eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

Artificial Intelligence in Law Enforcement Settings

AI Solutions for Disrupting Illicit Money Flows

Dimitrios Kafteranis, Athina Sachoulidou, Umut Turksen *

ABSTRACT

With the rise and spread of ICT-enabled crimes and illicit money flows (IMFs), law enforcement authorities and financial intelligence units need innovative investigative tools and skills, and organisational and regulatory adjustments to counter crime. The multi-disciplinary TRACE project is developing AI solutions to identify, track, and document IMFs to pave the way for effectively prosecuting money laundering and predicate offences and recovering criminal proceeds. In this article, the authors present the TRACE project to reveal some of the challenges faced by law enforcement authorities in adopting AI-driven investigative tools, taking into account the ongoing legislative procedures in preparation for the adoption of the EU Artificial Intelligence Act. It is argued that more empirical research is required on the design and feasibility of these AI-enabled tools given their implications for various legal principles, such as privacy, data protection, and the right to a fair trial. An "ethics and rule of law by design" approach, as is also being pursued by the TRACE project, is mapped out as a robust framework for developing AI tools intended to be used for law enforcement purposes.

AUTHORS

Dimitrios Kafteranis
Assistant Professor in Law
Coventry University, United Kingdom

Athina Sachoulidou
Assistant Professor
Universidade Nova de Lisboa, Portugal

Umut Turksen
Professor in Law
Coventry University, United Kingdom

CITATION SUGGESTION

D. Kafteranis, A. Sachoulidou, U. Turksen, "Artificial Intelligence in Law Enforcement Settings", 2023, Vol. 18(1), eucrim, pp60–66. DOI: https://doi.org/10.30709/eucrim-2023-006

Published in
2023, Vol. 18(1) eucrim pp 60 – 66
ISSN: 1862-6947
https://eucrim.eu

I. Introduction

Rooted in popular culture, the catchphrase “follow the money” is often invoked in the context of investigations aimed at uncovering financial malfeasance.[1] As Europol notes: “To effectively disrupt and deter criminals involved in serious and organised crime, law enforcement authorities need to follow the money trail as a regular part of their criminal investigation with the objective of seizing criminal profits”.[2]

This is particularly true for investigating money laundering, which involves disguising the proceeds of criminal activity (predicate offences) to make them appear legitimate. By following the money trail, namely identifying individuals, companies, or transactions that require closer scrutiny, law enforcement authorities (LEAs) are able to seize criminal assets and profits, and bring offenders to justice.[3]

The European Union (EU) and its Member States are not immune from cross-border financial crime, including but not limited to money laundering. To address this phenomenon, the EU has taken various legislative measures and is currently negotiating a new anti-money laundering and countering the financing of terrorism legislative package that was first proposed in July 2021.[4] The creation of the European Public Prosecutor’s Office (EPPO) consolidated the EU’s institutional framework in this regard.[5] While it is also putting in place steps towards a more efficient legal framework for combatting financial crime, the development of new technologies has opened up new opportunities for criminals to exploit in many different areas, such as crypto-assets and fast internet connections.[6] Notwithstanding the above, such technologies may also revolutionise the way LEAs gather and evaluate evidence in order to assist criminal justice authorities in prosecuting crime effectively, particularly to the extent that borderless crime requires cross-border cooperation.

Combining expertise in computer engineering, law, and social sciences from academia, policy makers, and law enforcement agencies, the TRACE project has embarked on exploring illicit money flows (IMFs) in the context of six use cases: terrorist financing, web forensics, cyber extortion, use of cryptocurrency in property market transactions, money laundering in arts and antiquities, and online gambling.[7] Its ultimate goal is to equip European LEAs with the tools and resources necessary to identify, track, document, and disrupt IMFs in a timely and effective manner. This can involve, among other things, the analysis and visualisation of financial data (virtually in any given language), the identification of suspicious financial activity patterns, and collaboration with other agencies to share information. These tools are developed with the help of cutting-edge technologies, such as artificial intelligence (AI) and machine learning (ML). As a consequence, they should represent trustworthy solutions adhering to the rule of law, fundamental rights, and ethical design principles. For this purpose, the TRACE project has a dedicated work package (WP8) on the ethical, legal, and social impact of the AI solutions it develops.[8]

Informed by the research conducted for the TRACE project, this article outlines some of the key findings on the use of AI in law enforcement settings as follows: Firstly, it provides a conceptual framework, including a definition of AI (Section II). Secondly, it explains how AI systems may reshape law enforcement with an emphasis on crime analytics (Section III), and which law governs such uses of AI (Section IV). In doing so, the article employs EU law as a system of reference and sheds light on the AI governance model included in the European Commission’s Proposal for a Regulation laying down harmonised rules on AI (EU AIA).[9] Finally, by critically analysing the EU legal regime for AI, the article identifies key shortcomings and offers suggestions and recommendations (Section V).

II. Conceptual Framework: Definition of AI and Data Informing AI Systems

Although there is (still) no unanimously accepted definition of AI,[10] the past two decades have been marked by the exponential development of AI systems using algorithms, statistical models, and other techniques. These are used to analyse and interpret large amounts of data (originating from various sources and often referred to as "big data"), with the help of advances in computing power, and to make predictions or decisions based on the analysis of this data.[11] This goes hand in hand with the diversification of AI applications, including natural language processing, image and voice recognition, autonomous vehicles, and predictive analytics.

At policy-making level, as early as in 2018, the UK government referred to AI in its Industrial Strategy White Paper as: "[t]echnologies with the ability to perform tasks that would otherwise require human intelligence, such as visual perception, speech recognition and language translation".[12] In the same year, the European Commission, in its Communication on AI for Europe, emphasised not only the element of intelligent behaviour, but also the degree of autonomy AI systems may present.[13] Furthermore, the Commission set up a multi-disciplinary expert group, namely the High-Level Expert Group on AI (AI HLEG) to clarify the definition of AI and to develop ethics guidelines for trustworthy AI.[14] The findings of this group have informed the first attempt to regulate AI at EU level, i.e. the EU AIA, which includes a proposal for the first formal legal definition of AI. In particular, art. 3 nr.1 EU AIA defines an "AI system" as: "software that […] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[15] Designed to classify AI as a sociotechnical concept, this definition has also been used by the TRACE project.

AI applications are data-driven applications. The data used to train an AI system, and the data it processes, depend on the type of tasks a system is designed to perform. AI systems intended to be employed for law enforcement purposes are no exception, namely they require various types of data, whether personal[16] or not, to become effective. This may include, for instance: 1) data on past criminal activity that can be used to train AI systems to forecast criminal activity, 2) social media data that can be analysed to identify behavioural patterns that correlate with suspicious activity, 3) demographic data, such as age, gender, race, that can be used to inform decisions about the allocation of law enforcement resources, or 4) travel, communication, and financial data, the combination of which can decode the specifics of past criminal activity.

Gathering and processing data for developing, training, and using AI systems may raise significant ethical and legal issues, including but not limited to privacy, data protection, bias, and due process.[17] To capitalise on the benefits of data-driven applications in a law enforcement environment, it is therefore imperative that the respective algorithms are trained and supplied with *accurate* data, previously collected in appropriate contexts, and that this data is properly linked, in order to avoid false negatives and, more importantly, false positives.[18] What is more, the data used to train an algorithm may reflect discriminatory practices and entrench biases.[19] One danger of algorithmic bias is the generation of a bias "feedback loop", in which the analysis or predictions of an ML-based system influence how the same system is validated and updated.[20] In other words, this is a case of algorithms influencing algorithms, because their analysis then influences the way LEAs act on the ground.[21] If the algorithmic output were to be used in law enforcement decisions or even as evidence in a courtroom, this reality could adversely affect the rights of the defence and lead to severe consequences, including deprivation of a person's freedom.[22] This suggests that high-quality and accurate data is needed to ensure that the resulting predictions, decisions, or actions are also accurate, fair, and unbiased. In fact, the respective AI systems should be tested and audited for accuracy and fairness on a regular basis.[23]

III. Use of AI in Law Enforcement Settings

The use of AI for law enforcement purposes has already been challenged by legal scholars with the focus placed predominantly on predictive policing and facial recognition, that allows for the automatic identification or authentication of individuals, and on AI applications employed in criminal proceedings to calculate the risk of recidivism.[24] The EU AIA covers the use of AI in law enforcement settings in two scenarios. Firstly, it prohibits the use of real-time remote biometric identification systems in publicly accessibly spaces unless this is strictly necessary for achieving the purposes set out in art. 5 (1) lit. d.[25] Secondly, the EU AIA classifies other AI systems employed for law enforcement purposes as high-risk (art. 6) – based on the risks they may pose to fundamental rights (recital 38) – and stipulates a series of legal obligations on their providers (see Section IV). In particular, point 6 Annex III to EU AIA introduces a typology of high-risk automated law enforcement, including AI systems intended to be used:

- For individual risk assessments of natural persons in order to assess the risk of (re-)offending or the risk for potential victims of criminal offences (lit. a);
- As polygraphs and similar tools or to detect the emotional state of a natural person (lit. b);
- To detect deep fakes (lit. c);
- To evaluate the reliability of evidence in the course of criminal investigations or crime prosecution (lit. d);
- For predicting the (re-)occurrence of an actual or potential crime based on profiling of natural persons (art. 3 (4) Directive (EU) 2016/680) or assessing personality traits and characteristics or past criminal behaviour of natural persons and groups (lit. e);
- For profiling of natural persons in the course of crime detection, investigation or prosecution (lit. f);
- For crime analytics regarding natural persons, allowing LEAs 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 (lit. g).

This typology does not include AI-driven consumer products that may not be intended for law enforcement purposes but do have the potential to produce an output of probative value that could be evaluated as a piece of evidence before criminal courts.[26]

In the context of AI-driven crime analytics, AI can be used to organise, categorise, analyse, and interpret suspicious activity reports and evidence and, in particular, electronic evidence (such as online shopping, financial transactions, emails, chat logs, social media posts, and the corresponding subscriber and traffic data) with the aim of consolidating the prosecution files. This suggests that the respective evidence, corresponding to *past* criminal activity, has already been collected, with or without the help of AI applications. In that sense, the focus lies on identifying patterns in the data available to LEAs and connections that may not be visible to human analysts or the detection of which may be particularly resource- and time-consuming.[27]

The TRACE tools, which are aimed at disrupting IMFs that usually comprise voluminous, often publicly accessible data, fit better into the category of AI-supported crime analytics (point 6, lit. g EU AIA), considering that their current design does not allow for individual risk assessment or for profiling of specific natural persons. Based on this classification, the TRACE consortium has decided to comply with the requirements set out in arts. 6–52 EU AIA. Interestingly, however, all Compromise Texts released to date and the

https://doi.org/10.30709/eucrim-2023-006

Council's General Approach to the EU AIA do not list AI-supported crime analytics anymore under high-risk AI systems and, thus exempt the providers of those systems from complying with the requirements for developing high-risk AI.[28]

IV. What Law – If Any – Governs AI Systems in Law Enforcement Settings?

Currently, there is no specific law in the EU that governs the use of AI in law enforcement settings. However, there are several existing legal frameworks that may apply to the development and use of AI in general and AI-driven crime analytics in particular.

1. Data protection and management

The rights to privacy and to personal data protection (arts. 8 European Convention on Human Rights (ECHR); 7–8 Charter of Fundamental Rights of the EU (CFR)) are cardinal with respect to both the development and the use of AI applications. Out of the EU laws setting out data protection and management rules, the focus lies on Regulation (EU) 2016/679 (a.k.a. GDPR), and Directive (EU) 2016/680,[29] known as LED. The envisaged TRACE tool, which is intended to assist LEAs in investigating IMFs by, *inter alia*, visualising nodes and edges in real-life scenarios of money laundering and various predicate offences, cannot fully exclude access to and processing of personal data, even if publicly accessible data is given priority.

For data protection purposes, it is important to distinguish the stage of *developing* AI-driven crime analytics tools, which is governed by the GDPR, from that of LEAs *applying* such tools for operational purposes. The latter is governed by the LED to the extent that processing of personal data takes place. The LED – whilst having the same axiological basis as the GDPR, presents different nuances as to, for instance, enforceable data subject rights or the powers of data protection authorities related to the particularities of the police and criminal justice environment (see recitals 10, 11).[30] This means that personal data has to be processed lawfully for law enforcement purposes and that such personal data processing is also governed by the principles of purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality (art. 4 (1) LED). However, similar to data subject rights, these principles have been adapted to ensure a certain level of flexibility, in order to accommodate special security-related needs and day-to-day law enforcement practices.[31]

When it comes to the lawfulness of personal data processing for law enforcement purposes, the LED is more restrictive compared to the GDPR and its legal bases for personal data processing (art. 6 GDPR). More specifically, art. 8 (1) LED states that:

> Member States *shall* (emphasis added) provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) [namely prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security] and that it is based on Union or Member State law.

The processing of personal data is therefore only legal if it is linked to a task within the Directive's scope, as specified in the domestic laws transposing it.[32]

Art. 9 LED is applicable in the testing phase of AI-driven applications, when LEAs use LEA datasets that are only available to them. This dictates that personal data collected by competent authorities for the purpose of

https://doi.org/10.30709/eucrim-2023-006

the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal sanctions may only be processed for other purposes, *if such processing is authorised by Union or Member State law*. In this case, the GDPR is applicable, unless the processing is carried out as part of an activity which falls outside the scope of Union law (art. 9 (1) LED). The GDPR is also applicable when LEAs process personal data for, *inter alia*, scientific purposes (art. 9 (2) LED).

Furthermore, LEAs, in their capacity as data controllers, are obliged to conduct a data protection impact assessment (DPIA) as required by art. 27 (1) LED “where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons”. At a minimum, the DPIA must contain: a general description of the envisaged processing operations; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged to address those risks; safeguards; security measures; and mechanisms to ensure the protection of personal data and to demonstrate compliance with the LED (art. 27 (2) LED). Importantly, the LED’s wording makes a DPIA mandatory when it comes to the use of new technologies for personal data processing in a law enforcement environment.[33] This suggests that the future use of TRACE tools on the part of national LEAs will require a DPIA.

Finally, gathering and processing non-personal data is governed by Regulation (EU) 2018/1807,[34] which “aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users” (art. 1). Data localisation requirements may be imposed on grounds of public security (including crime investigation, detection, and prosecution) in compliance with the principle of proportionality (art. 4 (1)). Recital 9 expressly refers to AI as one of the major sources of non-personal data – with aggregate and anonymised datasets used for big data analytics being a specific example of non-personal data. Should it become possible to turn anonymised data into personal data, such data is to be treated as personal, and the GDPR applies accordingly.

2. Protection of fundamental rights

When AI is employed in fields tightly linked to public governance, such as law enforcement, it is necessary to broaden the scope of human rights considerations, namely to go beyond privacy and data protection as part of the ethical and legal impact assessment of the respective applications.[35] In other words, one should take a holistic approach to the protection of human rights of the affected individuals.[36] This also includes *procedural* fundamental rights, considering that, for instance, AI-driven crime analytics aims at organising and evaluating information of probative value for crime prosecution purposes. Thus, the legal framework that governs the utilisation of AI in law enforcement settings should comprise the ECHR and the CFR, complemented – with respect to defence rights – by EU secondary laws.[37]

In addition, the EU AIA adopts a risk-based approach to AI systems on the basis of their implications for safety, health, and fundamental rights (recitals 13, 27–28). This also applies to AI systems intended to be used for law enforcement purposes, which are classified as high-risk, considering the power imbalance inherent in law enforcement, the risk of discrimination and unfair treatment associated with the lack of high-quality data, accuracy, robustness *as well as* the risk of hampering important procedural fundamental rights that arises from a lack of transparency, explainability, and documentation (recital 38). As such, automated law enforcement applications must comply with certain requirements before they can be placed on the market or used in the EU. In particular, these requirements include the establishment, implementation, documentation, and maintenance of a risk management system (art. 9), the use of high-quality training, validation, and testing datasets (art. 10), technical documentation that enables the assessment of the AI system’s compliance with the requirements set out in the EU AIA (art. 11), logging capabilities (art. 12), design enabling the interpretability of the system (art. 13), and safeguarding human oversight (art. 14), accuracy, robustness, cybersecurity (art. 15).[38] These are significant safeguards to ensure that AI systems used in law enforcement do not perpetuate biases or discriminate against certain individuals or groups, are transparent and fair, and do not cause harm. In that sense, these requirements represent an important step towards ensuring that automated law enforcement applications are used responsibly and ethically.

V. Areas of Contention and Reform

The planned decategorisation of AI-driven crime analytics as high-risk, as part of the ongoing negotiations on the EU AIA, may be aligned with the realities of police investigations in the digital age, but remains predominantly effectiveness-centred. This approach fails to pay heed to the risks and challenges arising from the data-intensive character of these applications,[39] the potential bias inherent in the training and validation datasets as well as in the data which the system processes, or the risks inherent in repurposing AI and, particularly, the inadvertent shift from pattern-based to individual-based data mining. Additionally, it does not take into account the numerous societal concerns regarding the automation of law enforcement – concerns primarily related to risks to citizens' rights, ranging from privacy and non-discrimination to the fair trial principle – emerging from the use of unchecked or not sufficiently checked AI by LEAs. Such concerns suggest that the exceptions suggested by the Council's Compromise Texts and General Approach to the EU AIA should be treated with caution and require clear checks and balances.

Another area of regulation that requires further scrutiny when it comes to the specificities of using AI in law enforcement settings is the adoption of design standards at the EU level in order to ensure the responsible and ethical use of such AI applications in the future. The design frameworks for such standards and regulations must be informed by ethics, the rule of law, and fundamental rights.[40] This presupposes the co-operation between multiple stakeholders, including technology experts and end-users, policy- and law-makers, civil society, and affected individuals. Indeed, one of the unique features of TRACE Project is that scholars with legal, social, and ethical background are working closely with technical partners, LEAs and an independent ethics advisory board in an open dialogue so as to understand and provide solutions to all the relevant issues raised by AI tools. This multidisciplinary and collaborative style of research should be encouraged for the development of AI tools. The TRACE tripartite methodology of fundamental rights sensitive design[41] can serve as a reference for the future development of AI tools for law enforcement purposes.

VI. Conclusion

AI tools have the potential to assist investigators in analysing large amounts of data quickly and accurately, allowing them to identify patterns and insights that may be significantly more difficult to discern manually. With these upsides also come downsides– revealing, thus, the need for regulation. While there are various legal instruments which could be applied to AI in law enforcement, it is essential to have a comprehensive legal framework for the development *and* use of AI systems in general, and for law enforcement specifically. To that end, further multi- and interdisciplinary research and knowledge exchange are required. The TRACE Project is a good example of this approach, which is desirable not only for the development of AI tools in compliance with the rule of law and fundamental rights, but also for instilling societal trust in AI.

---

1. The expression "follow the money" was popularised by the 1976 film "All the President's Men" that depicted the investigation into the Watergate scandal. It is used to refer to the tracing of financial transactions in order to unveil criminal activity.↩
2. Europol, "Enterprising criminals: Europe's fight against the global networks of financial and economic crime", 2021 <https://www.europol.europa.eu/publications-events/publications/enterprising-criminals-%E2%80%93-europe%E2%80%99s-fight-against-global-networks-of-financial-and-economic-crime> *accessed 4 April 2023*, p.4.↩

https://doi.org/10.30709/eucrim-2023-006

[3] P. Alldridge, “Criminal asset recovery and the pursuit of justice”, (2018) 21(1) *Journal of Money Laundering Control*, 16–32.↩

[4] For an overview of the scheduled amendments of the EU AML/CFT legal framework see <https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en> *accessed 4 April 2023*.↩

[5] Regulation (EU) 2017/1939 implementing enhanced cooperation on the establishment of the European Public Prosecutor’s Office (“the EPPO”).↩

[6] See Europol, “Internet Organised Crime Threat Assessment (IOCTA) 2021” <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021> *accessed 4 April 2023*.↩

[7] See TRACE blog posts at <https://trace-illicit-money-flows.eu/news/> *accessed 4 April 2023*.↩

[8] For more information see <https://trace-illicit-money-flows.eu/project-outcomes/> *accessed 4 April 2023*.↩

[9] 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”, COM (2021) 206 final, art. 3 (1).↩

[10] For detailed definitions and applications of AI, see U. Turksen, “Legal and Societal Impacts of Lethal Autonomous Weapons Systems (LAWS)” in: A. Aigner, H. Cremer-Schäfer and A. Pilgram (eds.), *Gesellschaft. Kritik. Ironie: Liber Amicorum für Reinhard Kreissl*, 2023, pp.167–196; J.D. Joseph and U. Turksen, “Harnessing AI for Due Diligence in CBI Programmes: Legal and Ethical Challenges”, (2022) 4 (2) *Journal of Ethics and Legal Technologies*, 3–25.↩

[11] T. Wischmeyer and T. Rademacher (eds.), *Regulating Artificial Intelligence*, 2020, paras. 5–6.↩

[12] Department for Business, Energy and Industrial Strategy, “Industrial Strategy: Building a Britain for the future” <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf/> *accessed 4 April 2023*, p.37.↩

[13] Communication from the Commission, “Artificial Intelligence for Europe”, COM/2018/237 final, p.1.↩

[14] See AI HLEG, “A definition of AI: Main capabilities and disciplines. Definition developed for the purpose of AI HLEG’s deliverables” (2019) <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf/> accessed 4 April 2023; *id*, “Ethics Guidelines for Trustworthy AI” (2019), <https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai/> *accessed 4 April 2023*.↩

[15] Following the adoption of the Council’s common position (general approach) on the EU AIA, the definition of the term “AI system” reads: “a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts”.↩

[16] Regulation (EU) 2016/679 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), art. 1.↩

[17] N. Geslevich Packin and Y. Lev-Aretz, “Learning algorithms and discrimination”, in: W. Barfield and U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence*, 2018, pp. 88–94.↩

[18] See S. Greenstein, “Preserving the rule of law in the era of artificial intelligence (AI)” (2022) 30 *Artificial Intelligence and Law*, 291–323; A. Sachoulidou, “Going beyond the ‘common suspects’: to be presumed innocent in the era of algorithms, big data and artificial intelligence” (2023) *Artificial Intelligence and Law*, <https://link.springer.com/article/10.1007/s10506-023-09347-w#Sec4/> *accessed 4 April 2023*.↩

[19] See, for instance, B.D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter and L. Floridi, “The ethics of algorithms: Mapping the debate” (2016) 3(2) *Big Data & Society*, 1–12.↩

[20] See European Agency for Fundamental Rights (FRA), “Bias in Algorithms – Artificial Intelligence and Discrimination” (2022) <https://fra.europa.eu/en/publication/2022/bias-algorithm/> *accessed 4 April 2023*, pp.29–48.↩

[21] Cf. M. Oswald, J. Grace, S. Urwin and G.C. Barnes, “Algorithmic risk assessment policing models: lessons from the Durham HART model and ‘experimental’ proportionality” (2018) 27(2) *Information & Communication Technologies Law*, 223–250.↩

[22] See F. Palmiotto, “The black box on trial: The impact of algorithmic opacity on fair trial rights in criminal proceedings”, in: M. Ebers and M. Cantero Gamito (eds.), *Algorithmic governance and governance of algorithms*, 2018, pp.49–70; A. Sachoulidou, *op. cit.* (n. 18).↩

[23] See European Parliament, “Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters”, 2020/2021(INI) <https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html/> *accessed 4 April 2023*.↩

[24] See G.G. Fuster, “Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights” (2020), <https://www.europarl.europa.eu/thinktank/en/document/IPOLSTU(2020)656295> *accessed 4 April 2023*.↩

[25] These include the targeted search for specific potential victims of crime, the prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or of a terrorist attack, or the detection, localisation, identification, or prosecution of those involved in the offences listed in art. 2 (2) of the Council Framework Decision 2002/584/JHA (European Arrest Warrant) and punishable with at least three years’ imprisonment.↩

[26] See S. Gless, “AI in the courtroom: a comparative analysis of machine evidence in criminal trials” (2020) 51(2) *Georgetown Journal of International Law*, 195–253.↩

[27] Cf. European Police Chiefs, “Joint Declaration on the AI Act” (2022), <https://www.europol.europa.eu/cms/sites/default/files/documents/EPC%20Joint-Declaration%20on%20the%20AI%20Act.pdf/> *accessed 4 April 2023*, p.1.↩

[28] Council, “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 - Presidency compromise text”, 14278/21, <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf/> *accessed 4 April 2023*; “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 - Second Presidency compromise text”, 11124/22, <https://data.consilium.europa.eu/doc/document/ST-11124-2022-INIT/en/pdf/> *accessed 4 April 2023*; “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 - Presidency third compromise text (Articles 1-29, Annexes I-IV)” 12206/1/22, <https://data.consilium.europa.eu/doc/document/ST-12206-2022-REV-1/en/pdf/> *accessed 4 April 2023*; “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 Fourth Presidency compromise text”, 13102/22, <https://data.consilium.europa.eu/doc/document/ST-13102-2022-INIT/en/pdf/> *accessed 4 April 2023*; “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 (25 November 2022)", Interinstitutional file: 2021/0106 (COD) <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/> *accessed 4 April 2023*.↩

29. Directive (EU) 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 offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.↩
30. See P. De Hert and V. Papakonstantinou, "The new Police and Criminal Justice Data Protection Directive" (2016) 7(1) *New Journal of European Criminal Law*, 7–19; J. Sajfert and T. Quintel, "Data Protection Directive (EU) 2016/680 for police and criminal justice authorities", in: M. Cole and F. Boehm (eds.) *GDPR Commentary*, 2018; L. Drechsler, "Comparing LED and GDPR Adequacy: One Standard Two Systems", (2020) 1(2) *Global Privacy Law Review*, 93–103.↩
31. De Hert and Papakonstantinou, *op. cit.* (n. 30), 9, 11–12.↩
32. T. Wischmeyer and T. Rademacher (eds.), *op. cit.* (n. 11).↩
33. N. Geslevich Packin and Y. Lev-Aretz, *op. cit.* (n. 17).↩
34. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union.↩
35. Cf. FRA, "Getting the future right – Artificial intelligence and fundamental rights" (2020), <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights/> *accessed 4 April 2023*, p.7.↩
36. See A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, 2022, pp. 12–13.↩
37. See, for instance, Directive 2012/13/EU on the right to information in criminal proceedings; Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings.↩
38. Cf. the changes undertaken in the formulations of the so-called essential requirements in Council, 'General Approach' *op. cit.* (n. 28).↩
39. Cf. A. Mantelero, *op. cit.* (n. 36), pp. 2–3.↩
40. See AI HLEG, *op. cit.* (n. 14), p.21; K. Yeung, A. Howes and G. Pogrebna, "AI Governance by Human Rights–Centered Design, Deliberation, and Oversight: An End to Ethics Washing", in: M. Dubber, F. Pasquale and S. Das (eds.), *The Oxford Hand-book of Ethics of AI*, 2020, pp. 76–106.↩
41. See E. Aizenberg and J. van den Hoven, "Designing for human rights in AI" (2020) *Big Data & Society*, 1–14.↩

* Authors statement

Research for this article is part of the TRACE Project (https://trace-illicit-money-flows.eu) which received funding from the EU Horizon 2020 Research & Innovation Programme under Grant Agreement No. 101022004.

COPYRIGHT/DISCLAIMER

Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For 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.

https://doi.org/10.30709/eucrim-2023-006

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

https://doi.org/10.30709/eucrim-2023-006