Using US Artificial Intelligence to Fight Human Trafficking in Europe

Potential Impacts on European Sovereignties

Salomé Lannier

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

Human trafficking is keeping pace with new technologies, but so is its repression. Nowadays, artificial intelligence (AI) systems support the daily work of law enforcement authorities in detecting and investigating trafficking schemes. These systems were developed, and are used primarily, in the United States of America (US). As the fight against human trafficking is a worldwide priority, they are often exported from the US or replicated. Yet, so far, little research has been done to examine how (US) policies and values might be embedded in these specific systems. This article argues that the spread of US tools using artificial intelligence to combat human trafficking hinders the autonomy of foreign States. Particularly in the European context, these tools might challenge national criminal sovereignty as well as Europe's digital sovereignty. The article highlights the US policies surrounding human trafficking that are embedded in these AI systems (legal definition, political priorities and decisions) and the lack of adequate consideration of existing European standards. These are meant to protect human rights while developing and using AI systems, i.e. the protection of personal data and control over technical standards.

AUTHOR

Salomé Lannier

PhD candidate
University of Bordeaux (France) and
University of Valencia (Spain)

CITE THIS ARTICLE

Lannier, S. (2023). Using US Artificial Intelligence to Fight Human Trafficking in Europe : Potential Impacts on European Sovereignties. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-002

Published in eucrim 2023, Vol. 18(1) pp 67 – 72

https://eucrim.eu

ISSN:

I. Introduction

In public international law, sovereignty derives from the independence and autonomy of States. The parallel aspect of enjoying the monopoly of legitimate authority over a territory is the exclusion of other States' authority.[1] At the core of the autonomy of States' sovereignty lies their criminal sovereignty: defining offences, sanctions, powers of investigation, policies, priorities, etc.[2] Yet, sovereignty was mainly conceptualised in the 16th century,[3] and such idealization of States' autonomy strikes us a utopia in our globalised[4] and digitalised[5] world. Consequently, the concept of digital sovereignty was developed to adapt to new realities. Originally meant as informational sovereignty (control over information[6]), today digital sovereignty covers different concepts, such as technological sovereignty and data sovereignty,[7] due to the lack of a uniform use. In this article, the modern-day theory of (digital) sovereignty will allow us to highlight the contradiction between the supposed autonomy 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."[8] These disparities of power are particularly threatening to independent sovereignty when they impact criminal law, which is seen as being at the heart of the State's monopoly of legitimate violence.[9]

One of these disparities of power lies in the ability to develop, to use, and to regulate artificial intelligence (AI) systems when applied to repress criminal offences. Since AI relies on humans and institutions for its creation and functioning, "it depends entirely on a […] set of political and social structures."[10] While no unique definition exists regarding AI,[11] computer systems have been assisting States' decision-making processes since the 1970s.[12]

There are many examples of AI systems in use to support the prevention and prosecution of offences. Human trafficking (in particular for the purpose of sexual exploitation) is taken as an example in this article to draw conclusion on the use of AI systems for law enforcement purposes, as they have received little attention from legal scholars (in this area) until now. Human trafficking is an internationally criminalised offence defined in the 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Art. 3.a). It is defined as follows:

> [t]he recruitment, transportation, transfer, harbouring or receipt of persons [element 1: actions], by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person [element 2: coercive means], for the purpose of exploitation [element 3: purpose].

Therefore, trafficking represents a security threat violating the human rights of victims. Protecting victims and prosecuting perpetrators is a manifestation of States' criminal sovereignty. Nowadays, the fight against human trafficking is also at the crossroads of States' digital sovereignty. Indeed, technologies, in particular the internet, can exacerbate the trafficking schemes. Consequently, the term e-trafficking was "coined to describe human trafficking facilitated/enabled or regulated through the use of the internet and other communication platforms."[13] To recruit victims, traffickers actively impersonate an employer, rely on cyber seduction,[14] or use different types of bait online, usually a false job offer.[15] The internet is used to book transportation and accommodation for the potential victim.[16] During the exploitation stage, when the victims are trafficked for the specific purpose of sexual exploitation, technology enables their sexual services to be advertised online.[17] Although trafficking encompasses many forms of exploitation (sexual exploitation, labour exploitation, forced begging and criminality, etc.), American AI systems exclusively, as far as we know, focus on the repression of the federal offence of "sex trafficking." Thus, the intended comprehensive

https://doi.org/10.30709/eucrim-2023-002

approach of the human trafficking phenomena adopted by this article is limited by the existing technologies. Traffickers might take advantage of technology for the anonymity it provides or to hasten trafficking processes. However, e-trafficking also creates data that might be helpful to investigators and used as evidence. Yet, the sheer volume of data challenges their productive analysis by law enforcement authorities.

The creation of AI systems was intended as a solution, namely to support the fight against human trafficking facilitated by the internet. It can automate the crawling and processing of data, organise information linked to ongoing cases, or improve the detection of patterns and red flags to multiply proactive investigations. This idea was first developed by researchers in the United States in 2012.[18] Later, their elaboration was framed into the Defense Advanced Research Projects Agency.[19] Currently, similar systems are being developed outside of the US (e.g. in Canada[20]), and US systems are being exported to Europe (e.g. to the United Kingdom and to Ireland[21]). However, the actual or potential use of foreign tools, especially within the European Union, is not neutral with respect to the autonomy of European sovereignties. The following two sections analyse the risks inherent in the use of US AI systems to the criminal national sovereignty and the digital European sovereignty.

II. Risks of Influencing European *Criminal* Sovereignty

First, the spread of US AI systems developed to support the investigation and prosecution of sex trafficking questions the protection of European national criminal sovereignty. AI systems might be seen as neutral, as they are based on objective data and criteria to combat well-defined criminal phenomena. However, such a perspective reflects mere technological solutionism;[22] it "would postulate the existence of a technical solution to any problem."[23] However, these systems are actually not neutral, as they might be imbued with political positions and policies. As such, when they are used abroad, the politics of their State of origin might be applied in the States of reception, potentially impacting the latter's autonomous sovereign powers. This risk genuinely exists regarding AI systems designed to prevent and prosecute human trafficking.

Despite benefiting from an international definition, the offence of human trafficking has not been fully harmonised. Firstly, the 2000 Protocol was adapted and broadened by European texts[24] (the addition of types of exploitation and suppression of the criterion of a transnational traffic). Secondly, even within Europe, national definitions reveal a wide variety of transpositions of the Directive 2011/36/EU.[25] For instance, in Belgium, coercive means are not an element of the offence but an aggravating circumstance.[26] In France and in Spain, as in the supranational definitions, these means are part of the elements of the offence, although they are slightly differently defined.[27] A comparison between the European definitions and the US code is particularly striking; the latter only recognises trafficking in the context of, on the one hand, peonage, slavery, involuntary servitude, or forced labour, and, on the other hand, sex trafficking.[28] Therefore, an AI system to combat human trafficking needs to be adaptable to national definitions, which might not be applicable, as most of them were developed in the United States and for the United States.

The development of such systems is based on the criminal realities and priorities of each country, particularly regarding the types of exploitation. For instance, in Europe, there is a stronger focus on trafficking for labour exploitation.[29] Yet, systems of AI financed in the United States exclusively focus on the repression of trafficking for domestic sexual exploitation.[30] One of the major means is the analysis of classified advertisements. In particular, these US AI systems emphasise the identification of victims who are minors.[31] The fact that the existing systems are mainly made in the United States impacts worldwide priorities in the fight against the complex and multifaceted phenomenon of human trafficking. It reinforces the continuous focus on sexual exploitation,[32] which has been strongly criticised as a very limited conception of human trafficking.[33]

In the latter context, one should consider as well that trafficking for sexual exploitation can, under some national legislations, be conflated with sex work. Certain states' policies consider commercial sex as exploitative *per se*, regardless of working conditions and the legitimacy of a sex workers' agency.[34] This is the case in the United States, where sex work is mainly illegal.[35] On the contrary, there are various sex work regulations in Europe: legal regulation (the Netherlands, Germany), prohibition (Romania), criminalisation of clients (France, following the Nordic model)[36], and decriminalization (Belgium[37]). To qualify as an act of adult sex trafficking in the United States, the US code only requires a commercial sexual act as the purpose. Yet, it still requires proof of "means of force, threats of force, fraud, [or] coercion"[38] (child trafficking does not require this element: to identify an underage trafficked victim, an AI system would only have to detect underage persons advertised for a commercial sexual act). Nevertheless, indicators of potential trafficking in advertisements for sex workers' services hardly take this element into consideration; they rely only on indirect potential flags of exploitation[39] (it is obviously rare to find explicit proof of coercion in the ads). They have been identified on the basis of US prosecutions and by experts and databases, but the indicators remain the basis of the criteria used abroad, although criminal realities might differ.[40] It must be pointed out that American researchers developing these systems mostly rely on a conflation between trafficking and sex work, and they do not consider nor mention the existing discussions on whether sex trafficking should be, or not, conflated with sex work.[41] Researchers and sex workers have come to criticise the criteria set by the systems as not being able to detect victims of trafficking but instead discriminating sex workers.[42] Consequently, this conflation is embedded in the functioning of most of the US systems of AI designed to support the investigation of sex trafficking cases. Therefore, their use in Europe, in particular in countries where sex work policies are different, could have a significant impact on the autonomy of their criminal sovereignty.

III. Risks of Influencing European *Digital* Sovereignty

Apart from the potential threat to European criminal national sovereignty by not taking into account national definitions, law enforcement priorities, and the delimitation of human trafficking, the use of AI systems originating from the United States to prevent and combat human trafficking in Europe might also hinder digital sovereignty.

Firstly, the use of AI systems from the United States challenges data sovereignty, which is understood as "the ability to store and process certain types of data."[43] Classical sovereignty prioritises the possibilities to exercise control and authority over data. Interpreted through the lens of human rights, sovereignty also includes the protection of citizens' personal data. Data, in particular personal data, is a "genuine power issue between States."[44] EU data sovereignty, in particular, lies in its innovative and unique approach to protect it. Processing personal data for the purpose of combating an offence is regulated by Directive 2016/680.[45] Despite setting out more lenient obligations than the General Data Protection Regulation,[46] the Directive still lists a number of principles to be implemented by design (Art. 4), which can be summarised as the following:

- Lawful and fair processing, delimited by specific purposes;
- Limitation of collection and conservation of data;
- Data accuracy, integrity, and confidentiality;
- Liability on the part of the data processor.

If AI systems have been developed in the United States for an originally American-only use, however, these AI systems do not fall within the scope of the European data protection framework. Therefore, it is doubtful whether the protection of personal data has been incorporated into the systems from the start of their

https://doi.org/10.30709/eucrim-2023-002

development. Since the transparency principle is absent from the Directive, the necessary safeguards to control the use of these AI systems are particularly important to balance any interference with the right of privacy.

Another important point is the localisation of the processed data. Indeed, it would be particularly sensitive to store European data related to criminal investigations in the United States if the AI systems use a cloud version saved on US servers. The Directive provides for the possibilities of transferring data outside the EU (Arts. 35 to 40). Specifically, the Umbrella agreement was signed between the EU and the United States on this matter in 2016.[47] A few months earlier, the Privacy Shield[48] set a supposedly adequate level of data protection for data transfers for commercial and civil purposes. Yet, it was invalidated by the CJEU.[49] On the contrary, the lawfulness of the Umbrella agreement has not been questioned. As these AI systems process large quantities of data, including, sensitive data, the effectivity of safeguards when data is transferred abroad should be particularly reviewed.

Secondly, European digital sovereignty is not limited to data sovereignty but also covers the regulation of technical aspects, leading to a technical sovereignty. Indeed, Directive 2016/680 hardly considers the specificities of AI systems. For instance, it does not take into account the principle of transparency or the explanation of the algorithms that comprise the AI system,[50] even though this is at the core of ensuring that data used to train it does not lead to any discrimination.[51] The Directive also does not take into consideration any protection against discriminating results.[52] This is why the European Commission launched a proposal for an AI Act in 2021.[53] This act would apply whenever the AI systems are used by European users, including law enforcement authorities (Art. 2.2). As these systems are to be used for the prosecution of offences (Art. 7.1.a in relation to Annex III.6), they are classified as high-risk and must comply with the highest level of obligations. Yet, transparency obligations have been excluded for these systems (Art. 52).

While this act is still under negotiation, the CJEU provided guidance for the regulation of automated systems. In its Opinion of 2017 on the EU-Canada PNR Agreement, the Court recognised the possibility of carrying out an automated analysis based on predefined models and criteria and a comparison with various databases.[54] The Court introduced five elements to assess the lawfulness of the use of AI systems to prosecute offences:[55]

- Establishing specific, reliable, and non-discriminatory models and criteria to ensure the targeting of individuals with a level of “reasonable suspicion”;
- Using automated means only for serious transnational crime;
- Ensuring databases are reliable and up-to-date;
- Introducing an individual re-examination by non-automated means to offset the margin of error;
- Concluding a review of the implementation.

Against this background, it should be stressed that the US systems are mainly used to assist in the investigation of domestic trafficking, which calls into question their applicability in Europe. The conclusion on data sovereignty applies to technical sovereignty: US systems did not integrate European standards (existing standards and those under development) when developing their algorithm. Furthermore, when the software code is developed by private entities, the lack of transparency and the protection of the code by intellectual property rights challenge the access to technical elements to ensure their conformity to European frameworks.

IV. Conclusion

As human trafficking schemes are being increasingly supported by online services, one challenge for law enforcement to combat human trafficking lies in the processing and organisation of available data online. It is next to impossible for individual investigators to develop an efficient means of manually processing data. Manual processing is indeed unsuitable for the volume of data and to keep up with the speed of deletion and updates. As a solution, the automatic processing of data and systems relying on AI have been developed to assist law enforcement authorities. These instruments are intended to support the exercise of sovereignty by states by protecting their populations and borders.

Yet, AI systems used to combat offences are not neutral: depending on the context of their development, they embed specific values and policies. As such, due to the digital interconnectedness of the world, if exported abroad, they might hinder the autonomy of other States by limiting their own exercise of sovereign powers.

A first challenge in this regard relates to European *criminal* national sovereignty In particular as regards human trafficking, systems are based on a specific national definition of an offence that might not be consistent with foreign definitions. Similarly, they are often developed in a particular national criminal context, making them harder to adapt to foreign criminal realities if a consistent reprogramming is not considered. Furthermore, because they were developed primarily in the United States, they underline a continued focus on combating sex trafficking while disregarding other forms of trafficking, such as labour exploitation. Lastly, the American AI systems have usually been programmed according to a prohibitionist policy that equates sex trafficking with sex work, which leads to these values and political decisions being integrated in the systems. All of these elements indicate that the autonomy of European national criminal justice sovereignty could be threatened if American systems are used or if national systems are developed on the basis of American systems without specific adaptation.

The use of US AI systems in Europe to combat human trafficking also challenges European *digital* sovereignty. The EU has developed regulations and standards to safeguard the protection of personal data and the specific risks linked to the use of AI systems. Yet, these norms are not applicable to systems originally developed for a US-only use. Although transparency requirements of AI systems are to be limited when used by law enforcement authorities, European norms under development still require conformity with human rights standards. This reinforces the potential threats to European autonomy when developing AI systems that are consistent with its own policies and values, both from a criminal law and a human rights perspective.

---

1. K. Irion, "Government Cloud Computing and National Data Sovereignty", (2012) 4(3-4) *Policy & Internet*, 40, 53.↩
2. M. Massé, "La souveraineté pénale", (1999) *Revue de science criminelle et de droit pénal comparé*, 905, 905.↩
3. J. Bodin, J.H. Franklin, *On sovereignty: four chapters from the six books of the commonwealth*, Cambridge University Press, Cambridge texts in the history of political thought, 1992.↩
4. J.A. Agnew, *Globalization and sovereignty: beyond the territorial trap*, Rowman & Littlefield, Globalization, 2nd ed., 2018.↩
5. M. Kettemann, *The normative order of the internet, a theory of rule and regulation online*, Oxford University Press, 2020.↩
6. A. Gotlieb, C. Dalfen, K. Katz, "The Transborder Transfer of Information by Communications and Computer Systems: Issues and Approaches to Guiding Principles", (1974) 68(2) *American Journal of International Law*, 226.↩
7. Communication from the Commission, "Shaping Europe's digital future", COM(2020) 67 final, p. 2.↩
8. T. Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", (2020) *SSRN Scholarly Paper, ID 3748098*, <https://papers.ssrn.com/abstract=3748098> accessed 28 February 2023.↩
9. M. Weber, *The vocation lectures: science as a vocation, politics as a vocation*, Hackett Pub, 2004↩
10. K. Crawford, *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021, 8.↩
11. One definition is the following: a "set of scientific methods, theories and techniques whose aim is to reproduce, by a machine, the cognitive abilities of human beings", European Commission for the Efficiency of Justice (Council of Europe), "European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment", 2018, 69.↩

https://doi.org/10.30709/eucrim-2023-002

12. D.K. Citron, "Technological Due Process", (2008) 85(6) *Washington University Law Review*, 1248, 1257.↩
13. S. Milivojević, "Gendered exploitation in the digital border crossing? An analysis of the human trafficking and information-technology nexus", in: M. Segrave and L. Vitis (eds.), *Gender, Technology and Violence*, 2017, pp. 28-29.↩
14. Resolution 27/2 of the Commission on Crime Prevention and Criminal Justice, Economic and Social Council, United Nations, "Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies", E/2018/30 E/CN. 15/2018/15.↩
15. L. Holmes, "Introduction: the issue of human trafficking", in: L. Holmes (ed.), *Trafficking and human rights: European and Asia-Pacific perspectives*, 2010, pp. 1, 9; Council of Europe report by A. Sykiotou, "Trafficking in human beings: Internet recruitment – Misuse of the Internet for the recruitment of victims of trafficking in human beings", 2007, p. 32; A. Lavorgna, *Transit crimes in the Internet age: How new online criminal opportunities affect the organization of offline transit crimes*, Thesis, University of Trento, 2013, p. 126; A. Di Nicola, G. Baratto, E. Martini, *Surf and sound – The role of the internet in people smuggling and human trafficking*, University of Trento, ECrime Research Reports, 2017, p. 62.↩
16. Europol Intelligence Notification 15/2014, "Trafficking in human beings and the internet", 2014.↩
17. J. Middleton, "From the Street Corner to the Digital World: How the Digital Age Impacts Sex Trafficking Detection and Data Collection", in: J. Winterdyk and J. Jones (eds.), *The Palgrave International Handbook of Human Trafficking*, 2020, pp. 467, 471; J.L. Musto, D. Boyd, "The Trafficking-Technology Nexus" (2014) 21(3) *Social Politics*, 461, 467; 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, 2020, p. 45.↩
18. E. Kennedy, *Predictive Patterns of Sex Trafficking Online*, Thesis, Carnegie Mellon University, 2012.↩
19. 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*, 2015, p. 205; C. Pellerin, "DARPA Program Helps to Fight Human Trafficking", *U.S. Department of Defense*, <https://www.defense.gov/News/News-Stories/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/> accessed 28 February 2023; Department of Justice of the United States of America, "National Strategy to Combat Human Trafficking", 2017, p. 11.↩
20. Mila, "Infrared: AI for combating human trafficking in Canada", *Mila*, <https://mila.quebec/en/project/ai-for-combating-human-trafficking-in-canada/> accessed 28 February 2023.↩
21. Marinus Analytics, "About", *Marinus Analytics*, <https://www.marinusanalytics.com/about> accessed 4 October 2022.↩
22. E. Morozov, *To save everything, click here: the folly of technological solutionism*, 1st ed. PublicAffairs, 2013.↩
23. Y. Meneceur, *L'intelligence artificielle en procès: Plaidoyer pour une réglementation internationale et européenne*, Bruylant, 2020, p. 2; M. Broussard, *Artificial unintelligence: how computers misunderstand the world*, The MIT Press, 2018, pp. 7-8.↩
24. Council of Europe Convention n°197 on Action against Trafficking in Human Beings, 2005; 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, *O.J.* L 101, 15.4.2011, 1.↩
25. 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, University of Bordeaux and Vietnam National University, 2019, pp. 32ff. Case law also highlighted the potential multiple interpretations of the concept, L. Esser, C. Dettmeijer-Vermeulen, "The Prominent Role of National Judges in Interpreting the International Definition of Human Trafficking" (2016) 6 *Anti-Trafficking Review*, 91; E. Coreno, "Finding the Line between Choice and Coercion: An Analysis of Massachusetts's Attempt to Define Sex Trafficking" (2021) 13(1) *Northeastern University Law Review*, 124.↩
26. Articles 433 quinquies and 433 septies of the Belgium criminal code.↩
27. Article 225-4-1 of the French criminal code; article 177 bis of the Spanish criminal code.↩
28. 18 U.S. Code § 1590 and § 1591.↩
29. Group of Experts on Action against Trafficking in Human Beings (Council of Europe), "Guidance note on preventing and combatting trafficking in human beings for the purpose of labour exploitation", GRETA(2020)12 ; Communication from the Commission, "EU Strategy on Combatting Trafficking in Human Beings 2021-2025", COM(2021) 171 final, pp. 7-8.↩
30. Yet, most of the titles of the articles on them are misleading, as they target human trafficking in general; see, for instance, M. Ibanez, D. Suthers, "Detection of Domestic Human Trafficking Indicators and Movement Trends Using Content Available on Open Internet Sources", (2014) *47th Hawaii International Conference on System Sciences*, <http://ieeexplore.ieee.org/document/6758797/> accessed 28 February 2023; A. Dubrawski et al., "Leveraging Publicly Available Data to Discern Patterns of Human-Trafficking Activity" (2015) 1(1) *Journal of Human Trafficking*, 65; P. Szekely et al., *op. cit.* (n. 19), p. 205.↩
31. B. Westlake, M. Bouchard, R. Frank, "Comparing Methods for Detecting Child Exploitation Content Online", (2012) *European Intelligence and Security Informatics Conference*, <http://ieeexplore.ieee.org/document/6298826/> accessed 28 February 2023, 156; H. Wang et al., "Data integration from open internet sources to combat sex trafficking of minors" (2012) *Proceedings of the 13th Annual International Conference on Digital Government Research*, <http://dl.acm.org/citation.cfm?doid=2307729.2307769> accessed 28 February 2023; 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 (STIR), 2018.↩
32. Only two European researchers 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", (2015) *Proceedings of the ACM Web Science Conference on ZZZ – WebSci'15*, <http://dl.acm.org/citation.cfm?doid=2786451.2786510> accessed 28 February 2023; A. Volodko, E. Cockbain, B. Kleinberg, "'Spotting the signs' of trafficking recruitment online: exploring the characteristics of advertisements targeted at migrant job-seekers" (2020) 23 *Trends in Organized Crime*, 7.↩
33. J. Chuang, "Giving as Governance? Philanthrocapitalism and Modern-Day Slavery Abolitionism", (2015) 62 *UCLA Law Review*, 1522.↩
34. 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", (2006) 29(2) *Harvard Women's Law Journal*, 347; C. Plumauzille, "Prostitution", in: J. Rennes (ed.), *Encyclopédie critique du genre*, 2021, p. 590.↩
35. R. Russo, "Online Sex Trafficking Hysteria: Flawed Policies, Ignored Human Rights, and Censorship" (2020) 68(2) *Cleveland State Law Review*, 314, 323.↩
36. 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.↩

37. Loi modifiant le Code pénal en ce qui concerne le droit pénal sexuel, 2022.↩
38. 18 U.S. Code § 1591(a).↩
39. Setting aside criteria linked to minority: shared management, geographic displacements, E. Kennedy, *op. cit.* (n. 18); shared phone number, M. Latonero, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking*, Center on Communication Leadership & Policy, University of Southern California, 2012; inconsistencies in story, third party language, ethnicity, potential restricted movement ("in calls only"), M. Ibanez, D. Suthers, (2014) *47th Hawaii International Conference on System Sciences*, *op. cit.* (n. 28) 1556; unconventional sex advertised, disguised phone number, transient language, M. Hultgren, *An exploratory study of the indicators of trafficking in online female escort ads*, Thesis, San Diego State University, 2015. 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" (2018) 7(1) *Security Informatics*, 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" (2020) 35(23-24) *Journal of Interpersonal Violence*, 5607.↩
40. 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, 2022 ; L. Giommoni, R. Ikwu, "Identifying human trafficking indicators in the UK online sex market" (2021) *Trends in Organized Crime*, < https://doi.org/10.1007/s12117-021-09431-0> accessed 11 October 2022.↩
41. On the contrary, explicitly trying to differentiate between consensual sex work and sexual exploitation, refer to 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, 2021; B. Cartwright et al., *op. cit.* (n. 38).↩
42. R. Kjellgren, "Good Tech, Bad Tech: Policing Sex Trafficking with Big Data" (2022) 11(1) *International Journal for Crime, Justice and Social Democracy*, 149; M. Draughn, "No Ground Truth: Sex Trafficking and Machine Learning", *Windypundit* <https://windypundit.com/2022/07/no-ground-truth-sex-trafficking-and-machine-learning/> accessed 23 August 2022.↩
43. K. Irion, (2012) 4(3-4) *P&I*, *op. cit.* (n. 1), 40, 62.↩
44. M. Quéméner, *Le droit face à la disruption numérique: adaptation des droits classiques: émergence de nouveaux droits*, Gualino, 2018, p. 22.↩
45. 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, *O.J.* L 119, 4.5.2016, 89.↩
46. In particular, regarding the principle of transparency, information, and obligations to delete, O. Tambou, J.F. López Aguilar, *Manuel de droit européen de la protection des données à caractère personnel*, Bruylant, 2020, pp. 130-131, 188-194, 202.↩
47. 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 offences, *O.J.* L 336, 10.12.2016, 3.↩
48. 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-U.S. Privacy Shield (notified under document C(2016) 4176), *O.J.* L 207, 1.8.2016, 1.↩
49. CJEU, 16 July 2020, Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II)*.↩
50. Commission White Paper, "Artificial Intelligence – A European approach to excellence and trust", COM/2020/65 final, p. 17.↩
51. European Union Agency for Fundamental Rights, "#BigData: discrimination in data supported decision making", 2018.↩
52. S. Wachter, B. Mittelstadt, L. Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) *International Data Privacy Law*, 82.↩
53. Proposal from the Commission, "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", COM/2021/206 final.↩
54. CJEU, 26 July 2017, Opinion 1/15, *Draft agreement between Canada and the European Union – Transfer of Passenger Name Record data*, para. 168.↩
55. *Ibid.* para. 172-174. Further criteria were developed when "it covers, generally and indiscriminately, the data of person s using electronic communication systems", CJEU, 6 October 2020, Joined Cases C-511/18, C-512/18, and C-520/18, *La Quadrature du Net, and Others*, para. 174-191.↩

over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union