*, Committee for Equality between Women and Men, May 2001.

HUGHES D., GROUP OF SPECIALISTS ON THE IMPACT OF THE USE OF NEW INFORMATION TECHNOLOGIES ON TRAFFICKING IN HUMAN BEINGS FOR THE PURPOSE OF SEXUAL EXPLOITATION, *The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation. Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation*, Committee for Equality between Women and Men, November 2001.

KUBÍČEK M., COMMITTEE OF EXPERTS ON THE OPERATION OF EUROPEAN CONVENTIONS ON CO-OPERATION IN CRIMINAL MATTERS, EUROPEAN COMMITTEE ON CRIME PROBLEMS, “Consolidated document reflecting the applicable provisions of the European Convention on Mutual Assistance in Criminal Matters and its two Additional Protocols,” November 4, 2011, PC-OC (2011) 15 Rev.

MONEYVAL, *Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction*, Research Report, March 2012.

MONEYVAL, *Typologies report on laundering the proceeds of organised crime*, April 17, 2015.

PARLIAMENTARY ASSEMBLY, “Recommendation 1325 (1997) Traffic in women and forced prostitution in Council of Europe member states,” April 23, 1997.

PARLIAMENTARY ASSEMBLY, “Recommendation 1545 (2002) Campaign against trafficking in women,” January 21, 2002.

PARLIAMENTARY ASSEMBLY, “Recommendation 1663 (2004) Domestic slavery: servitude, au pairs and mail-order brides,” June 22, 2004.

SYKIOTOU A., *Trafficking in human beings: Internet recruitment - Misuse of the Internet for the recruitment of victims of trafficking in human beings*, 2007.

ZUIDERVEEN BORGESIUS F., “Discrimination, Artificial Intelligence and Algorithmic Decision-Making,” 2018.

B. European Union

ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 4/2007 on the concept of personal data,” June 20, 2007.

ARTICLE 29 DATA PROTECTION WORKING PARTY, “Opinion 1/2008 on data protection issues related to search engines,” European advisory body on data protection and privacy, April 4, 2008, 00737/EN WP 148.

DIRECTORATE GENERAL FOR MIGRATION AND HOME AFFAIRS, *Study on reviewing the functioning of Member States’ National and Transnational Referral Mechanisms*, European Commission, 2020.

COUNCIL OF THE EU, “Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence,” *Council of the EU*, January 25, 2023, online https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/ (retrieved on April 21, 2023).

COUNCIL OF THE EU, “Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace,” December 2, 2016.

COUNCIL OF THE EU, “Resolution on Encryption - Security through encryption and security despite encryption,” November 24, 2020, 13084/1/20 REV 1.

EU ANTI-TRAFFICKING COORDINATOR, “Common Anti-Trafficking Plan to address the risks of trafficking in human beings and support potential victims among those fleeing the war in Ukraine,” 2022.

EU COUNCIL, “Council conclusions on improving criminal justice in cyberspace,” June 9, 2016.

EUROJUST, “Strategic project on Eurojust’s action against trafficking in human beings Final report and action plan,” October 2012.

EUROJUST, “Report on Eurojust’s casework in the field of the European Investigation Order,” November 2020.

EUROJUST, “Report on Trafficking in Human Beings Best practice and issues in judicial cooperation,” February 2021.

EUROJUST, “Annual report 2020 - Criminal justice across borders,” 2021.

EUROJUST, EUROPOL, “Communiqué de presse - Le démantèlement d’un réseau crypté crée une onde de choc au sein des groupes criminels organisés à travers l’Europe,” June 2, 2020.

EUROPEAN COMMISSION, “Commission Staff working document - Impact assessment report accompanying the document Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse,” May 11, 2022, SWD(2022) 209 final.

EUROPEAN COMMISSION, “Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal

matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings," April 17, 2018, SWD(2018) 118 final.

EUROPEAN COMMISSION, "Commission Staff Working Document Statistics and trends in trafficking in human being in the European Union in 2019-2020 Accompanying the document Report on the progress made in the fight against trafficking in human beings (Fourth Report)," December 19, 2022, SWD(2022) 429 final.

EUROPEAN COMMISSION, "Communication Guidelines on non-financial reporting (methodology for reporting non-financial information)," July 5, 2017, (2017/C 215/01).

EUROPEAN COMMISSION, "Communication to the Council and the European Parliament on trafficking in women for the purpose of sexual exploitation," November 20, 1996.

EUROPEAN COMMISSION, "Communication to the Council and the European Parliament - For further actions in the fight against trafficking in women," December 9, 1998.

EUROPEAN COMMISSION, "Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime," January 26, 2001.

EUROPEAN COMMISSION, "Communication to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Illegal and Harmful Content on the Internet," October 16, 1996, COM(96)487 final.

EUROPEAN COMMISSION, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025," April 14, 2021, COM(2021) 171 final.

EUROPEAN COMMISSION, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - 2030 Digital Compass: the European way for the Digital Decade," September 3, 2021.

EUROPEAN COMMISSION, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital future," February 19, 2020.

EUROPEAN COMMISSION, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025," April 14, 2021, COM(2021) 170 final.

EUROPEAN COMMISSION, "Communication to the European Parliament and the Council - Fighting trafficking in human beings : an integrated approach and proposals for an action plan," October 18, 2005.

EUROPEAN COMMISSION, "Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016," June 19, 2012, COM/2012/0286 final.

EUROPEAN COMMISSION, "Communication To The European Parliament, The European Council And The Council - Eleventh progress report towards an effective and genuine Security Union," October 18, 2017, COM(2017) 608 final.

EUROPEAN COMMISSION, "Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on victims' rights (2020-2025)," June 24, 2020, COM(2020) 258 final.

EUROPEAN COMMISSION, *Data collection on trafficking in human beings in the EU*, 2018.

EUROPEAN COMMISSION, *Data collection on trafficking in human beings in the EU*, Publications Office of the EU, 2020.

EUROPEAN COMMISSION, “DSA: Very Large Online Platforms and Search Engines,” *European Commission*, April 25, 2023, online https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413 (retrieved on May 12, 2023).

EUROPEAN COMMISSION, “Fourth report on the progress made in the fight against trafficking in human beings,” December 19, 2022, COM(2022) 736 final.

EUROPEAN COMMISSION, “Questions and Answers: Mandate for the EU-U.S. cooperation on electronic evidence,” February 5, 2019.

EUROPEAN COMMISSION, “Recommendation concerning the definition of micro, small and medium-sized enterprises,” May 6, 2003.

EUROPEAN COMMISSION, “Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters,” February 5, 2019, COM(2019) 70 final.

EUROPEAN COMMISSION, “Report on the progress made in the fight against trafficking in human beings as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims,” May 19, 2016, COM(2016) 267 final.

EUROPEAN COMMISSION, “Report on the review clauses in Directives 2013/34/EU, 2014/95/EU, and 2013/50/EU,” April 21, 2021, COM(2021) 199 final.

EUROPEAN COMMISSION, “Security Union facilitating Access to Electronic Evidence,” April 2018.

EUROPEAN COMMISSION, *Study on the gender dimension of trafficking in human beings: executive summary*, 2016.

EUROPEAN DATA PROTECTION SUPERVISOR, “Opinion 1/2021 on the Proposal for a Digital Services Act,” February 10, 2021.

EUROPEAN DATA PROTECTION SUPERVISOR, EUROPEAN DATA PROTECTION BOARD, “Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence,” July 10, 2019.

EUROPEAN INSTITUTE FOR GENDER EQUALITY, “Gender-specific measures in anti-trafficking actions Report,” 2018.

EUROPEAN PARLIAMENT, “Resolution on equality between women and men in the European Union in 2018-2020,” December 15, 2021, 2021/2020(INI).

EUROPEAN PARLIAMENT, “Resolution on the exploitation of prostitution and the traffic in human beings,” April 14, 1989, OJ No C 120/2, p.352.

EUROPEAN PARLIAMENT, “Resolution on the EU Gender Action Plan III,” March 10, 2022, 2021/2003(INI).

EUROPEAN PARLIAMENT, “Resolution on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims,” February 10, 2021, 2020/2029(INI).

EUROPEAN PARLIAMENT, “Resolution on sexual exploitation and prostitution and its impact on gender equality,” February 26, 2014, 2013/2103(INI).

EUROPEAN PARLIAMENT, “Resolution on trade in women,” September 16, 1993, OJ No C 268, p.141.

EUROPEAN PARLIAMENT, “Resolution on trafficking in human beings,” February 5, 1996, OJ No C 120/2, p.352.

EUROPEAN PARLIAMENT, “Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence,” October 20, 2020, P9_TA(2020)0276.

EUROPEAN PARLIAMENT, “Resolution with recommendations to the Commission on combating gender-based violence: cyberviolence,” December 14, 2021, 2020/2035(INL).

EUROPEAN PARLIAMENT, “Resolution with recommendations to the Commission on corporate due diligence and corporate accountability,” March 10, 2021, P9_TA(2021)0073.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, “Protecting migrant workers from exploitation in the EU: workers’ perspectives,” 2019.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS., “Data quality and artificial intelligence: mitigating bias and error to protect fundamental rights.,” Publications Office, 2019, online https://data.europa.eu/doi/10.2811/546219 (retrieved on June 8, 2021).

EUROPOL, “European Union serious and organised crime threat assessment - Crime in the age of technology,” 2017.

EUROPOL, “European Union serious and organised crime threat assessment - A corrupting influence,” 2021.

EUROPOL, “Human traffickers luring Ukrainian refugees on the web targeted in EU-wide hackathon,” *Europol*, June 23, 2022, online https://www.europol.europa.eu/media-press/newsroom/news/human-traffickers-luring-ukrainian-refugees-web-targeted-in-eu-wide-hackathon (retrieved on July 11, 2022).

EUROPOL, “Intelligence Notification 15/2014 Trafficking in human beings and the internet,” October 2014.

EUROPOL, “Internet organised crime threat assessment,” 2018.

EUROPOL, “Internet organised crime threat assessment,” 2019.

EUROPOL, “Internet organised crime threat assessment,” 2020.

EUROPOL, “Internet organised crime threat assessment,” 2021.

EUROPOL, “The challenges of countering human trafficking in the digital era,” October 2020.

EUROPOL, “The THB financial business model - Assessing the Current State of Knowledge,” Europol public information, July 2015.

EUROPOL, EUROJUST, “Common challenges in combating cybercrime,” June 2019.

EUROPOL, EUROJUST, “Second report of the observatory function on encryption - Joint report,” 2020.

SIRIUS, “EU Digital Evidence Situation 2nd Annual Report,” 2020.

SPOTLIGHT INITIATIVE, “Mobile women and mobile phones Women migrant workers’ use of information and communication technologies in ASEAN,” EU and ILO, 2019.

TAMPERE EUROPEAN COUNCIL, “Tampere European Council of 15 and 16.10.1999 - Conclusions of the Presidency,” October 1999.

C. International Labor Organization

8.7 ALLIANCE, “Global Estimates of Modern Slavery - Forced labour and forced marriage,” 2017.

GOVERNANCE AND TRIPARTISM DEPARTMENT, *Achieving decent work in global supply chains*, Report for discussion at the technical meeting on achieving decent work in global supply chains (Geneva, 25–28 February 2020), 2020.

ILO, *Decent work in global supply chains*, IV, Geneva, International Labour Conference 105th Session, 2016, ILC.105/IV.

ILO, “Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy,” UN, March 2017.

ILO (ed.), *The cost of coercion: global report under the follow-up to the ILO Declaration on Fundamental Principles and Rights at Work ; International Labour Conference, 98th Session*, International Labour Office Geneva, Report / International Labour Conference no. 98,1,B, 2009.

ILO et al., *Ending child labour, forced labour and human trafficking in global supply chains*, 8.7 Alliance, 2019.

MALPANI R., *Legal Aspects of Trafficking for Forced Labour Purposes in Europe*, International Labour Office, 2006.

PHILLIPS N., LEBARON G., WALLIN S., *Mapping and Measuring the Effectiveness of Labour-related Disclosure Requirements for Global Supply Chains*, Research Department Working Paper, no. 32, International Labour Office, June 2018.

D. Organisation for Economic Co-operation and Development

OECD, *Guidelines for multinational enterprises*, 2011.

OECD, “Mise en oeuvre de la Convention de l’OCDE sur la lutte contre la corruption Rapport de Phase 4 France,” 2021.

OECD, “Recommendation of the Council concerning Guidelines for Cryptography Policy,”2020, OECD/LEGAL/0289.

OECD, “The economic and social role of Internet intermediaries,” 2010.

E. Organization for Security and Co-operation in Europe

ARONOWITZ A., THEUERMANN G., TYURYKANOVA E., *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime*, May 2010.

OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS, *National referral mechanisms - Joining efforts to protect the rights of trafficked persons - A practical handbook*, 2nd ed., 2022.

OFFICE OF THE SPECIAL REPRESENTATIVE AND COORDINATOR FOR COMBATING TRAFFICKING IN HUMAN BEINGS, *Applying gender-sensitive approaches in combating trafficking in human beings*, Occasional paper, no. 10, 2021.

OFFICE OF THE SPECIAL REPRESENTATIVE AND COORDINATOR FOR COMBATING TRAFFICKING IN HUMAN BEINGS, TECH AGAINST TRAFFICKING, *Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools*, May 2020.

OFFICE OF THE SPECIAL REPRESENTATIVE AND COORDINATOR FOR COMBATING TRAFFICKING IN HUMAN BEINGS, *Trafficking in Human Beings and Terrorism: Where and How They Intersect - Analysis and recommendations for more effective policy responses*, 2021.

OSCE, “Decision No. 557: OSCE Action Plan to Combat Trafficking in Human Beings,” July 24, 2003, PC.DEC/557.

OSCE, “Decision No. 557/Rev.1: OSCE Action Plan to Combat Trafficking in Human Beings,” July 7, 2005, PC.DEC/1107/Corr.1.

OSCE, “Decision nº 1107 Addendum to the OSCE Action plan to combat trafficking in human beings: one decade later,” December 6, 2013, PC.DEC/1107/Corr.1.

OSCE, “Leveraging Anti-Money Laundering Regimes to Combat Trafficking in Human Beings,” 2014.

F. Interntional Organization for Migration

BAULOZ C., MCADAM M., TEYE J., "Human trafficking in migration pathways: Trends, challenges and new forms of cooperation," *in* INTERNATIONAL ORGANIZATION FOR MIGRATION (ed.), *World Migration Report 2022*, May 21, 2020, p. 255.

BEDUSCHI A., MCAULIFFE M., "Artificial intelligence, migration and mobility: Implications for policy and practice," *in* INTERNATIONAL ORGANIZATION FOR MIGRATION (ed.), *World Migration Report 2022*, May 21, 2020, p. 281.

DAVID F., BRYANT K., LARSEN J.J., "Migrants and their vulnerability to human trafficking, modern slavery and forced labour," 2019.

G. United Nations

COMMISSION ON CRIME PREVENTION AND CRIMINAL JUSTICE, "Resolution 27/2 Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies," Economic and Social Council, 2018.

COMMISSION ON HUMAN RIGHTS, "Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights," Economic and Social Council, August 26, 2003, E/CN.4/Sub.2/2003/12/Rev.2.

CONFERENCE OF THE PARTIES TO THE UN CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME, "Resolution 5/2 Implementation of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime," 2010.

COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE, "Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing," Security Council, 2019.

DEPUTY SECRETARY-GENERAL, "Add 'partnership' to 'three P' agenda of United Nations anti-trafficking protocol, deputy secretary-general urges General Assembly thematic debate," Press Release, June 3, 2008, DSG/SM/397-GA/10713-HR/4956.

GENERAL ASSEMBLY, "Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power," November 29, 1985, A/RES/40/34.

GENERAL ASSEMBLY, "Resolution 58/137. Strengthening international cooperation in preventing and combating trafficking in persons and protecting victims of such trafficking," February 4, 2004.

GENERAL ASSEMBLY, "Resolution 61/180. Improving the coordination of efforts against trafficking in persons," December 20, 2006.

GENERAL ASSEMBLY, "Resolution 63/194. Improving the coordination of efforts against trafficking in persons," December 18, 2008.

GENERAL ASSEMBLY, "Resolution 64/293. United Nations Global Plan of Action to Combat Trafficking in Persons," UN, July 30, 2010, A/RES/64/293.

GENERAL ASSEMBLY, "Resolution 67/190. Improving the coordination of efforts against trafficking in persons," December 20, 2012.

GENERAL ASSEMBLY, "Resolution 70/1 Transforming our world: the 2030 Agenda for Sustainable Development," September 25, 2015, A/RES/70/1.

GENERAL ASSEMBLY, "Resolution 72/1. Political declaration on the implementation of the United Nations Global Plan of Action to Combat Trafficking in Persons," September 27, 2017, A/RES/72/1.

GENERAL ASSEMBLY, "Resolution 72/195. Improving the coordination of efforts against trafficking in persons," December 19, 2017.

HUMAN RIGHTS COUNCIL, "Resolution 20/8. The promotion, protection and enjoyment of human rights on the Internet," July 16, 2012, A/HRC/RES/20/8.

HUMAN RIGHTS COUNCIL, "Resolution 26/13. The promotion, protection and enjoyment of human rights on the Internet," July 14, 2014, A/HRC/RES/26/13.

INTER-AGENCY COORDINATION GROUP AGAINST TRAFFICKING IN PERSONS, *Human trafficking and technology: trends, challenges and opportunities*, Issue Brief, no. 7, 2019.

OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, "Recommended Principles and Guidelines on Human Rights and Human Trafficking," 2010.

SECRETARIAT OF THE WORKING GROUP ON TRAFFICKING IN PERSONS, *Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons Background paper*, Conference of the Parties to the United Nations Convention against Transnational Organized Crime, July 23, 2021, CTOC/COP/WG.4/2021/2.

SECRETARY-GENERAL, "Report. Improving the coordination of efforts against trafficking in persons," Crime prevention and criminal justice, June 28, 2021, A/76/120.

SECRETARY-GENERAL, "Extreme poverty and human rights Note," General Assembly, July 19, 2021, A/76/177.

SECURITY COUNCIL, "Resolution 2331 (2016)," UN, December 20, 2016, S/RES/2331 (2016).

SPECIAL RAPPORTEUR ON CONTEMPORARY FORMS OF SLAVERY, INCLUDING ITS CAUSES AND CONSEQUENCES, "Current and emerging forms of slavery - Report," Human Rights Council, General Assembly, July 25, 2019, A/HRC/42/44.

SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, "Report," Human Rights Council, General Assembly, May 16, 2011, A/HRC/17/27.

SPECIAL RAPPORTEUR ON THE SALE OF CHILDREN, CHILD PROSTITUTION AND CHILD PORNOGRAPHY, "Report on the sale of children, child prostitution and child pornography," Commission on Human Rights, Economic and Social Council, December 23, 2004, E/CN.4/2005/78.

SPECIAL RAPPORTEUR ON THE SALE OF CHILDREN, CHILD PROSTITUTION AND CHILD PORNOGRAPHY, "Report," Human Rights Council, General Assembly, December 22, 2014, A/HRC/28/56.

SPECIAL RAPPORTEUR ON TRAFFICKING IN PERSONS, ESPECIALLY WOMEN AND CHILDREN, "Report," General Assembly, August 7, 2012, A/67/261.

SPECIAL RAPPORTEUR ON TRAFFICKING IN PERSONS, ESPECIALLY WOMEN AND CHILDREN, "Report - Trafficking in persons in the agriculture sector: human rights due diligence and sustainable development," General Assembly, April 25, 2022, A/HRC/50/33.

SPECIAL RAPPORTEUR ON TRAFFICKING IN PERSONS, ESPECIALLY WOMEN AND CHILDREN, "Report - Addressing the gender dimensions of trafficking in persons in the context of climate change, displacement and disaster risk reduction," General Assembly, July 15, 2022, A/77/170.

SPECIAL REPRESENTATIVE OF THE SECRETARY GENERAL ON THE ISSUE OF HUMAN RIGHTS AND TRANSNATIONAL CORPORATIONS AND OTHER BUSINESS ENTERPRISES, "Report - Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," Human Rights Council, 2011, A/HRC/17/31.

UNITED NATIONS, "World Day Against Trafficking in Persons," *United Nations*, no date, online https://www.un.org/en/observances/end-human-trafficking-day (retrieved on August 23, 2022).

H. United Nations Office on Drugs and Crime

EXPERT GROUP TO CONDUCT A COMPREHENSIVE STUDY ON CYBERCRIME, "Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector Executive summary," January 23, 2013, UNODC/CCPCJ/EG.4/2013/2.

GLOBAL PROGRAMME AGAINST TRAFFICKING IN HUMAN BEINGS, "Toolkit to Combat Trafficking in Persons," 2008.

JANDL M., "Investigaciones sobre la trata de personas: lagunas y limitaciones de los datos en los ámbitos del delito y la justicia penal," *in* CHAWLA S. (ed.), *Foro sobre el delito y la sociedad. Número especial Reunión de datos sobre la delincuencia: indicadores y cuantificadores*, 2008, vol. 7, p. 33.

UN.GIFT, "Background Paper 017 Workshop : Technology and Human Trafficking," Austria Center Vienna, February 2008.

UNODC, "Human trafficking indicators," 2020, online https://www.unodc.org/pdf/HT_indicators_E_LOWRES.pdf (retrieved on October 10, 2021).

UNODC, *Compendium on promising practices on Public-Private Partnerships to prevent and counter trafficking in persons*, 2021.

UNODC, *Global report on trafficking in persons 2020*, January 2021.

UNODC, *Global report on trafficking in persons 2022*, January 2023.

UNODC, *Comprehensive Study on Cybercrime*, February 2013.

UNODC, *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*, October 2011.

UNODC, *Organized crime involvement in trafficking in persons and smuggling of migrants*, Issue Paper, 2010.

UNODC, *Report Informal Expert Working Group on Mutual Legal Assistance Casework Best Practice*, 2001.

UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, May 2015.

UNODC, *The effects of the COVID-19 pandemic on trafficking in persons and responses to the challenges - A global study of emerging evidence*, 2021.

I. Others

BARTLETT B.L., *The negative effects of money laundering on economic development*, Regional Technical Assistance Project No.5967, The Asian Development Bank, May 2002, online https://search.informit.org/doi/abs/10.3316/agispt.20030578 (retrieved on September 2, 2021).

CHAMBRE DE COMMERCE INTERNATIONALE, "Code ICC consolidé sur les pratiques de publicité et de communication commerciale," 2011.

FINANCIAL ACTION TASK FORCE, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - 2012 Recommendations," 2022.

FINANCIAL ACTION TASK FORCE, "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants," July 2011.

FINANCIAL ACTION TASK FORCE, ASIA/PACIFIC GROUP ON MONEY LAUNDERING, "Financial Flows from Human Trafficking," July 2018.

INTERNATIONAL COUNCIL ON HUMAN RIGHTS POLICY (ed.), *Beyond voluntarism: human rights and the developing international legal obligations of companies*, International Council on Human Rights Policy, 2002.

INTERNATIONAL TRADE UNION CONFEDERATION, ANTI SLAVERY, CHURCHES' COMMISSION FOR MIGRANTS IN EUROPE, *The role of the Internet in trafficking for labour exploitation*, Project FINE TUNE, Co-financed by EU Prevention of and Fight against Crime Program, 2011.

§9. Press news

AFP, "Démantèlement d'un réseau de prostitution qui exploitait des femmes dans le Nord et le Vaucluse," *La Dépêche*, June 1, 2021, online https://www.ladepeche.fr/2021/06/01/demantelement-dun-reseau-de-prostitution-qui-exploitait-des-femmes-dans-le-nord-et-le-vaucluse-9579683.php (retrieved on June 17, 2021).

AFP, "Le site de petites annonces Wannonce visé par une plainte pour proxénétisme aggravé," *LExpress.fr*, January 27, 2022, online https://www.lexpress.fr/actualites/1/societe/le-site-de-petites-annonces-wannonce-vise-par-une-plainte-pour-proxenetisme-aggrave_2166957.html (retrieved on February 4, 2022).

AFP, "Nancy : trois clans de Roms jugés pour «vols» et «traite d'êtres humains»," *Le Figaro.fr*, November 16, 2020, online https://www.lefigaro.fr/flash-actu/nancy-trois-clans-de-roms-juges-pour-vols-et-traite-d-etres-humains-20201116 (retrieved on November 19, 2020).

ALBERTINI A., "Un vaste réseau de prostitution démantelé à Paris," *Le Monde.fr*, June 10, 2021, online https://www.lemonde.fr/police-justice/article/2021/06/10/un-vaste-reseau-de-prostitution-demantele-a-paris_6083529_1653578.html (retrieved on June 17, 2021).

ALVAREZ J., "Detenido por trata de personas el polémico 'streamer' que intentó vacilar a Greta Thunberg," *ElHuffPost*, December 30, 2022, online https://www.huffingtonpost.es/entry/andrew-tate-detenido-rumania-streamer-intento-vacilar-greta-thunberg-detenido-rumania-por-trata-de-personas_es_63ae2335e4b0d6f0b9f28625 (retrieved on January 2, 2023).

BERTUZZI L., "EU Council nears common position on AI Act in semi-final text," *Euractiv*, October 19, 2022, online https://www.euractiv.com/section/digital/news/eu-council-nears-common-position-on-ai-act-in-semi-final-text/ (retrieved on October 25, 2022).

BRULL I ORTEGA S., "El Parlament pide no criminalizar a quienes ejercen la prostitución 'libre y voluntariamente,'" *ElNacional.cat*, July 7, 2022, online https://www.elnacional.cat/es/politica/parlament-pide-no-criminalizar-ejercen-prostitucion-libre-voluntariamente_784329_102.html (retrieved on September 20, 2022).

BUCHANAN M., SWANN S., "Comment le téléphone d'un adolescent a permis de démanteler un réseau de trafic d'êtres humains," *BBC News Afrique*, February 4, 2023, online https://www.bbc.com/afrique/64484326 (retrieved on February 20, 2023).

BURKE M., "Amazon's Alexa may have witnessed alleged Florida murder, authorities say," *NBC News*, November 2, 2019, online https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 (retrieved on October 12, 2022).

COLCOMBET L., "Proxénétisme en ligne : rencontre avec les limiers de la PJ qui luttent contre cette menace « gigantesque »," *Leparisien.fr*, July 31, 2022, online https://www.leparisien.fr/faits-divers/proxenetisme-en-ligne-rencontre-avec-les-limiers-de-la-pj-qui-luttent-contre-cette-menace-gigantesque-31-07-2022-HECM4QK5LFDQBA64MDJDDMP2DQ.php (retrieved on August 2, 2022).

COOK J., “Instagram’s Shadow Ban On Vaguely ‘Inappropriate’ Content Is Plainly Sexist,” *HuffPost*, April 29, 2019, online https://www.huffpost.com/entry/instagram-shadow-ban-sexist_n_5cc72935e4b0537911491a4f (retrieved on March 6, 2021).

D’ANGELO R., “Une enquête pour traite des êtres humains expose les pratiques de l’industrie du porno,” *Mediapart.fr*, November 23, 2020.

DE FOUCHER L., CHAPUIS N., LAURENT S., “« C’était des viols déguisés en vidéo » : le réseau, le recruteur et les proies,” *Le Monde.fr*, December 15, 2021, online https://www.lemonde.fr/police-justice/article/2021/12/15/c-etait-des-viols-deguises-en-video-le-reseau-le-recruteur-et-les-proies_6106152_1653578.html (retrieved on December 15, 2021).

DUFFY C., “Facebook has known it has a human trafficking problem for years. It still hasn’t fully fixed it,” *CNN*, October 25, 2021, online https://www.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking/index.html (retrieved on November 7, 2021).

ETX DAILY UP, “Google bannit les applications de type 'Sugar Daddy' dans une nouvelle mise à jour,” *Ladepeche.fr*, July 30, 2021, online https://www.ladepeche.fr/2021/07/30/google-bannit-les-applications-de-type-sugar-daddy-dans-une-nouvelle-mise-a-jour-9704136.php (retrieved on August 7, 2021).

FOLLOROU J., “Piratage d’EncroChat : les recours se multiplient contre la justice française,” *Le Monde.fr*, March 10, 2021, online https://www.lemonde.fr/societe/article/2021/03/10/piratage-d-encrochat-les-recours-se-multiplient-contre-la-justice-francaise_6072569_3224.html (retrieved on April 29, 2021).

GONZALES P., “Un risque de pénurie pèse sur les bracelets électroniques,” *Le Figaro*, March 10, 2021, online https://www.lefigaro.fr/actualite-france/un-risque-de-penurie-pese-sur-les-bracelets-electroniques-20210310 (retrieved on October 28, 2021).

GRIESSEL A., “France, Colombie, Espagne : un réseau international de proxénétisme démantelé,” *France Inter*, December 2, 2022, online https://www.radiofrance.fr/franceinter/france-colombie-espagne-un-reseau-international-de-proxenetisme-demantele-8069358 (retrieved on December 2, 2022).

INFOBAE, “Trata de personas: un estudio de modelos webcam se convirtió en un infierno para jóvenes de la comunidad LGBT+ en Barranquilla,” *Infobae*, November 23, 2022, online https://www.infobae.com/america/colombia/2022/11/23/trata-de-personas-un-estudio-de-modelos-webcam-se-convirtio-en-un-infierno-para-jovenes-de-la-comunidad-lgbt-en-barranquilla/ (retrieved on January 2, 2023).

KESSLER G., “Has the sex-trafficking law eliminated 90 percent of sex-trafficking ads? - The Washington Post,” *Washington Post*, August 20, 2018, online https://www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/ (retrieved on March 18, 2021).

LA PRESSE CANADIENNE, “Mindgeek, société mère de Pornhub, visée par une poursuite aux États-Unis,” *Radio-Canada.ca*, Radio-Canada.ca, June 18, 2021, online https://ici.radio-canada.ca/nouvelle/1802513/sites-porno-consentement-exploitation-sexuelle-feras-antoon-mindgeek (retrieved on June 24, 2021).

LA VANGUARDIA, “El Parlament rechaza la criminalización del trabajo sexual voluntario,” *La Vanguardia*, July 7, 2022, online https://www.lavanguardia.com/politica/20220707/8392910/parlament-rechaza-criminalizacion-trabajo-sexual-voluntario.html (retrieved on September 20, 2022).

LE CREURER O., “Prostitution : un réseau international démantelé depuis Montpellier,” *France 3 Occitanie*, March 4, 2021, online https://france3-regions.francetvinfo.fr/occitanie/herault/montpellier/prostitution-un-reseau-international-demantele-depuis-montpellier-1982317.html (retrieved on March 9, 2021).

LE FIGARO, AFP, “Un réseau international de traite des êtres humains démantelé dans le sud de l’Europe,” *Le Figaro.fr*, March 5, 2021, online https://www.lefigaro.fr/faits-divers/un-reseau-international-de-traite-des-etres-humains-demantele-dans-le-sud-de-l-europe-20210305 (retrieved on April 19, 2021).

LE MONDE, “Prostitution : Vivastreet suspend sa rubrique Rencontres,” *Le Monde.fr*, June 19, 2018, online https://www.lemonde.fr/societe/article/2018/06/19/prostitution-vivastreet-suspend-sa-rubrique-rencontres_5317513_3224.html (retrieved on May 18, 2022).

LELOUP D., REYNAUD F., “OnlyFans, Pornhub… Le monde bancaire régulateur de facto de l’industrie pornographique,” *Le Monde.fr*, August 24, 2021, online https://www.lemonde.fr/pixels/article/2021/08/24/onlyfans-pornhub-le-monde-bancaire-regule-de-facto-de-l-industrie-pornographique_6092199_4408996.html (retrieved on September 7, 2021).

MCCOMBS E., “'This Bill Is Killing Us': 9 Sex Workers On Their Lives In The Wake Of FOSTA,” *HuffPost*, May 11, 2018, online https://www.huffpost.com/entry/sex-workers-sesta-fosta_n_5ad0d7d0e4b0edca2cb964d9 (retrieved on March 20, 2021).

MOTET L., “Vivastreet : les dessous de la prostitution par petites annonces,” *Le Monde.fr*, February 2, 2017, online https://www.lemonde.fr/les-decodeurs/article/2017/02/02/vivastreet-les-dessous-de-la-prostitution-par-petites-annonces_5073149_4355770.html (retrieved on May 18, 2022).

PERRIGO B., “Meta Accused Of Human Trafficking and Union-Busting in Kenya,” *Time*, May 11, 2022, online https://time.com/6175026/facebook-sama-kenya-lawsuit/ (retrieved on May 19, 2022).

PINNELL O., KELLY J., “Slave markets found on Instagram and other apps,” *BBC News*, October 31, 2019, online https://www.bbc.com/news/technology-50228549 (retrieved on September 24, 2021).

STEADMAN O., “Porn Stars Vs. Instagram: Inside The Battle To Remain On The Platform,” *BuzzFeed News*, October 18, 2019, online https://www.buzzfeednews.com/article/otilliasteadman/porn-stars-instagram-account-takedowns-jessica-jaymes (retrieved on March 6, 2021).

TITHERADGE N., “OnlyFans: How it handles illegal sex videos - BBC investigation,” *BBC News*, August 19, 2021, online https://www.bbc.com/news/uk-58255865 (retrieved on September 17, 2021).

TONDO L., “Ukraine prosecutors uncover sex trafficking ring preying on women fleeing country,” *The Guardian*, July 7, 2022, online https://www.theguardian.com/global-development/2022/jul/07/ukraine-prosecutors-uncover-sex-trafficking-ring-preying-on-women-fleeing-country (retrieved on July 29, 2022).

UNTERSINGER M., “Justice : les enquêteurs pourront bientôt utiliser des logiciels espions,” *Le Monde.fr*, November 14, 2017, online https://www.lemonde.fr/pixels/article/2017/11/14/justice-les-enqueteurs-pourront-bientot-utiliser-des-logiciels-espions_5214397_4408996.html (retrieved on April 29, 2021).

WITT E., “After the Closure of Backpage, Increasingly Vulnerable Sex Workers Are Demanding Their Rights,” *The New Yorker*, June 8, 2018, online https://www.newyorker.com/news/dispatch/after-the-closure-of-backpage-increasingly-vulnerable-sex-workers-are-demanding-their-rights (retrieved on March 20, 2021).

§10. Websites

AIRBNB, “Airbnb soutient le travail du Gouvernement contre la prostitution,” *Airbnb Newsroom*, November 15, 2021, online https://news.airbnb.com/fr/airbnb-soutient-le-travail-du-gouvernement-contre-la-prostitution/ (retrieved on November 20, 2021).

BARNETT D., “2021 Year In Review: Sex Online,” *Electronic Frontier Foundation*, December 29, 2021, online https://www.eff.org/deeplinks/2021/12/year-review-sex-online (retrieved on January 6, 2022).

BENISTY M., “Après avoir fait son beurre sur le sexe, OnlyFans bannit les contenus explicites,” *Madmoizelle*, August 20, 2021, online https://www.madmoizelle.com/apres-avoir-fait-son-beurre-sur-le-sexe-onlyfans-bannit-les-contenus-explicites-1189063 (retrieved on August 20, 2021).

CHAPMAN A., “How Meta’s Failure to Act Upon Human Trafficking Claims Led to Another Lawsuit,” *Impakter*, March 28, 2023, online https://impakter.com/metas-failure-act-upon-human-trafficking-claims-lawsuit/ (retrieved on March 30, 2023).

COLE S., “Linktree Is Kicking Many Sex Workers Off Its Site,” *Vice*, January 14, 2022, online https://www.vice.com/en/article/jgmjpk/linktree-banned-removed-inappropriate-use-sex-work (retrieved on January 21, 2022).

DAIRE S., “Memex Helps Find Human Trafficking Cases Online,” *Human Trafficking Center*, May 13, 2015, online https://humantraffickingcenter.org/memex-helps-find-human-trafficking-cases-online/ (retrieved on January 13, 2021).

DELUZARCHE C., “Les emojis, nouveau langage codé du crime,” *Korii.*, November 11, 2020, online https://korii.slate.fr/et-caetera/emojis-emoticones-nouveau-langage-code-criminels-mafia-terroristes-messages (retrieved on November 17, 2020).

DJOUPA A., “Tribune contre la censure de l’éducation sexuelle sur Instagram,” *MadmoiZelle.com*, June 9, 2021, online https://www.madmoizelle.com/parler-deducation-sexuelle-sur-instagram-et-en-faire-son-metier-cest-vivre-avec-la-peur-au-ventre-1137662 (retrieved on June 10, 2021).

DORRIS J., “The Queer Past Gets Deleted on eBay,” *The New Yorker*, August 27, 2021, online https://www.newyorker.com/culture/cultural-comment/the-queer-past-gets-deleted-on-ebay (retrieved on September 9, 2021).

DRAUGHN M., “No Ground Truth: Sex Trafficking and Machine Learning,” *Windypundit*, July 27, 2022, online https://windypundit.com/2022/07/no-ground-truth-sex-trafficking-and-machine-learning/ (retrieved on August 23, 2022).

FACEBOOK, “Facebook Community Standards,” *Transparency Center*, 2022, online https://transparency.fb.com/policies/community-standards/ (retrieved on October 5, 2022).

FEINGOLD S., “Why the European Union is opening a Silicon Valley 'embassy,'” *World Economic Forum*, August 16, 2022, online https://www.weforum.org/agenda/2022/08/why-the-european-union-is-opening-a-silicon-valley-embassy/ (retrieved on August 23, 2022).

GARLAND E., “How FOSTA/SESTA Will Change the Future of Indie and Feminist Porn,” *Vice*, August 15, 2018, online https://www.vice.com/en/article/zmk89y/how-fostasesta-will-change-the-future-of-indie-and-feminist-porn (retrieved on May 15, 2021).

GREENEMEIER L., “Human Traffickers Caught on Hidden Internet,” *Scientific American*, February 8, 2015, online https://www.scientificamerican.com/article/human-traffickers-caught-on-hidden-internet/ (retrieved on January 8, 2021).

GUILBERT K., “Chasing shadows: can technology save the slaves it snared?,” *Reuters*, June 21, 2018, online https://www.reuters.com/article/us-technology-trafficking-fight-insight-idUSKBN1JH005 (retrieved on March 18, 2021).

INSTITUTE FOR HUMAN RIGHTS AND BUSINESS, “Corporate Liability for Forced Labour and Human Trafficking,” October 2016, https://www.ihrb.org/focus-areas/migrantworkers/corporate-liability-for-forced-labour-and-human-trafficking.

LE CORRE M., “Pourquoi 34 femmes ont attaqué Pornhub, « système mafieux », en justice,” *Madmoizelle*, June 21, 2021, online https://www.madmoizelle.com/pourquoi-34-femmes-ont-attaque-pornhub-systeme-mafieux-en-justice-1139769 (retrieved on August 2, 2021).

LEVY A., “Online sex trafficking bill will make things worse for victims, expert says,” *Perma*, March 29, 2018, online https://perma.cc/8ND4-5DGQ (retrieved on March 18, 2021).

LLORIA GARCÍA P., “La protección integral de la libertad sexual,” *Agenda Pública*, June 7, 2022, online https://agendapublica.elpais.com/noticia/18033/proteccion-integral-libertad-sexual (retrieved on June 10, 2022).

MARINUS ANALYTICS, “About,” *Marinus Analytics*, no date, online https://www.marinusanalytics.com/about (retrieved on October 4, 2022).

MARLASCA M., RENDUELES L., “Territorio Negro: La estrecha relación entre el cine porno y la trata de personas,” *Ondacero*, March 20, 2023, online https://www.ondacero.es/programas/julia-en-la-onda/audios-podcast/territorios/negro/territorio-negro-estrecha-relacion-cine-porno-trata-personas_20230313640f4b0996c07c00017f63d6.html (retrieved on March 23, 2023).

MILA, “AI for Combating Human Trafficking in Canada,” *Mila*, 2021, online https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/ (retrieved on May 1, 2021).

MILA, “Infrared,” *Mila*, no date, online https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/ (retrieved on July 5, 2023).

MINIWATTS MARKETING GROUP, “Top Ten Internet Languages in The World - Internet Statistics,” *Internet World Stats*, January 31, 2020, online https://www.internetworldstats.com/stats7.htm (retrieved on September 22, 2021).

MORRISON S., “The mystery behind OnlyFans’ flip-flop on porn,” *Vox*, August 26, 2021, online https://www.vox.com/recode/22642250/onlyfans-reverse-ban-porn-sexually-explicit-content-policy-bbc-mystery (retrieved on September 9, 2021).

NAST C., “Under the threat of new laws, British sex workers fear for their websites and their safety,” *Wired UK*, July 17, 2018, online https://www.wired.co.uk/article/adult-work-vivastreet-fosta-law (retrieved on April 7, 2023).

PERARNAUD C., “Pour automatiser la censure, cliquez ici,” *Le Monde diplomatique*, July 1, 2022, online https://www.monde-diplomatique.fr/2022/07/PERARNAUD/64826 (retrieved on July 11, 2022).

PORTER J., “Google is kicking ‘sugar dating’ apps out of the Play Store,” *The Verge*, July 29, 2021, online https://www.theverge.com/2021/7/29/22599561/google-play-store-sugar-daddy-apps-dormant-developer-accounts-policy-change (retrieved on August 7, 2021).

RAHMAN S., “Trouble in Romancelandia: Online Censorship of Romance and Erotica,” *BOOK RIOT*, December 3, 2021, online https://bookriot.com/online-censorship-of-romance-and-erotica/ (retrieved on December 9, 2021).

ROMANO A., “A new law intended to curb sex trafficking threatens the future of the internet as we know it,” *Vox*, April 13, 2018, online https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom (retrieved on March 6, 2021).

SMILEY S., LAVOIPIERRE A., “Australian sex workers struggle to survive after US bans online advertising,” *ABC.net*, June 6, 2018, online https://www.abc.net.au/news/2018-06-07/fosta-the-us-law-punishing-australian-sex-workers/9842722 (retrieved on March 6, 2021).

SMITH L., “Shared Hope Statement Regarding FOSTA-SESTA and the Backpage Seizure,” *Shared Hope International*, April 11, 2018, online https://sharedhope.org/2018/04/11/statement-regarding-fosta-sesta/ (retrieved on March 6, 2021).

STATISTA, “User-generated internet content per minute 2022,” *Statista*, April 2022, online https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (retrieved on October 17, 2022).

STEMPEL J., “Zuckerberg, Meta are sued for failing to address sex trafficking, child exploitation,” *Reuters*, March 21, 2023, online https://www.reuters.com/legal/zuckerberg-meta-are-sued-failing-address-sex-trafficking-child-exploitation-2023-03-21/ (retrieved on March 23, 2023).

STOKEL-WALKER C., “'What Does Seggs Mean?' The Rise of Sex Euphemisms on Social Media,” *Vice*, February 2, 2022, online https://www.vice.com/en/article/7kbwx4/tiktok-instagram-shadowban-sex (retrieved on March 1, 2022).

#SURVIVORSAGAINSTSESTA, “Platforms which Discriminate Against Sex Workers,” *#SurvivorsAgainstSESTA*, April 7, 2018, online https://survivorsagainstsesta.org/platforms-discriminate-against-sex-workers/ (retrieved on March 6, 2021).

TIERNEY A., “How the US 'Sex Trafficking' Crackdown Is Hurting Sex Workers in Canada,” *Vice*, April 12, 2018, online https://www.vice.com/en/article/9kggwe/how-the-us-sex-trafficking-crackdown-is-hurting-sex-workers-in-canada (retrieved on July 4, 2022).

I. Research blogs

ALBERT K., “Enough About FOSTA’s 'Unintended Consequences'; They Were Always Intended,” *Techdirt.*, July 29, 2021, online https://www.techdirt.com/articles/20210728/13245147264/enough-about-fostas-unintended-consequences-they-were-always-intended.shtml (retrieved on August 7, 2021).

BARATA J., “Obligations, Liabilities and Safeguards in Content Moderation,” *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, March 2, 2021, online https://intr2dok.vifa-recht.de/receive/mir_mods_00010155 (retrieved on November 27, 2021), DOI:10.17176/20210302-154101-0.

BENSAMOUN A., “Artificial Intelligence Act : l’Union européenne invente la pyramide des risques de l’intelligence artificielle,” *Le Club des Juristes*, May 21, 2021, online https://blog.leclubdesjuristes.com/artificial-intelligence-act-lunion-europeenne-invente-la-pyramide-des-risques-de-lintelligence-artificielle/ (retrieved on June 17, 2021).

CHRISTAKIS T., “Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament’s E-Evidence Draft Report,” *Cross-Border Data Forum*, January 7, 2020, online https://www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/ (retrieved on April 12, 2021).

CHRISTAKIS T., “E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead,” *Cross-Border Data Forum*, January 14, 2019, online https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/ (retrieved on April 12, 2021).

DASKAL J., KENNEDY-MAYO D., “Budapest Convention: What is it and How is it Being Updated?,” *Cross-Border Data Forum*, July 2, 2020, online https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/ (retrieved on April 11, 2021).

DELMAS-MARTY M., “Gouverner la mondialisation par le droit,” *Le Grand Continent*, March 18, 2020, online https://legrandcontinent.eu/fr/2020/03/18/coronavirus-mondialisation-droit-delmas-marty/ (retrieved on July 30, 2021).

GOLDMAN E., “Uh-Oh, the Ninth Circuit Is Messing Again With Its Roommates Ruling-Vargas v. Facebook,” *Technology & Marketing Law Blog*, June 26, 2023, online https://blog.ericgoldman.org/archives/2023/06/uh-oh-the-ninth-circuit-is-messing-again-with-its-roommates-ruling-vargas-v-facebook.htm (retrieved on June 26, 2023).

GOLDMAN E., “Defendants Get Important FOSTA Win in 9th Circuit-Doe v. Reddit,” *Technology & Marketing Law Blog*, October 26, 2022, online https://blog.ericgoldman.org/archives/2022/10/defendants-get-important-fosta-win-in-9th-circuit-doe-v-reddit.htm (retrieved on October 26, 2022).

GOLDMAN E., “The Ninth Circuit’s FOSTA Jurisprudence Is Getting Clearer (and More Defense-Favorable),” *Technology & Marketing Law Blog*, May 5, 2023, online https://blog.ericgoldman.org/archives/2023/05/the-ninth-circuits-fosta-jurisprudence-is-getting-clearer-and-more-defense-favorable.htm (retrieved on May 5, 2023).

GOLDMAN E., “Section 230 Doesn’t Protect App Stores That Sell Virtual Chips for Casino Apps-In re Apple App Store,” *Technology & Marketing Law Blog*, September 6, 2022, online https://blog.ericgoldman.org/archives/2022/09/section-230-doesnt-protect-app-stores-that-sell-virtual-chips-for-casino-apps-in-re-apple-app-store.htm (retrieved on September 7, 2022).

GOLDMAN E., “Section 230 Protect Apple’s App Store from Claims Over Cryptocurrency Theft-Diep v. Apple,” *Technology & Marketing Law Blog*, September 8, 2022, online https://blog.ericgoldman.org/archives/2022/09/section-230-protect-apples-app-store-from-claims-over-cryptocurrency-theft-diep-v-apple.htm (retrieved on September 8, 2022).

GOLDMAN E., “Why FOSTA’s Restriction on Prostitution Promotion Violates the First Amendment (Guest Blog Post),” *Technology & Marketing Law Blog*, March 19, 2018, online https://blog.ericgoldman.org/archives/2018/03/why-fostas-restriction-on-prostitution-promotion-violates-the-first-amendment-guest-blog-post.htm (retrieved on March 18, 2021).

JOUX A., “DMA, DSA : l’Europe va réguler les plateformes,” *La revue européenne des médias numériques*, March 18, 2021, online https://la-rem.eu/2021/03/dma-dsa-leurope-va-reguler-les-plateformes/ (retrieved on April 29, 2021).

KUCZERAWY A., “The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act,” *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, January 12, 2021, online https://verfassungsblog.de/good-samaritan-dsa/ (retrieved on May 27, 2021).

WAGNER B., “A first impression of regulatory powers in the Digital Services Act,” *Verfassungsblog: On Matters Constitutional*, Fachinformationsdienst für internationale und interdisziplinäre Rechtsforschung, January 4, 2021, online https://intr2dok.vifa-recht.de/receive/mir_mods_00009734 (retrieved on November 27, 2021), DOI:10.17176/20210104-182911-0.

INDEX

D

E

F

G

H

I

R

S

TABLE OF CONTENTS