AI and Ethics
https://doi.org/10.1007/s43681-024-00560-0

ORIGINAL RESEARCH

Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: the ALIGNER Fundamental Rights Impact Assessment

Donatella Casaburo[1,2] · **Irina Marsh**[3,4]

Received: 30 May 2024 / Accepted: 21 August 2024

Abstract
Artificial intelligence systems can expand the capabilities and enhance the efficiency of law enforcement agencies preventing, investigating, detecting, and prosecuting criminal offences in the European Union. At the same time, the deployment of artificial intelligence in the security domain often raises numerous legal and ethical concerns. The ALIGNER Fundamental Rights Impact Assessment is an operational tool, rooted in fundamental rights and in the principles of AI ethics, ready to be integrated in the AI governance measures of European law enforcement agencies to inform their decision-making processes and ensure compliance with the recently adopted Artificial Intelligence Act. This paper first introduces the main tensions between law enforcement AI and fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union; then, it gives an overview of the main developments and best practices in AI governance and their relationship with fundamental rights as well as AI ethics; and finally, it describes the structure of the ALIGNER Fundamental Rights Impact Assessment.

Keywords Artificial intelligence · Fundamental rights · Ethics · Governance · AI act · Trustworthiness

1 Introduction

Artificial intelligence (AI) systems can incredibly expand the operational capabilities of law enforcements agencies (LEAs) and enhance their efficiency, by collecting, analysing, and using a vast amount of data from multiple sources.

Based on their functionalities [38], law enforcement AI can be grouped into four main categories: (1) *exploration* systems, e.g., autonomous patrolling; (2) *recognition* systems, e.g., biometric identification; (3) *communication* systems, e.g., chatbots; and (4) *prediction and analysis* systems, e.g., digital forensics [30]. LEAs can deploy these four categories of AI to fulfil the most diverse duties imposed upon them by the law, including crime prevention, investigation, detection and prosecution – activities collectively referred to as 'law enforcement purposes'.

Surprisingly, empirical research on the use of law enforcement AI in Europe reveals a *status quo* that clashes with the positive impact that the AI systems can have on LEAs' operational capabilities [32]. Between May and August 2022, the H2020 project ALIGNER ran an online survey among practitioners and professionals working in the field of law enforcement and policing to further understand the capability enhancement needs of European LEAs. The survey results show how the majority of the participants (52%) either does not use AI at all in their work (22% of participants) or uses it to very little extent (30% of participants). Among the reasons leading to such a limited use of AI, only 24% of the participants indicated the existence of institutional and technical challenges such as a low level of digitalisation of the LEA, complex procurement procedures, or lack of adequate training data. The other 76% of the participants broadly mentioned societal-, law-, and

✉ Donatella Casaburo
donatella.casaburo@kuleuven.be

1 Centre for IT & IP Law, KU Leuven, Leuven, Belgium

2 imec, Leuven, Belgium

3 CBRNE Ltd, Tenterden, UK

4 National School of Political Science and Public Administration, Bucharest, Romania

Published online: 02 September 2024

ethics-related challenges, with 49% of the participants referring to fundamental rights and ethical constraints.

The concerns expressed by the surveyed LEAs are more than justified: the use of AI systems in the security and law enforcement domains raises numerous legal and ethical concerns that are commonly underlined by policy-makers, scholars, practitioners, and civil society organizations [12, 27]. To ensure both full fundamental rights compliance and trustworthiness of the AI systems they wish to deploy, LEAs must first adequately assess and address these two sets of concerns. With this aim, the research conducted in the framework of the ALIGNER project provides LEAs with an operational impact assessment methodology that incorporates the requirements of both fundamental rights and of AI ethics, as recognised and reconstructed in the European Union (EU).

This paper first introduces the main tensions between law enforcement AI and the fundamental rights enshrined in the Charter of Fundamental Rights of the EU (Sect. 2.). Then, it gives an overview of the main AI governance measures in the EU and highlights their necessary relationship with EU fundamental rights and AI ethics (Sect. 3.). Finally, it describes the structure of the ALIGNER Fundamental Rights Impact Assessment (Sect. 4.) and paves the way forward in ensuring fundamental rights compliance and trustworthiness of AI systems deployed in the European law enforcement domain (Sect. 5.).

2 Law enforcement AI and fundamental rights: the main tensions

Article 2 of the Treaty on European Union states how "[*t*]*he Union is founded on the values of respect for human dignity*, *freedom*, *democracy*, *equality*, *the rule of law and respect for human rights*, *including the rights of persons belonging to minorities*" [15]. Article 6 of the same Treaty further identifies the Charter of Fundamental Rights of the EU (the Charter) [16] as the cornerstone legal framework for the protection of fundamental rights in the EU. The Charter recognises and safeguards a wide array of fundamental rights and freedoms, including personal, civic, political, economic, and social rights. These fundamental rights are closely intertwined in such a way that they are all interdependent and indivisible [15, 20].

Since 2009, the fundamental rights and principles enshrined in the Charter are legally binding for each and every EU Member State [15]. However, the protection granted to the Charter rights is not absolute and can be subjected to limitations. Pursuant to Article 52 of the Charter, interferences and limitations on the exercise of the recognised rights and freedoms can be justified if they: (1) are provided for by the law; (2) respect the essence of the same rights and freedoms; (3) genuinely meet the objectives of general interest recognised by the EU or need to protect the rights and freedom of others; and (4) are proportionate. According to the Court of Justice of the European Union (CJEU), a fundamental objective of general interest, such as that of crime prevention, investigation, detection and prosecution, is not sufficient in itself to justify an interference with other recognised rights, but it is always necessary to verify the legality and proportionality of the interference, as well as to evaluate the adverse effect on the protected rights [4].

AI systems can have unintended effects, leading to breaches of individuals' fundamental rights [12, 25]. Law enforcement AI can have an even more significant impact on fundamental rights and freedoms: the area of law enforcement in itself is highly sensitive, as it touches upon the "*very heart of the relation between individuals and public authorities*" [27].

Due to their interdependency and indivisibility, law enforcement AI can virtually affect all the fundamental rights and freedoms enshrined in the Charter [27]. The following sections illustrate some of the tensions between AI systems deployed for law enforcement purposes and those fundamental rights most likely to be affected.

a. **Presumption of innocence and right to an effective remedy and to a fair trial**.

Chapter VI of the Charter, '*Justice*', confers various basic procedural rights upon accused persons in criminal proceedings, to guarantee the fairness of the trial. Article 48(1) of the Charter safeguards the presumption of innocence, a guiding principle of criminal justice requiring that a person charged with a criminal offence is presumed innocent until proven guilty by a court [19]. Accordingly, the burden of proof is placed on the prosecution, who needs to demonstrate the guilt of the accused beyond reasonable doubt. Directive (EU) 2016/343 further strengthens this cornerstone safeguard, by extending its scope of application to suspected persons [17]. As a consequence, the presumption of innocence applies to all the stages of the criminal proceeding, including the pre-trial investigations conducted by LEAs.

Article 47(1) of the Charter grants the right to seek effective redress before a tribunal to everyone whose rights and freedoms guaranteed by the EU law have been violated. The right to an effective remedy is a core expression of the rule of law and, by safeguarding the access to justice, constitutes a reaffirmation of the principle of effective judicial protection [24]. The Charter does not further define the requirements of an 'effective remedy'. According to the CJEU, EU Member States can discretionarily lay down the procedural

rules governing the actions for safeguarding the rights guaranteed by the EU law, as long as these rules do not render practically impossible or excessively difficult the exercise of the protected rights [8, 9].

Finally, Article 47(2) of the Charter safeguards the right to a fair trial, namely the right to access to an independent and impartial tribunal previously established by the law, in a fair and public hearing and within a reasonable time. According to the CJEU, to qualify as a 'tribunal' for the purposes of the Article, a body needs to be established by law, be permanent, have compulsory jurisdiction, include an *inter-partes* procedure, apply rules of law and be independent and impartial [6]. The CJEU has further detailed the notions of 'independence' and 'impartiality'. The requirement of independence relates to the structure of the tribunal, which needs to act as a third party in relation to both administrative authorities and the parties to the proceeding [7]. The requirement of impartiality is an individual characteristic of the tribunal, which needs to be unbiased when determining disputes [24]. However, accessing to an independent and impartial tribunal is not per se sufficient to ensure the fairness of the hearing, as the proceeding also needs to uphold the principle of 'equality of arms' between the parties. The principle aims to ensure that each party can effectively participate to the proceeding and have a reasonable opportunity to present their case, and includes the right to have knowledge and comment on all evidence, the right to have sufficient time to familiarise with the evidence and the right to produce additional evidence [24].

Law enforcement AI can cause two main types of serious interferences with the abovementioned 'due process' rights [27]. First, AI systems may unduly interfere with the decision-making process of both LEAs and the judiciary, especially if used to sort individuals into categories and to assess their risk of (re-)committing crimes (e.g., predictive policing tools). For instance, those individuals who are scrutinised, profiled, and then labelled as '(potential) criminals' may be subjected to investigations, questioning and incrimination in absence of a reasonable suspicion [26]. While this may not lead to a direct shift of the burden of proof upon the suspect or accused individuals, it may still oblige them to have to prove the inaccuracy of the AI system's output, thus undermining the presumption of innocence as safeguarded by Directive (EU) 2016/343 [37]. Moreover, an uncritical overreliance on AI systems may also weaken the impartiality of the tribunal, thus undermining the fairness of the trial, as defined by Article 47(2) of the Charter.

Second, AI systems may negatively affect the participation of subjected individuals to court proceedings. As the AI decision-making process often lacks sufficient traceability and explainability, individuals may not be able to obtain the necessary information to adequately challenge the AI-assisted evidence or decisions of both LEAs and the judiciary. This knowledge asymmetry between parties may violate the principle of equality of arms in the proceeding and undermine the overall fairness of the trial, as defined by Article 47(2) of the Charter [25].

b. **Right to equality and non-discrimination**.

Chapter III of the Charter, '*Equity*', contains several provisions conjugating the right to equality for different categories of people and in different contexts. Article 20 of the Charter enshrines the general principle of 'equality before the law', which requires that comparable situations must not be treated differently, and different situations must not be treated in the same way [5]. The Article is complemented, as *lex specialis*, by Article 21 of the Charter, which explicitly prohibits discriminations focused upon those perceived or personal characteristics that often create inequalities [36]. These 'protected grounds' are: sex; race; colour; ethnic or social origin; genetic features; language; religion or belief; political or any other opinion; membership of a national minority; property; birth; disability; age; or sexual orientation [16].

Since it is most deployed to profile and categorise, law enforcement AI may create serious interferences with the rights to equality and non-discrimination [21]. AI systems may be 'biased', meaning that they can deviate from a standard [10]. Biases in AI systems can be of different types and come from different sources: the training or input data used may be of poor quality or incomplete; the focus of the algorithm may deviate from the standard; the algorithmic processing in itself may deviate from the standard; the algorithm may unduly be applied outside of its intended contexts; or the algorithm's output may be misinterpreted by the user or by a broader AI system [10]. While biased AI systems do not necessarily generate discriminatory results, they may still either lead to an unjustified unfavourable treatment or reinforce and systematically exacerbate already existing discriminations, especially towards minorities or vulnerable groups [18]. This is particularly relevant in the case of law enforcement AI, where AI systems heavily rely on historical crime data. Due to both the under- and over-reporting of certain crimes and human errors and biases, historical crime data do not represent accurately enough the criminality landscape, but rather provide a partial record of LEAs' activities [21, 26]. As a consequence, if the AI-based unfavourable treatment relies on prohibited grounds and is not adequately justified, law enforcement AI can violate the rights to equality and non-discrimination as safeguarded by Articles 20 and 21 of the Charter.

c. **Freedom of expression and information**.

Chapter II of the Charter, '*Freedoms'*, enshrines the classical civil, political, educational and property rights. Among these, Article 11 of the Charter particularly safeguards the freedom of expression, a foundation of a democratic society. As conceived by the Charter, the freedom of expression includes the right to hold opinions and to (not) express them, without inferences by public authorities. Rather, EU Member States are subjected to the positive obligation to adopt measures to protect and stimulate a favourable environment for a pluralistic debate [36]. Moreover, the freedom of expression includes the right to receive information, a necessary precondition for forming, holding, and expressing an opinion [17].

Law enforcement AI can create severe chilling effects on the exercise of the freedom of expression, especially when used for untargeted surveillance. The awareness of being watched by facial recognition systems deployed in public areas, as well as of being monitored by AI systems retaining and analysing telecommunications and social media data deprive individuals of their 'group anonymity' [22, 27]. This may discourage individuals from lawfully expressing their opinions, particularly if minority ones, and may lead to a change in their behaviour that violates the freedom of expression, as protected by Article 11 of the Charter.

d. **Right to respect for private life and right to protection of personal data**.

Contained in Chapter II, '*Freedoms*', Article 7 of the Charter protects from unjustified interferences four different interests: private life, family life, home, and communications. Of particular importance is the right to respect for private life, which stretches beyond the traditional concept of 'privacy', by also encompassing various aspects of the personal and social identity, such as the physical and psychological integrity and autonomy [21, 36]. Article 7 of the Charter is often read by the CJEU in conjunction with the following Article 8, which lays down the right to the protection of personal data. In EU law, persona data is any information relating to an identified or (directly or indirectly) identifiable natural person [14]. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of personal identification, data concerning health, sex life or sexual orientation form special categories of personal data, frequently referred to as 'sensitive data' [14]. Article 8 of the Charter establishes an elaborated system of check and balances to ensure the lawfulness of the personal data processing, which is further complemented and detailed by the EU secondary legislation [36]. The processing of personal data for law enforcement purposes is regulated by Directive (EU) 2016/680, the 'Law Enforcement Directive' ('LED') [14].

Article 8 of the LED establishes the conditions rendering the processing lawful. While consent has little relevance in a law enforcement context, LEAs are obliged to process personal data only if and to the extent that the processing is necessary for the performance of their duties, as entrusted by the EU or national legislation. Pursuant to Article 10 of the LED, LEAs can process sensitive data only where strictly necessary, subject to appropriate safeguards, and only where authorised by law, to protect the vital interest of individuals, or where the data was manifestly made public by the data subject. Under the LED, data subjects have limited rights. Pursuant to Articles 14 and 15 of the LED, data subjects have the right to know whether their personal data are being processed and to access to the data, unless this would obstruct ongoing investigations or otherwise prejudice the prevention, detection, or prosecution of criminal offences. Pursuant to Article 16 of the LED, data subjects have the right to obtain from LEAs the rectification or the completion of inaccurate or incomplete personal data relating to them, as well as to obtain the erasure of their personal data where the processing is unlawful or does not uphold the data protection principles. Finally, pursuant to Article 11 of the LED, data subjects have the right to not be subjected to a decision based solely on automated processing, including profiling, which produces an adverse legal effect or similarly significantly affects them. When authorised by law, automated individual decision-making is possible, insofar as it allows human intervention by LEA-practitioners [14].

The relationship between law enforcement AI and the right to respect for private life, as safeguarded by Article 7 of the Charter, is characterised by fundamental tensions that, if unjustified or unproportionate, can lead to infringements. First, similarly to what is considered above for the freedom of expression (see Sect. 2.c.), surveillance systems deployed by LEAs may severely hinder the individuals' right to freely develop their personal and social identity [21]. Moreover, AI systems relying on vast amount of (repurposed) data from various sources, especially if used for profiling and categorising individuals, may generate further personal data that predict, infer, or reveal otherwise unknown or undisclosed information about individuals, even without their awareness [21, 24].

Likewise, the right to protection of personal data and its declinations, protected by Article 8 of the Charter and the LED, are particularly challenged by law enforcement AI. First, ensuring full compliance with the strict lawfulness conditions set by Article 8 of the LED may be particularly burdensome for LEAs: being impossible to rely on more flexible legal bases (e.g., consent or legitimate

interest), the processing of each personal data needs to find its legal basis in an explicit EU or national legal provision, however vast the amount of data may be. The same type of difficulty stands, a *fortiori*, when the processing involves sensitive data, for which Article 10 of the LED establishes even stricter lawfulness criteria. Second, guaranteeing the quality, accuracy and completeness of the personal data demanded by Article 4(1)(d) of the LED may be almost impossible when the personal data processed by the AI system are biased and inherently incomplete historical data (see Sect. 2.b.). Finally, risk assessments, profiling algorithms and predictive policing tools are difficult to reconcile with Article 11 of the LED, for two main reasons. The first is related to the data subject's right to obtain human intervention: a meaningful human intervention by LEAs-practitioners cannot only be limited to signing-off the AI-based decision, but requires the authority and competence to change the decision [21]. However, research demonstrates how humans tend to overrule AI-based decisions mainly when not in line with their stereotypes, which often leads to discriminatory outcomes [21]. The second reason is related to the prohibition of discrimination on the basis of sensitive data: in principle, sensitive data can be used to profile individuals only insofar as there are reasonable grounds for suspicion [23]. While this is already particularly difficult to ensure when the AI system processes vast amount of data, it becomes impossible in the case of untargeted processing.

3 AI governance

As AI permeates various aspects of the law enforcement domain, concerns regarding its governance have become increasingly pertinent. In this section, we delve into the multifaceted landscape of AI governance, focusing specifically on the intersection with ethics and fundamental rights.

While ethics plays a significant role in shaping our understanding of the 'big issues in AI', it is not inherently designed as a governance framework. AI ethics is a multidisciplinary field seeking to establish a set of values, principles and accepted standards of right and wrong to guide the moral conduct in the development and use of AI technologies [31]. However, the absence of agreed vocabulary and consensual understanding often limits the practical application of ethics in addressing the complex implications of AI. Therefore, alternative and more practical approaches are necessary to guide AI development and deployment effectively [35]. To this aim, AI ethics needs to be translated into AI governance, namely "*a system of rules*, *practices*, *processes*, *and technological tools that are employed to ensure an organization's use of AI technologies aligns with the organization's strategies*, *objectives*, *and values; fulfills legal requirements; and meets principles of ethical AI followed by the organization*" [33].

Supranational fundamental rights legislation, including the EU Charter of Fundamental Rights, is explicitly designed to identify and protect against 'individual and societal harms' and, thus, offers a concrete basis for approaching algorithmic accountability and AI governance [34]. Integrating the EU Charter of Fundamental Rights into AI governance frameworks brings two main benefits: (1) identifying and assessing harm on the basis of substantive rights of near universal recognition; and (2) defining mechanisms and processes to determine whether an AI-assisted or -enabled activity constitutes a lawful interference with fundamental rights or an unlawful violation [35]. Thus, a fundamental rights-based approach can serve as an organising framework, capable of incorporating other approaches, including the ethical and technical ones [35]. Importantly, by building on existing legal obligations, the fundamental rights enshrined in the Charter can inform all stages of the (law enforcement) AI lifecycle, from the design and development to the deployment, by guiding processes and decision-making, as well as providing a route to remedy and accountability.

The EU Independent High-Level Expert Group on Artificial Intelligence adopted the same approach when proposing the Ethics Guidelines for Trustworthy AI [28]. Based on the three pillars of the EU, namely fundamental rights, democracy and the rule of law, the Ethics Guidelines highlight that AI should not be an end in itself but should rather serve as a means to improve human welfare and freedom. To achieve this aim, trustworthiness is identified as a key concept in the development and deployment of AI systems. The risks raised by AI systems must be duly recognised and proportionately addressed to prevent a loss of trust and guarantee that societies will develop, deploy, and use trustworthy AI. According to the Ethics Guidelines, trustworthy AI should be:

- *lawful*, namely it should respect all applicable laws and regulations;
- *ethical*, namely it should respect ethical principles and values; and
- *robust* both from a technical and social perspective.

Based on fundamental rights and ethical principles such as the respect for human autonomy, prevention of harm, fairness and explicability, the Ethics Guidelines put forward a set of seven key requirements for trustworthy AI systems, which now constitute the foundation of AI ethics and governance in the EU and are universally recognised in the United Nations Educational, Scientific and Cultural Organization's

Recommendation on the Ethics of Artificial Intelligence [39]. These key requirements are:

- *Human agency and oversight*. AI systems need to empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured and can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.
- *Technical robustness and safety*. AI systems need to be resilient and secure. They need to be safe, ensuring a fall back plan in case of adversarial attacks or other unexpected situations Their output needs to be accurate, reliable and reproducible. This ensures that also unintentional harm can be minimised and prevented.
- *Privacy and data governance*. Besides ensuring full compliance with the rights to privacy and data protection, AI systems need to be subjected to adequate data governance mechanisms, taking into account the quality and integrity of the data, and ensuring legitimised access to data.
- *Transparency*. AI systems, the data processed and related business models need to be transparent and traceable. The decision-making process and the outcome of AI systems and their decisions need to be explainable in a manner adapted to the concerned stakeholder. Humans need to be aware that they are interacting with AI systems, and need to be informed of their capabilities and limitations.
- *Diversity*, *non-discrimination and fairness*. Unfair biases in AI systems need to be avoided, as they could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems need to be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire lifecycle.
- *Societal and environmental well-being*. AI systems need to benefit all human beings, including future generations. Hence, they need to be sustainable and environmentally friendly. Moreover, their social and societal impact need to be carefully considered.
- *Accountability*. AI systems need to embed mechanisms to ensure responsibility and accountability for their activity and outcomes. AI systems, the data processed and related business models need to be evaluated, to minimise negative impacts. Eventual trade-offs among key requirements need to be documented and continually reviewed. When unjust negative impacts verify, adequate redress needs to be ensured.

At the supranational level, the EU adopted in May 2024 its Artificial Intelligence Act (AI Act), the first legal framework addressing the risks created by AI systems [13]. By categorising law enforcement AI applications as either prohibited or high-risk, the AI Act establishes binding governance obligations for LEAs providing or deploying AI substantiating in the implementation of risk management systems, *ex ante* conformity assessments and fundamental rights impact assessments. Additionally, the EU Agency for Law Enforcement Cooperation (Europol) published in 2022 the blueprint of an accountability framework for AI in the internal security domain, as part of a project to guide law enforcement on the use of AI [1]. Finally, in 2024, the International Criminal Police Organization (INTERPOL) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), with support of the EU, released an updated version of their Toolkit for Responsible AI Innovation in Law Enforcement, which includes a Risk Assessment Questionnaire aiming to identify and evaluate the risks that may emerge in relation to the four 'principles for responsible AI innovation': lawfulness, minimisation of harm, human autonomy and fairness [29].

Often, LEAs already have in place policies and procedures to address a variety of legal and ethical issues arising in operational contexts. New policies and procedures specifically addressing the risks likely to arise from the use of AI systems need to be created, when necessary, to complement the existing ones. In that vein, the following guidelines need to be taken into account [40]:

- Create a governance system by combining flexible and adaptable policy guidelines and soft law (i.e. quasi-legal instruments) with hard law.
- Promote fundamental rights, ethical, and societal impact assessments of the deployed AI systems based on an operational setting.
- Establish a functional accountability of ethical process and designate a responsible figure (e.g. Institutional Ethics Board, Ethics Officer).
- Deploy the technologies that demonstrate enhanced security and diminished negative fundamental rights, ethical and other societal implications – compared with other possible technological solutions or available technologies.
- Comply with the adequate regulation, control, and licensing regime to prevent AI systems being misused outside a given jurisdiction, and contrary to established fundamental rights and ethical standards.
- Educate and raise awareness among law enforcement professionals regarding the fundamental rights, ethical and societal issues of using AI systems.

- Seek advice from external experts, as properly addressing fundamental rights and ethical concerns requires a depth of knowledge that cannot realistically be expected from LEA-decision-makers and operational planners.

4 The ALIGNER Fundamental Rights Impact Assessment[1]

Pursuant to Article 27 of the EU AI Act, LEAs deploying AI for law enforcement purposes will need to further reinforce their governance policies and procedures, by conducting a fundamental rights impact assessment of each of the AI systems used for law enforcement purposes [13]. Fundamental rights impact assessments are essential tools to ensure compliance of law enforcement AI with the fundamental rights of subjected individuals, as they allow LEAs to identify the risks to those rights likely to be affected, as well as mitigation measures.

">Despite the existence of several methodologies or templates to carry out fundamental rights impact assessments of AI systems in general, the topic of fundamental rights impact assessments specifically targeted at law enforcement AI remains underexplored in the existing state-of-the-art. To facilitate compliance with the AI Act, the H2020 project ALIGNER released its ALIGNER Fundamental Rights Impact Assessment (AFRIA), an operational tool rooted in fundamental rights and implementing the principles and requirements of AI ethics [28], as recognised and reconstructed in the EU [2]. The AFRIA is a reflective exercise, addressed to LEAs deploying law enforcement AI systems in the EU and conceived to be integrated in their already existing AI governance policies and procedures as a complementary tool to the other types of assessments mandated by the relevant legal framework (e.g., data protection impact assessments [14], AI risk management systems and *ex ante* conformity assessments [13]).">

An iteration of the AFRIA assesses a single AI system deployed by LEAs for a single law enforcement purpose or connected law enforcement purposes (e.g., detection and prosecution of criminal offences). It is of paramount importance for LEAs to always perform the AFRIA in relation to the AI system's pre-determined purposes and circumstances of use, including: trigger conditions; time and frequency of use; subjected individuals and/or groups, as well as geographical areas. In line with Article 27 of the AI Act, LEAs need to carry out an AFRIA prior to the first use of the AI system, to assist informed and reasoned decisions on the conditions of deployment. Then, LEAs need to review and update the AFRIA throughout the entire AI lifecycle, to reflect and record eventual significant changes in the functioning of the AI system or in its deployment. To more efficiently perform the AFRIA, LEAs should establish a diverse and multidisciplinary team, including legal, technical, and operational expertise.">

The preliminary information on the AI system assessed, its purposes and circumstances of use, and the team responsible for conducting its assessment is summarised in the AFRIA as shown in Fig. 1 below.

For instance, in the case of a predictive policing tool predicting the risk of a natural person committing a criminal offence, the preliminary table may be filled in as shown in Fig. 2 below.

LEAs can perform the AFRIA by relying on two connected templates: the Fundamental Rights Impact Assessment (Sect. 4.a.) and the AI System Governance (Sect. 4.b.).

a. **Fundamental Rights Impact Assessment**.

The Fundamental Rights Impact Assessment template enables LEAs to identify and evaluate the specific risks of harm likely to impact the enjoyment of the fundamental

ALIGNER Fundamental Rights Impact Assessment	
Name	
Organisation/Position	
Date	
Contributors	
AI system assessed	
Detailed description of the technology and input data	
Detailed description of the purposes and circumstances of use, including the categories of natural persons or groups affected	
Geographical area of use	
Time and frequency of use	

Fig. 1 Preliminary information in AFRIA

[1] Some paragraphs of this section are an expansion and update of the following report: Casaburo, D., Marsh, I.: ALIGNER D4.2: methods and guidelines for ethical & law assessment [2]

ALIGNER Fundamental Rights Impact Assessment	
Name	Jane Doe
Organisation/Position	Legal Officer at EU Law Enforcement Agency
Date	July 2024
Contributors	John Doe (Technical Officer at EU Law Enforcement Agency), Jane Smith (Police Officer at EU Law Enforcement Agency)
AI system assessed	XYZ
Detailed description of the technology and input data	The AI system is trained by relying on historical crime data, including criminal evidence, records and circumstantial information, as well as open source intelligence collected by the EU Law Enforcement Agency. The AI system identifies patterns and correlations and, ultimately, profiles natural persons by predicting the risk level of commiting a criminal offence.
Detailed description of the purposes and circumstances of use, including the categories of natural persons or groups affected	The AI system is used to prevent future crimes in the jurisdiction of the EU Law Enforcement Agency. It is planned to be used in relation to all residents of pre-defined geographical locations.
Greographical area of use	The geographical locations are pre-defined on the basis of available heat maps and include Region Y and Region Z under the jurisdiction of the EU Law Enforcement Agency.
Time and frequency of use	The AI system is planned to be used 24/7 for a period of a year, renewable in case of positive performance evaluation.

Fig. 2 Example of preliminary information in AFRIA

1. Presumption of innocence and right to an effective remedy and to a fair trial Everyone charged with a criminal offence must be presumed innocent until proved guilty according to law. Everyone whose rights and freedoms are violated has the right to an effective remedy before a tribunal. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law, including rights: ❖ to be informed promptly of the nature and cause of the accusation; ❖ to bring their arguments and evidence as well as scrutinise and counteract the evidence presented against them; and to obtain an adequately reasoned and accessible decision.		
Challenge	Evaluation	Estimated risk level
1.1 The AI system does not communicate that a decision/advice or outcome is the result of an algorithmic decision		-
1.2 The AI system does not provide percentages or other indication on the degree of likelihood that the outcome is correct/incorrect, prejudicing the user that there is no possibility of error and therefore that the outcome is undoubtedly incriminating		-
1.3 The AI system produces an outcome that forces a reversal of burden of proof upon the suspect, by presenting itself as an absolute truth, practically depriving the defence of any chance to counter it		-
1.4 There is no explanation of reasons and criteria behind a certain output of the AI system that the user can understand		-
1.5 There is no indication of the extent to which the AI system influences the overall decision-making process		-
1.6 There is no set of measures that allow for redress in case of the occurrence of any harm or adverse impact		-

Fig. 3 Section of Fundamental Rights Impact Assessment template

rights of the subjected individuals. In line with the theoretical framework analysed above in Sect. 2., the template is divided in four sections focusing on those fundamental rights most likely to be impacted by law enforcement AI: the presumption of innocence and right to an effective remedy and to a fair trial; the right to equality and non-discrimination; the freedom of expression and information; and the right to respect for private life and right to protection of personal data.

As shown in Fig. 3 below, a template section first contains a short description of the relevant fundamental right, as reconstructed by the Charter.

Then, the template section is divided in three columns. The first column, titled 'challenge', includes a non-exhaustive list of some characteristics that, if implemented in the AI system, may negatively impact the relevant fundamental right of the subjected (groups of) individuals. To reduce the risk of acquiescence biases while performing the AFRIA, when possible, the challenges are formulated in a negative form (e.g., "*The AI system does not/There is no…*").

The second column, titled 'evaluation', needs to be filled by LEAs to precise to what extent and how the challenges listed in the first column apply to the AI system assessed. When LEAs conclude that some of the listed challenges do not apply to the AI system assessed, they need to adequately justify and record their reasoning.

The third and last column, titled 'estimated risk level', needs to be filled by LEAs by relying on a risk matrix (see Sect. 4.b.i.).

For instance, in the case of a predictive policing tool predicting the risk of a natural person committing a criminal offence, the first section of the Fundamental Rights Impact Assessment template may be filled in as shown in Fig. 4 below.

1. Presumption of innocence and right to an effective remedy and to a fair trial Everyone charged with a criminal offence must be presumed innocent until proved guilty according to law. Everyone whose rights and freedoms are violated has the right to an effective remedy before a tribunal. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law, including rights: ❖ to be informed promptly of the nature and cause of the accusation; ❖ to bring their arguments and evidence as well as scrutinise and counteract the evidence presented against them; and to obtain an adequately reasoned and accessible decision.		
Challenge	Evaluation	Estimated risk level
1.1 The AI system does not communicate that a decision/advice or outcome is the result of an algorithmic decision	The AI system communicates that the outcome is the result of an algorithmic decision only in case the risk of the assessed natural person offending equals to or overcomes the threshold of 70%, while the communication is omitted in case of risk level below 70%	Limited
1.2 The AI system does not provide percentages or other indication on the degree of likelihood that the outcome is correct/incorrect, prejudicing the user that there is no possibility of error and therefore that the outcome is undoubtedly incriminating	The AI system does not communicate the confidence score of the output and/or of the algorithm and is impossible for the user to establish it	Serious
1.3 The AI system produces an outcome that forces a reversal of burden of proof upon the suspect, by presenting itself as an absolute truth, practically depriving the defence of any chance to counter it	When the AI system flags that the risk of the assessed natural person offending overcomes the threshold of 70%, an investigation against them is immediately started, even in absence of other evidence incriminating them	Critical
1.4 There is no explanation of reasons and criteria behind a certain output of the AI system that the user can understand	The AI system does not communicate neither the criteria nor the data leading to the output and the users cannot understand them with any other means	Critical
1.5 There is no indication of the extent to which the AI system influences the overall decision-making process	The weight of the output of the AI system in the overall decision-making process is not specifically evaluated	Serious
1.6 There is no set of measures that allow for redress in case of the occurrence of any harm or adverse impact	The subjected natural person can seek redress only in court, if and when an official trial starts	Critical

Fig. 4 Example of section of Fundamental Rights Impact Assessment template

i. **Risk matrix**.

While estimating the level of the risks created by the AI systems assessed, LEAs need to weigh up two different dimensions: (1) the *impact* of the risk, namely the level of severity of the prejudice experienced by the affected individuals; and (2) the *likelihood* of the risk, namely the level of probability of the risk occurring. The risk matrix shown in Fig. 5 below helps LEAs estimate and visualise the risk.

In the risk matrix, the impact level of the risk ranges between:

1. *Insignificant*, if the affected individuals will experience no consequences if the risk occurs;
2. *Minor*, if the affected individuals will experience little consequences if the risk occurs;
3. *Moderate*, if the affected individuals will experience a prejudice if the risk occurs;
4. *Major*, if the affected individuals will experience a significant prejudice if the risk occurs; and.
5. *Extreme*, if the affected individuals will experience a significantly detrimental prejudice if the risk occurs.

The likelihood level of the risk ranges between:

1. *Rare*, if the risk may occur only in exceptional circumstances;
2. *Unlikely*, if the risk may occur at some time, but probably will not;
3. *Possible*, if the risk may occur at some time, and probably will;
4. *Likely*, if the risk will probably occur in most or many circumstances; and.
5. *Almost certain*, if the risk will occur in many or most circumstances.

Based on their estimations, LEAs find the overall risk level in the square where the estimated impact level and the estimated likelihood level meet. The overall risk level ranges between: (1) *Low*; (2) *Limited*; (3) *Serious*; and (4) *Critical*.

b. **AI System Governance**.

The AI System Governance template enables LEAs to mitigate the specific risks of harm impacting the enjoyment of the fundamental rights of the subjected individuals already identified and evaluated through the Fundamental Rights Impact Assessment template (Sect. 4.a.). The template is divided in seven sections implementing and further operationalising the 7 key requirements for trustworthy AI identified by the High-Level Expert Group on AI: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; accountability [28] (Sect. 3).

As shown in Fig. 6 below, a template section is divided in seven groups of columns.

Impact	Likelihood: Rare	Unlikely	Possible	Likely	Almost Certain
Extreme	Limited	Serious	Critical	Critical	Critical
Major	Limited	Serious	Serious	Critical	Critical
Moderate	Low	Limited	Serious	Serious	Critical
Minor	Low	Limited	Limited	Serious	Serious
Insignificant	Low	Low	Low	Limited	Limited

Fig. 5 Risk matrix

1. Human autonomy								
Component	Minimum standards to be achieved	Initial risk estimate: Challenge no.	Initial risk estimate: Risk level	Additional mitigation measures implemented	Final assessment: Final estimated risk level	Final assessment: Further actions	Responsible department	Timeline
Human agency	The task allocation between the AI system and the user allows meaningful interactions	[1.2]	-					
		[1.5]	-					
	There are procedures to describe the level of human involvement and the moments for human interventions	[1.5]	-					
		[2.2]	-					
		[4.1]	-					
Human oversight	The AI system does not affect human autonomy by interfering with the user decision-making process	[1.2]	-					
		[1.3]	-					
		[1.5]	-					
		[4.1]	-					
	There are mechanisms to prevent overconfidence or over-reliance in the results offered by the AI system	[1.1]	-					
		[1.2]	-					
	There are mechanisms to detect and correct wrong outputs	[1.6]	-					
		[2.2]	-					
		[2.3]	-					
	There are mechanisms to safely abort an entire operation when needed							

Fig. 6 Section of AI System Governance template

1. Human autonomy								
Component	Minimum standards to be achieved	Initial risk estimate		Additional mitigation measures implemented	Final assessment		Responsible department	Timeline
		Challenge no.	Risk level		Final estimated risk level	Further actions		
Human agency	The task allocation between the AI system and the user allows meaningful interactions	[1.2]	Serious	The AI system communicates the confidence score of the output, so that an informed decision on the follow-up actions is possible	Low	N/A	Technical department	dec/24
		[1.5]	Serious	The deployer can play an active role in the decision-making process, by modifying the parameters informing the decision of the AI system	Limited	Implementing a mechanism to allow the user to add new parameters informing the decision of the AI system	Legal and technical departments	mar/25
	There are procedures to describe the level of human involvement and the moments for human interventions	[1.5]	Serious	The weight of the output of the AI system in the decision-making processes of the organisation is concretely evaluated. The results are made known to the deployers, who are tasked to take an informed decision on the follow-up actions	Low	N/A	Legal and technical departments	mar/25
		[2.2]	Serious	Deployers can flag the poor performance of the AI system and this triggers an evaluation from the technical department	Limited	Establishing a framework for periodical performance evaluation	Technical department	dec/24
		[4.1]	Limited	A data protection impact assessment is performed yearly	Low	N/A	Legal and technical departments	dec/24

Fig. 7 Example of section of AI System Governance template

The first column, titled 'component', decomposes the considered key requirement into sub-requirements, namely necessary building blocks further substantiating the key requirement's content.

For each sub-requirement, the second column, titled 'minimum standards to be achieved', includes a non-exhaustive lists of governance measures that LEAs should strive to implement to enhance the trustworthiness of the deployed AI system.

When a minimum standard is suitable to mitigate the risks to fundamental rights identified and estimated in the Fundamental Rights Impact Assessment template (Sect. 4.a.), the third group of columns, titled 'initial risk estimate', automatically connects the standard with (at least) one challenge and its estimated risk level.

The fourth column, titled 'additional mitigation measures implemented', needs to be filled by LEAs to further precise if and how the minimum standard is (or will be) implemented in their AI governance policies and procedures. If the minimum standard is suitable to mitigate the already identified and estimated risks to fundamental rights, LEAs also need to explain how the standard is (or will be) reducing the severity or the likelihood of the connected risks.

When a minimum standard is (or will be) mitigating the connected risks, in the fifth group of columns, titled 'final assessment', LEAs need to use the same risk matrix described above (Sect. 4.b.i.) to estimate the final level of the identified risks to fundamental rights, after the implementation of additional mitigation measures. LEAs can also record further actions suitable to improve the implementation of the minimum standard and the mitigation of risks.

The sixth and seventh columns, titled 'responsible department' and 'timeline', need to be filled by LEAs to specify which department of the organisation is responsible for the implementation of the minimum standards and additional mitigation measures and their estimated timeline of adoption.

For instance, in the case of a predictive policing tool predicting the risk of a natural person committing a criminal offence, the first section of the AI System Governance template may be filled in as shown in Fig. 7 below.

5 Conclusion

AI systems can enhance the capabilities of LEAs to prevent, investigate, detect, and prosecute crime (Sect. 1.). Yet, AI systems can also create serious interferences, if not limitations to or violations of, the fundamental rights of subjected individuals, as enshrined in the EU Charter of Fundamental Rights (Sect. 2.). Recent developments in the field of law enforcement AI governance (Sect. 3.), such as the Accountability Principles for Artificial Intelligence drafted by Europol [1] and the Toolkit for Responsible AI Innovation in Law Enforcement released by INTERPOL and UNICRI [29], can support European LEAs by enhancing

their understanding of the fundamental rights and ethical challenges of deploying law enforcement AI. In particular, INTERPOL and UNICRI's Risk Assessment Questionnaire can assist LEAs in identifying and evaluating the risks that may emerge in relation to four ethical principles [29]. However, neither the Accountability Principles for Artificial Intelligence nor the Risk Assessment Questionnaire were designed to assist EU LEAs in performing a fundamental rights impact assessment of their law enforcement AI systems, as prescribed by Article 27 of the EU AI Act [13]: while the former instrument lacks the necessary operationality, the latter does not exhaustively address fundamental rights-related risks and does not provide sufficient guidance on the measures to be taken in case of materialisation of the evaluated ethical risks.

Following the adoption of the final text of the AI Act, the AFRIA templates have been revised to implement all the necessary components of fundamental rights impact assessments, as established by Article 27 of the AI Act. Moreover, by implementing the requirements for trustworthy AI set by the EU AI Ethics [28], the AFRIA templates are in line with the current standardisation work of the European Standards Organisations CEN-CENELEC [3], as requested by the European Commission in 2023 [11]. Finally, the AFRIA templates have been validated through a series of interactive workshop sessions and conference presentations, during which law enforcement practitioners, AI developers, researchers, legal and ethical experts, and civil society representatives provided extensive feedback on its methodology, completeness, and usability [2].

In sum, as explained above in Sect. 4., the AFRIA templates stimulate LEAs to:

- Through the table summarising preliminary information (see Sect. 4.), describe the processes and frequency in which the assessed law enforcement AI system is planned to be used, as well as the categories of subjected individuals likely to be affected (Article 27(1)(a) to (c) of the AI Act);
- Through the Fundamental Rights Impact Assessment template (see Sect. 4.a.), identify and evaluate the specific risks of harm likely to impact the subjected individuals (Article 27(1)(d) of the AI Act); and
- Through the AI System Governance template (see Sect. 4.b.), identify measures to mitigate the evaluated risks of harm likely to impact the subjected individuals (Article 27(1)(f) of the AI Act), as well as describe possible human oversight measures (Article 27(1)(e) of the AI Act).

In absence of a harmonised and law enforcement-dedicated template developed by the AI Office [13], the AFRIA currently remains the only instrument specifically addressing the peculiarities of law enforcement AI and that can be immediately integrated in the EU LEAs' AI governance policies and procedures to enhance their compliance with fundamental rights, ethical principles and the newly established legal obligation of conducting a fundamental rights impact assessment of high-risk AI systems.

Acknowledgements The authors thank Dr. Lindsay Clutterbuck and Dr. Richard Warnes for their input on the risk matrix.

Funding This research has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 101020574.

Declarations

Conflict of interest The authors have no other financial or non-financial interests to disclose.

References

1. Akhgar, B., Bayerl, P.S., Bailey, K., Dennis, R., Gibson, H., Heyes, S., Lyle, A., Raven, A., Sampson, F.: Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. (2022). https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf Accessed 20 May 2024
2. Casaburo, D., Marsh, I.: ALIGNER D4.2: Methods and guidelines for ethical & law assessment. (2023). https://aligner-h2020.eu/wp-content/uploads/ALIGNER-D4.2-Methods-and-guidelines-for-ethical-law-assessment-v20230324-FINAL.pdf Accessed 20 February 2024
3. CEN-CENELEC JTC 21: Business Plan for JTC 21. (2022). https://standards.cencenelec.eu/BPCEN/2916257.pdf Accessed 29 July 2024
4. Court of Justice of the European Union: Judgement of the Court (Grand Chamber) in Joined Cases C-293 and C-594/12. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. (2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293 Accessed 19 January 2024
5. Court of Justice of the European Union: Judgement of the Court (Third Chamber) in Case C-21/10. Károly Nagy v Mezőgazdasági és Vidékfejlesztési Hivatal. (2011). https://eur-lex.europa.

eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0021 Accessed 23 January 2024
6. Court of Justice of the European Union: Judgement of the Court in Case C-54/96. Dorsch Consult Ingenieurgesellschaft mbH v Bundesbaugesellschaft Berlin mbH. (1997). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1427395815954&uri=CELEX:61996CJ0054 Accessed 22 January 2024
7. Court of Justice of the European Union: Judgement of the Court in Case C/24/92. Pierre Corbiau v Administration des contributions. (1993). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1427397368851&uri=CELEX:61992CJ0024 Accessed 22 January 2024
8. Court of Justice of the European Union: Judgement of the Court in Case 179/84. Piercarlo Bozzetti v Invernizzi SpA and Ministero del Tesoro. (1985). https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:61984CJ0179 Accessed 22 January 2024
9. Court of Justice of the European Union: Judgement of the Court in Case C 33–76. Rewe-Zentralfinanz eG et Rewe-Zentral AG v Landwirtschaftskammer für das Saarland. (1976). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61976CJ0033 Accessed 22 January 2024
10. Danks, D., London, A.J.: Algorithmic Bias in Autonomous Systems. In Sierra, C. (ed.) Proceedings of the 26th International Joint Conference on Artificial Intelligence, pp. 4691–4697. AAAI Press, Melbourne (2017)
11. European Commission: Commission implementing decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence. (2023). https://ec.europa.eu/transparency/documents-register/api/files/C(2023)3215_0/de00000001048942?rendition=false Accessed 29 July 2024
12. European Commission: White Paper on Artificial Intelligence– A European approach to excellence and trust. (2020). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065 Accessed 18 January 2024
13. European Parliament and Council: Regulation (EU): 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). (2024). https://eur-lex.europa.eu/eli/reg/2024/1689/oj Accessed 19 July 2024
14. European Parliament and Council: Directive (EU): 2016/680 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. Official Journal of the European Union L 119/89. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 Accessed 25 January 2024
15. European Union: Consolidated Version of the Treaty on European Union: Official Journal of the European Union C 326/13. (2012). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016M%2FTXT Accessed 18 January 2024
16. European Union: Charter of Fundamental Rights of the European Union: Official Journal of the European Union C 326/391. (2012). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT Accessed 18 January 2024
17. European Parliament and Council: Directive (EU) 2016/343 of March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings. Official Journal of the European Union L 65/1. (2016). https://eur-lex.europa.eu/eli/dir/2016/343/oj Accessed 22 January 2024
18. European Union Agency for Fundamental Rights: Bias in Algorithms– Artificial Intelligence and Discrimination. Publication Office of the European Union, Luxembourg. (2022). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf Accessed 23 January 2024
19. European Union Agency for Fundamental Rights: Presumption of Innocence and Related Rights– Professional Perspectives. Publications Office of the European Union, Luxembourg. (2021). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-presumption-of-innocence_en.pdf Accessed 22 January 2024
20. European Union Agency for Fundamental Rights: What are fundamental rights? https://fra.europa.eu/en/content/what-are-fundamental-rights. Accessed 18 January 2024
21. European Union Agency for Fundamental Rights: Getting the Future Right– Artificial Intelligence and Fundamental Rights. Publications Office of the European Union, Luxembourg. (2020). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf Accessed 23 January 2024
22. European Union Agency for Fundamental Rights: Facial recognition technology: fundamental rights consideration in the context of law enforcement. Publications Office of the European Union, Luxembourg. (2019). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf Accessed 25 January 2024
23. European Union Agency for Fundamental Rights: Preventing unlawful profiling today and in the future: a guide. Publications Office of the European Union, Luxembourg. (2019). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf Accessed 25 January 2024
24. European Union Agency for Fundamental Rights and Council of Europe: Handbook on European law relating to access to justice. Publications Office of the European Union, Luxembourg. (2016). https://www.echr.coe.int/documents/d/echr/handbook_access_justice_eng Accessed 22 January 2024
25. Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence: A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. (2019). https://rm.coe.int/a-study-of-the-implications-of-advanced-digital-technologies-including/168096bdab Accessed 23 January 2024
26. Fair, T.: Automating injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe. (2021). https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf Accessed 22 January 2024
27. González Fuster, G.: Artificial Intelligence and Law Enforcement– Impact on Fundamental Rights. Policy Department for Citizens' Rights and Constitutional Affairs– Directorate-General for Internal Policies. (2020). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf Accessed 18 January 2024
28. Independent High-Level Expert Group on Artificial Intelligence: Ethics Guidelines for Trustworthy AI. (2019). https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 Accessed 20 February 2024
29. INTERPOL, U.N.I.C.R.I.: Toolkit for Responsible AI Innovation in Law Enforcement. (2024). https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit Accessed 20 May 2024
30. INTERPOL: UNICRI: Artificial Intelligence and Robotics for Law Enforcement. (2019). https://unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf Accessed 17 January 2024

31. Leslie, D.: Understanding Artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. Alan Turing Inst. (2019). https://doi.org/10.5281/zenodo.3240529
32. Lückerath, D., Wischott, V., Casaburo, D., Clutterbuck, L., Svenmarck, P., Westmann, T.: ALIGNER D5.5: First Update of the Research Roadmap for AI in Support of Law Enforcement and Policing. (2023). https://aligner-h2020.eu/wp-content/uploads/ALIGNER_D5.5_ResearchRoadmap_v2_20230331-FINAL.pdf Accessed 17 January 2024
33. Mantymaki, M., Minkkine, M., Birkstedt, T., Viljanen, M.: Defining organizational AI governance. AI Ethics. (2022). https://doi.org/10.1007/s43681-022-00143-x
34. McGregor, L., Murray, D., Ng, V.: International Human rights Law as a Framework for algorithmic accountability. Int. Comp. Law Q. (2019). https://doi.org/10.1017/S0020589319000046
35. Murray, D.: Using Human rights Law to inform States' decisions to deploy AI. Am. J. Int. Law. (2020). https://doi.org/10.1017/aju.2020.30
36. Peers, S., Hervey, T., Kenner, J., Ward, A. (eds.): The EU Charter of Fundamental Rights: A Commentary. Hart Publishing, London (2014)
37. Sachoulidou, A.: Going beyond the common suspects: To be presumed innocent in the era of algorithms, big data and artificial intelligence. Artif. Intell. Law. (2023). https://doi.org/10.1007/s10506-023-09347-w
38. Thanos, K.-G., Sinni, M., Kyriazanos, D.: popAI D2.1: Functionality taxonomy and emerging practices and trends. (2023). https://www.pop-ai.eu/wp-content/uploads/2023/07/D2_1_revised.pdf Accessed 17 January 2024
39. UNESCO: Recommendation on the Ethics of Artificial Intelligence. (2021). https://unesdoc.unesco.org/ark:/48223/pf0000381137 Accessed 12 August 2024
40. Vogiatzoglou, P., Quezada Tavárez, K., Marquenie, T., Royer, S., Marsh, I.: MAGNETO D9.4: Final Ethical and Legal Assessment (2021). https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5dc894f63&appId=PPGMS Accessed 20 May 2024