ALIGNER

ALIGNER D4.1

State-of-the-art reports on ethics & law aspects in Law Enforcement and Artificial Intelligence

Deliverable No.	D4.1
Work Package	WP4
Dissemination Level	PU
Author(s)	Ezgi Eren (KU Leuven) Donatella Casaburo (KU Leuven) Plixavra Vogiatzoglou (KU Leuven)
Due date	2022-06-30
Actual submission date	2022-07-14
Status	Final
Revision	1.0
Reviewed by	Irina Marsh (CBRNE)

This document has been prepared in the framework of the European project ALIGNER – Artificial Intelligence Roadmap for Policing and Law Enforcement. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101020574.

Contact:

info@aligner-h2020.eu
www.aligner-h2020.eu

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

Executive Summary

The European Commission-funded Coordination and Support Action ALIGNER: Artificial Intelligence Roadmap for Policing and Law Enforcement brings together European actors concerned with Artificial Intelligence, Law Enforcement, and Policing to collectively identify and discuss needs for paving the way for a more secure Europe in which Artificial Intelligence supports law enforcement agencies while simultaneously empowering, benefiting, and protecting the public.

This deliverable is the first output of ALIGNER Work Package 4 – Ethics & Law. It has the preliminarily aim of identifying the relevant legal and ethical frameworks, as well as the best practices and guidelines for the use of AI tools in the police and law enforcement sector. To this end, D4.1 specifically addresses the instruments adopted to date by the Council of Europe and the European Union and systematise the existing knowledge, while also building a common understanding of the relevant ethical and legal challenges relating to issues further examined by other ALIGNER Work Packages. The findings of this deliverable are, then, the starting point for the following tasks of Work Package 4.

Table of contents

EXECUTIVE SUMMARY **3**

TABLE OF CONTENTS **4**

LIST OF ABBREVIATIONS **6**

INTRODUCTION **8**

GENDER STATEMENT 9
RELATION TO OTHER DELIVERABLES 9
STRUCTURE OF THIS REPORT 10

1 KEY FRAMEWORKS RELATING TO AI IN POLICING **11**

2 ETHICAL FRAMEWORK **12**

2.2 COUNCIL OF EUROPE 12
2.2.1 European Ethical Charter on the use of artificial intelligence in judicial systems and their environment 12
2.2.2 Works of the Ad Hoc Committee on Artificial Intelligence (CAHAI) and the Committee on Artificial Intelligence (CAI) 14
2.2.3 Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems (8 April 2020) 14
2.2.4 Resolution 2342 (2020) on Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems 15
2.3 EUROPEAN UNION 17
2.3.1 High Level Expert Group on Artificial Intelligence (AI HLEG) – Ethics Guidelines for Trustworthy AI 17
2.3.2 European Commission – White Paper on Artificial Intelligence 23

3 LEGAL FRAMEWORK **25**

3.1 HUMAN RIGHTS RELEVANT FOR THE USE OF AI SYSTEMS BY LEAS 25
3.1.1 Right to a fair trial (ECHR Art. 6) and the right to an effective remedy (Charter Art. 47) 25
3.1.2 Presumption of innocence (ECHR Art 6(2)) and the right to defence (ECHR Art. 6.2, Charter Art. 48) 30
3.1.3 Freedom of expression and information (ECHR Art. 10, Charter Art. 11) 32
3.1.4 The right to equality and non-discrimination (ECHR Art 14, Charter Art 20 & 21, the International Convention on the Elimination of All Forms of Racial Discrimination (CERD)) 33
3.1.5 The right to respect for private and family life (ECHR Art. 8, Charter Art. 7 and 52) and the right to protection of personal data (Charter Art. 8) 36
3.2 SECONDARY LEGISLATION 41
3.2.1 Privacy and data protection legislation 42
3.2.1.1 Law Enforcement Directive (LED) *42*
i. Scope of application and definitions *42*
ii. Key actors: controllers and processors *45*
iii. Data protection principles *47*
iv. Rights of the data subject *51*
v. Automated decision-making and profiling *52*
vi. Data protection impact assessment *53*
3.2.1.2 ePrivacy Directive & ePrivacy Regulation *54*
3.2.1.3 Legal framework on the collaboration between LEAs and EU Agencies *55*
3.2.1.4 Relevant CoE privacy and data protection instruments *57*

3.2.2 The Regulation on the Free Flow of Non-Personal Data 60
3.2.3 EU Directives concerning the procedural rights of the suspected and accused persons 61
3.2.4 AI Act Proposal 62
i. Scope of application 62
ii. Risk-based approach 63
iii. Current developments and criticisms towards the proposal 68
3.2.5 Lawfulness of evidence 69
i. Divergent national laws and lack of an EU level harmonising regulation 70
ii. Admissibility of evidence 71

CONCLUSION 76

4 BIBLIOGRAPHY 77

4.1 LEGISLATION 77
4.2 JURISPRUDENCE 79
4.3 REFERENCES 80

List of Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
AI HLEG	High Level Expert Group on Artificial Intelligence
CAHAI	CoE Ad Hoc Committee on Artificial Intelligence
CEPEJ	European Commission for the Efficiency of Justice
CERD	The International Convention on the elimination of all forms of Racial Discrimination
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPIA	Data protection impact assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EPPO	European Public Prosecutor's Office
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
FRA	European Union Agency for Fundamental Rights
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

LED	Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive)
NPDR	Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union
ODR	Online Dispute Resolution
TEU	Treaty on European Union
TFEU	Treaty on Functioning of the European Union

Introduction

Traditionally, an algorithm is a "*sequence of computational steps that transform the input into the output*"[1] which aims to reach a specific outcome or solve a certain problem.[2] Algorithms are the building blocks of all complex computing methods, including technologies based on artificial intelligence (AI) and machine learning.[3]

'Artificial intelligence' is often defined as a software equipped with the capacity to act purposefully; in other words, AI is a software designed to take a specific action to achieve a given goal, by dealing effectively with its environment.[4] Machine learning is a particular subset of AI-technologies, where the system improves automatically its performance of a task ('learns') by gaining experience, after being fed by training datasets.[5]

The quick pace of developments in computing and the increasing availability of big data as a result of datafication surrounding everyday actions, allowed the AI-based technologies to quickly gain popularity. While many technologies marketed as revolutionary AI are merely snake oil,[6] riding the hype wave and playing to exaggerated expectations, many others have substantial potential and could significantly enhance the operational capabilities of entities acting both in the private and public sectors.

Thanks to this immense potential, AI-driven tools have been continuously attracting the attention of policymakers and Law Enforcement Agencies (LEAs) alike. Many such technologies have already been adopted by European LEAs for various aspects of their activities, helping them gather[7] and analyse[8] vast amounts of data with the aim to obtain evidence and assist various decisions that they need to make.[9] Such AI-based tools are used in various LEAs' activities, such as predictive policing, smart video surveillance (for facial recognition, number plate recognition, gait recognition and pattern matching, etc.), network and targeted device surveillance, and police robotics (surveillance drones, robots used to enter dangerous locations or secure explosives, etc.[10]).

---

[1] Thomas H Cormen and others (eds), Introduction to Algorithms (3rd ed, MIT Press 2009) 5.
[2] ibid.
[3] Thomas Marquenie, 'Legal and Ethical Challenges in Algorithmic Policing and Law Enforcement AI' in Marie-Amélie Bourguignon and others (eds), Technology and society: the evolution of the legal landscape (Gompel & Svacina 2021) 98.
[4] ibid 99; Rembrandt Devillé, Nico Sergeyssels and Catherine Middag, 'Basic Concepts of AI for Legal Scholars' in Jan de Bruyne and Cedric Vanleenhove (eds), Artificial intelligence and the law (Intersentia 2021) 2.
[5] ibid 6.
[6] The term "AI snake oil" was coined by Arvind Narayanan in his talk in 2019. See Arvind Narayanan, 'How to Recognize AI Snake Oil' (2019) <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>; Frederike Kaltheuner and Arvind Narayanan, 'AI Snake Oil, Pseudoscience and Hype - an Interview with Arvind Narayanan', *Fake AI* (Meatspace Press 2021) <https://ia804607.us.archive.org/3/items/fake-ai/Fake_AI.pdf>.
[7] As an example, we can recall here 4nseek, a tool developed by the Spanish National Cybersecurity Institute, helps LEAs in investigating cases of child abuse. The tool is able to analyse storage devices and find digital traces of child sexual abuse material, also among the deleted files. See, 'INCIBE' (*INCIBE*) <https://www.incibe.es/> accessed 8 July 2022.
[8] E.g, Hansken is an investigation and research platform developed by the Dutch National Forensic Institute with the aim of storing and analysing digital traces collected on a crime scene. See, Ministerie van Justitie en Veiligheid, 'Home - Forensischinstituut.nl' (27 January 2021) <https://www.forensischinstituut.nl/> accessed 8 July 2022.
[9] It is, for instance, the case of predictive policing tools, which are further analysed in Section 3.1.2 of this work.
[10] Marquenie (n 3) 101.

AI-driven tools can be quite beneficial for LEAs, however, they also raise numerous legal and ethical concerns. It has been observed in many cases how they can result in significant harm through discriminatory decisions, compounded by the lack of explainability of how these decisions are made as well as the lack of clarity concerning who should be held accountable and bear the legal responsibility in case of harm resulting from the use of these tools. Therefore, it is crucial to assess the potential risks that may arise from the use of these technologies within the scope of LEAs' activities, and identify methods and best practices to prevent harm, well before the said technologies are developed and deployed in practice.

The H2020 project ALIGNER brings together European practitioners from law enforcement and policing, civil society, policymaking, research, and industry with the objective of discussing opportunities, challenges, needs, and risks emerging from the use of AI technologies in the law enforcement field. The outcome of these discussions will be systematised in an AI research and policy roadmap, meeting the operational, cooperative, and collaborative needs of LEAs.[11] In this context, Work Package 4 – Ethics & Law aims to set up and maintain a systematic ethics and law assessment process for (novel) AI solutions with potential for enhancement of the LEAs' work. To this end, this first deliverable has the preliminary objective of identifying the relevant legal and ethical frameworks, as well as the best practices and guidelines concerning the use of AI tools by LEAs.

Gender Statement

The ALIGNER's WP4 – Ethics & Law deliverables aim to support a wide array of stakeholders (public, private, and third sector). ALIGNER is fully committed to a balanced participation and gender equality in all aspects of the project, including a balanced representation of men and women in management, research, dialogue, dissemination, advisory board, and outreach activities, as well as in work package / task leadership.

Every effort is being made to monitor gender equality addressing biases and constraints throughout all project stages. This deliverable will be gender-proofed during the internal review process under and in accordance with a gender-proofing checklist described in Deliverable 1.2 "Project Handbook".

Relation to other deliverables

By mapping out the ethical and legal framework applicable to AI systems used in the police sector, this deliverable lays the groundwork for D4.2 on the methods and guidelines for the ethical and law assessment of the AI solutions for law enforcement.

Additionally, D4.1 contributes to the other tasks of the project, by building a common framework and understanding of the relevant ethical and legal challenges relating to issues addressed under other

[11] See 'ALIGNER' <https://aligner-h2020.eu/> accessed 8 July 2022.

WPs. Finally, the findings of this deliverable will be integrated in D5.3, namely the research roadmap for AI in support of law enforcement and policing.

Structure of this report

This document consists of three sections. The first section lays down some preliminary concepts related to the key frameworks on AI in policing. The second section outlines the relevant ethical framework, consisting of the instruments adopted by both the Council of Europe and the European Union. Finally, the third section analyses the most relevant binding pieces of legislation.

1 Key frameworks relating to AI in policing

Within Europe, the regulation of AI is governed to a large extent by international instruments adopted by the Council of Europe (CoE), as well as legal and ethical frameworks adopted at the European Union (EU) and national level.

The CoE is an intergovernmental organization established in 1949 with the aim of promoting human rights, the unity of Europe and the economic and social progress of its members. Currently, it counts 46 Contracting Parties, including the 27 Member States of the European Union. Whereas the CoE is an organisation focused on monitoring compliance with human rights, the European Union produces legislation directly binding to its Member States in a broad array of economic and political matters.

Two major human rights instruments are crucial for the development and deployment of AI technologies in policing and beyond, the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (the Charter). The ECHR was adopted by the CoE and entered into force in 1953. As for the Charter, it has become binding on the EU member states and institutions in December 2009, with the entry into force of the Treaty of Lisbon. Reflecting the values of today's societies, the Charter also sets forth 'third generation' rights, such as the right to data protection, rights pertaining to guarantees on bioethics, and the obligations of administration to ensure transparency in their actions. Although at times the ECHR and the Charter differ from each other, the Charter is applied consistently with the ECHR, especially concerning the rights that stem from it.[12]

Each of these instruments has a dedicated judicial authority which ensures that the rights enshrined in the respective instruments are protected. The European Court of Human Rights (ECtHR) undertakes this role for the ECHR and the Court of Justice of the European Union (CJEU) for the Charter. These two courts interpret the respective instruments and rights and principles therein, and their judgments become binding for their Member States. For this reason, the case-law of the ECtHR and the CJEU is crucial for the deployment of AI-based tools by police and law enforcement authorities.

Besides that, both the CoE, and even more so the EU, produce legal and ethics instruments seeking to safeguard human rights in specific fields and sectors. For instance, specific rules, ethical principles and recommendations have been developed and are currently under development primarily in the fields of personal data protection, but also in relation to due process rights, cybercrime and AI. The following sections provide an analysis of the most important ethical and legal frameworks relevant for AI in policing.

[12] 'Why Do We Need the Charter?' (*European Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en> accessed 8 July 2022.

2 Ethical Framework

With the emergence and increasing popularity of AI-based technologies, a plethora of related problems started to come into light. The inherent characteristics of AI-based technologies and tools such as their opacity, lack of explainability and biased outcomes can lead to problems in any environment they are deployed. However, AI-assisted law enforcement practices raise more questions due to their higher potential to substantially affect individuals, as well as the power imbalance between law enforcement and citizens.

In the face of these problems, ethical frameworks have been increasingly attracting more attention as they could provide a broader framework of considerations before and beyond legal rules to ensure, *inter alia*, fairer, more accountable and transparent AI-powered tools that will be deployed within the scope of LEAs' activities. This section gives an overview of the most relevant European ethical frameworks to guide the adoption and deployment of AI-assisted tools by LEAs.

2.2 Council of Europe

The CoE has been making noteworthy efforts to document and contribute to the creation of ethical frameworks to address problems that may be raised by AI-driven technologies. Its work focusing on AI includes binding and non-binding legal instruments, guidelines and recommendations,[13] as well as a mapping effort documenting AI initiatives by governments and non-governmental institutions.[14] This section will explore the most relevant works of the CoE in the context of LEAs' use of AI-driven tools.

2.2.1 European Ethical Charter on the use of artificial intelligence in judicial systems and their environment

The European Ethical Charter on the use of artificial intelligence in judicial systems and their environment[15] was adopted by the European Commission for the Efficiency of Justice (CEPEJ) in December 2018. The charter is one of the first fundamental texts in Europe concerning the use of AI technologies in judicial systems. Importantly, it lays down five ethical principles that should be adhered to in judicial systems and their environment, followed by a more specific examination of the use of certain technologies in the field of justice. The five ethical principles that are set forth in the charter are the following:

PRINCIPLE OF RESPECT OF FUNDAMENTAL RIGHTS – Throughout their design and implementation phases, AI technologies should respect the fundamental rights guaranteed by the ECHR and by Convention 108+.[16] These technologies should not undermine the right to access to the judge and the right to a

[13] 'Council of Europe's Work in Progress' <https://www.coe.int/en/web/artificial-intelligence/work-in-progress> accessed 8 July 2022.
[14] 'AI Initiatives' <https://www.coe.int/en/web/artificial-intelligence/national-initiatives> accessed 8 July 2022.
[15] European Commission for the Efficiency of Justice (CEPEJ), 'European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment' <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> accessed 8 July 2022.
[16] For a detailed exploration of these instruments, see Section 3.1 and Section 3.2.1.4.

fair trial, in a manner to safeguard the principle of equality of arms and respect for the adversarial process.[17] Judges' independence and the rule of law shall be respected. These principles should be implemented into the AI technologies from the design stage.[18]

PRINCIPLE OF NON-DISCRIMINATION – AI technologies should not create any discrimination, exacerbate the existing discriminations between individuals or groups of individuals, or lead to deterministic analyses. More caution is advised when 'sensitive data'[19] are used in this process and if any discrimination is determined relating to such information, then corrective measures should be adopted, effort shall be made to limit or neutralise the negative effects of such discrimination and stakeholders should be educated to strengthen the efforts to fight against it.[20]

PRINCIPLE OF QUALITY AND SECURITY – This principle focuses on the development process of the AI technologies. Accordingly, a multidisciplinary approach should be adopted and the expertise of judicial professionals such as judges, prosecutors and lawyers, as well as researchers from related disciplines should be consulted to the extent possible in the design of machine learning models. Judicial decisions and other data that are processed should come from certified sources, following a traceable process to prevent modification. The security of the models and algorithms should be ensured, in order to guarantee the integrity and intangibility of the system.[21]

PRINCIPLE OF TRANSPARENCY, IMPARTIALITY AND FAIRNESS – AI technologies may be protected by intellectual property rights. Nevertheless, these technologies may have significant impacts over individuals when used in judicial environments, and thus, it is important to ensure the transparency, impartiality, fairness and intellectual integrity (*"prioritising the interests of justice"*[22]). It is crucial to strike a balance between the protection of intellectual property rights relating to the AI technologies and the need for transparency. For this reason, data processing methods should be made accessible and understandable and external audits should be authorised.[23] This principle also indicates the possibility of certification to be granted by public authorities.

PRINCIPLE "UNDER USER CONTROL" – This principle emphasizes that AI technologies should not restrict user autonomy. Judges, prosecutors, lawyers and other professionals in the judicial environment should be able to review how the judicial decisions are reached. They should have the option to not be bound by the decision made or assisted by AI technologies. Referring to Article 6 of the ECHR, this principle states that the users of these technologies should be clearly informed when AI technologies are used before or during judicial proceedings and they should have the right to object to it.[24]

---

[17] For a detailed explanation concerning rights, see Section 3.1.1.
[18] European Commission for the Efficiency of Justice (CEPEJ) (n 15) 8.
[19] According to the Charter, sensitive data may include "alleged racial or ethnic origin, socio-economic background, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health-related data or data concerning sexual life or sexual orientation". See ibid 9.
[20] ibid.
[21] ibid 10.
[22] ibid.
[23] ibid 11.
[24] ibid 12.

The ethical charter also emphasizes the benefits of AI tools to enhance case-law and to increase access to law by individuals. It suggests caution concerning other uses such as Online Dispute Resolution (ODR), underlining the need for people who take part in ODR processes to be informed of any involvement of an AI system so that they can make informed decisions. Judge profiling and anticipation of court decisions are identified as possible areas to further research. On the other hand, profiling of individuals, especially in criminal proceedings, is identified as a problematic area of the use of AI technologies and is warned against.

2.2.2 Works of the Ad Hoc Committee on Artificial Intelligence (CAHAI) and the Committee on Artificial Intelligence (CAI)

The Ad-Hoc Committee on Artificial Intelligence (CAHAI) was mandated for the years 2019-2021 to explore a legal framework regulating the development, design and application of AI. CAHAI based its works on the standards arising from the three fundamental pillars of the CoE, namely the human rights, democracy and the rule of law. It took into account the existing legal instruments, both on the universal and regional level. Through multi-stakeholder consultations, CAHAI produced two important documents:

- Feasibility study on a legal framework on AI design, development and application based on CoE standards, adopted by the CAHAI on 17 December 2020;[25] and
- The possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law.[26]

Following the end of CAHAI's mandate in December 2021, the CoE established the Committee on Artificial Intelligence (CAI),[27] as the body responsible for drafting an international binding legal instrument on artificial intelligence, based on the CoE's standards on human rights, democracy and the rule of law. CAI's mandate will continue until 31 December 2024.

2.2.3 Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems (8 April 2020)

In its Recommendation on the human rights impacts of algorithmic systems (8 April 2020),[28] the CoE states that Member States should revise their legislative frameworks, as well as the existing policies and practices in their jurisdiction with regard to the *"procurement, design, development and ongoing deployment of algorithmic systems"*.[29] They should establish *"appropriate legislative, regulatory and*

[25] Ad Hoc Committee on Artificial Intelligence (CAHAI), 'Feasibility Study' <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> accessed 8 July 2022.
[26] Ad Hoc Committee on Artificial Intelligence (CAHAI), 'Possible Elements of a Legal Framework on Artificial Intelligence, Based on the Council of Europe's Standards on Human Rights, Democracy and the Rule of Law' <https://rm.coe.int/cahai-2021-09rev-elements/1680a6d90d> accessed 8 July 2022.
[27] See Council of Europe, 'Terms of Reference of the Committee on Artificial Intelligence (CAI)' <https://rm.coe.int/terms-of-reference-of-the-committee-on-artificial-intelligence-for-202/1680a4ee36> accessed 8 July 2022.
[28] Council of Europe, 'Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems' <https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154> accessed 8 July 2022.
[29] ibid 1.

supervisory frameworks related to algorithmic systems"[30] to ensure that the private sector complies with the applicable laws and respect individuals' fundamental rights. The Member States should make sure that these laws and regulations are duly enforced, and in order to do so, they should ensure that the national supervisory, oversight, risk assessment and enforcement authorities have the sufficient authority and resources to address any concerns, and investigate matters.[31] The recommendation states the importance of *"regular, inclusive and transparent consultation, co-operation and dialogue with all relevant stakeholders"*.[32] Moreover, according to the recommendation, the Member States should build the expertise in all institutions that take a role in development and deployment of algorithmic systems, with an aim to protect human rights[33] and inform all members of the society so that they can better understand AI technologies and make informed decisions.[34] Significantly, the recommendation also urges the Member States to consider the environmental impact of the development of comprehensive digital systems and to *"optimise the use and consumption of natural resources and energy"*[35] in relation to these systems. In order to guide the Member States in the implementation of these suggestions, the recommendation also includes specific guidelines in its appendix.

2.2.4 Resolution 2342 (2020) on Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems

The resolution titled *"Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems"* (Resolution 2342 (2020))[36] was adopted by CoE's Parliamentary Assembly on 22 October 2020. It specifically targets policing and criminal justice systems, as opposed to many other more general guidelines and recommendations. The resolution identifies five core ethical principles, which the Parliamentary Assembly deems to be universally accepted and applicable:

- transparency, including accessibility and explicability;
- justice and fairness, including non-discrimination;
- human responsibility for decisions, including liability and the availability of remedies;
- safety and security; and
- privacy and data protection.

The resolution refers to "*facial recognition, predictive policing, the identification of potential victims of crime, risk assessment in decision-making on remand, sentencing and parole, and identification of 'cold cases' that could now be solved using modern forensic technology*"[37] as potential applications of AI

[30] ibid 3.
[31] ibid 4.
[32] ibid 5.
[33] ibid 6.
[34] ibid 7.
[35] ibid 8.
[36] Parliamentary Assembly of the Council of Europe, 'Justice by Algorithm – The Role of Artificial Intelligence in Policing and Criminal Justice Systems (Resolution 2342 (2020))' <https://pace.coe.int/en/files/28805/html> accessed 8 July 2022.
[37] ibid 6.

technologies by LEAs. One of the problems concerning the use of these technologies is that their use may at times clash with the five core ethical principles. For instance,

- AI technologies may be protected by intellectual property rights and this may allow the developers to reject third parties access to the source code. As a result, individuals who use and are subject to the use of an AI system may not understand how it operates, even on a very basic level, leading to significant transparency concerns.[38]
- Lack of sources and understanding may encourage LEA users of AI technologies to rely too much on those technologies, it may cause them to hesitate objecting to the decisions influenced by the AI technologies in question. In effect, this leads to the result of LEAs inadvertently deferring their responsibility for decision making.[39]
- Using the same AI systems in related but different contexts may be problematic. When AI systems are developed by using certain data coming from a certain use case, and then the same system is subsequently used for a related but different context, the outcomes may reflect the biases coming from the first use case to the second use case. Such uses may lead to unexpected negative impacts, which are challenging to identify in advance.[40] Similarly, including AI components to previously existing technologies may cause unforeseen problems.[41]

After identifying these potential issues, the Parliamentary Assembly encourages the Member States to adopt national legal frameworks directed to the use of AI and use the five ethical principles as a starting point. Significantly, it suggests establishing a registry for all AI applications used in the public sector, and underlines the need for all public authorities to have the internal expertise needed to independently evaluate and advise on the introduction, operation and impact of AI systems.

As a side note, the Recommendation 2182 (2020)[42] which accompanies the above mentioned resolution states that the lack of a harmonized regulatory framework, in other words *"a regulatory patchwork"* where each country adopts different standards, could give rise to *"ethics shopping"*.[43] Accordingly, this would encourage the AI developers to shift their activities to the regions where the ethical standards are lower. Taking this risk into account, the Parliamentary Assembly emphasizes the impact on human rights that the use of AI in policing and criminal justice may cause.[44] This statement can be interpreted as the Parliamentary Assembly's call to ensure that regulatory frameworks are rather harmonized and provide a similar level of protection of human rights and fundamental freedoms across jurisdictions.

---

[38] ibid 7.1.
[39] ibid 7.3.
[40] ibid 7.5.
[41] ibid 7.6.
[42] Parliamentary Assembly of the Council of Europe, 'Justice by Algorithm – The Role of Artificial Intelligence in Policing and Criminal Justice Systems (Recommendation 2182 (2020))' <https://pace.coe.int/en/files/28806/html> accessed 8 July 2022.
[43] ibid 2.
[44] For a more detailed explanation concerning the rationale behind both to the Resolution 2342 (2020) and Recommendation 2182 (2020), see the Explanatory Memorandum by the rapporteur Mr Boriss Cilevics, Boriss CILEVIČS, 'Justice by Algorithm – the Role of Artificial Intelligence in Policing and Criminal Justice Systems (Report - Doc. 15156)' 6 <https://pace.coe.int/en/files/28723/html> accessed 8 July 2022.

2.3 European Union

The EU's approach to AI has a double focus: obtaining excellence in AI and securing a trustworthy AI.[45] It aims to support innovation and rapid development in AI technologies, while also ensuring that the functioning of markets, the public sector, the individuals' safety and their fundamental rights will not be negatively impacted. The EU's AI strategy[46] guides its vision and efforts on various levels to effectively address the ethical concerns arising in relation to AI technologies.

The most influential of the EU's ongoing ethics-focused efforts are the Ethics Guidelines for Trustworthy AI, produced by the High Level Expert Group on Artificial Intelligence (AI HLEG) [Section 2.3.1] and the subsequent White Paper on Artificial Intelligence [Section 2.3.2] published by the European Commission. These instruments have propelled the EU as one of the leading actors in the regulation of AI, and guided the principles underlying the AI Act Proposal, which will be the first European binding legal instrument regulating AI.[47] This section addresses these two ethical instruments.

2.3.1 High Level Expert Group on Artificial Intelligence (AI HLEG) – Ethics Guidelines for Trustworthy AI

The European Commission established the High Level Expert Group on Artificial Intelligence (AI HLEG) with the aim of receiving specific guidance concerning its future AI strategies. Until the end of its mandate in July 2020, the AI HLEG produced four influential deliverables,[48] which have guided AI-related policymaking efforts of not only the European Commission but also of other EU institutions, as well as Member States. The AI HLEG's Ethics Guidelines for Trustworthy AI deliverable is examined in this section, as it is closely related to the activities of ALIGNER and the AI-driven tools that will be identified in this scope.

ETHICS GUIDELINES FOR TRUSTWORTHY AI[49] – Based on the three pillars of the EU, namely fundamental rights, democracy and the rule of law, the Ethics Guidelines for Trustworthy AI establish that AI should not be an end in itself but should rather serve as a means to improve human welfare and freedom. In order 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 recognized and addressed proportionately

[45] European Commission, 'A European Approach to Artificial Intelligence | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 8 July 2022.
[46] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe (COM/2018/237 Final)' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> accessed 8 July 2022.
[47] For a detailed examination of the AI Act, see Section 3.2.4.
[48] The AI HLEG's four deliverables are: the Ethics Guidelines for Trustworthy AI, the Policy and Investment Recommendations for Trustworthy AI, the final Assessment List for Trustworthy AI (ALTAI), and the Sectoral Considerations on the Policy and Investment Recommendations.
[49] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 12 July 2022.

to prevent a loss of trust and guarantee that societies will develop, deploy and use trustworthy AI systems.

The guidelines identify three key components that a trustworthy AI system should meet at all times: First, AI systems should be lawful, i.e., comply with all laws and regulations under the applicable legal framework. Second, AI systems should be ethical, in other words, they should be developed and operated in line with ethical principles and values. Third, AI systems should be robust, from both a technical and social perspective, to prevent the potential harms they may unintentionally cause. The guidelines recognizes that none of these three components are sufficient on their own to achieve a trustworthy AI: these may overlap and come into tension, so striving for a harmonious, balanced application is needed to secure trustworthy AI.

The lawfulness component, explained briefly, requires compliance with the binding rules of the European, national and International legal systems that are relevant to the development, deployment and the use of AI systems.[50] While the guidelines does not go into detail with regard to the lawfulness component, they emphasize the strict requirement to duly observe these legal frameworks.

After this brief emphasis on the lawfulness component, the guidelines place their focus on the latter two components, namely ethical and robust AI. In three chapters, the guidelines identify the ethical principles that need to be followed to secure trustworthy AI, translate them into seven key principles and finally set out concrete measures to implement them.

The seven key principles identified by the AI HLEG are 1) human agency and oversight, (2) technical robustness and safety, (3) privacy and data governance, (4) transparency, (5) diversity, non-discrimination and fairness, (6) environmental and societal well-being and (7) accountability.[51] They influenced many subsequent policy and legal approaches in Europe as well as in a global scale,[52] hence they are further explored below.

HUMAN AGENCY AND OVERSIGHT – Pursuant to the principle of respect for human autonomy, AI systems should support human autonomy and decision making. This requires AI systems to support the agency of the humans using them and foster their fundamental rights. Including human oversight into the process of decision-making by AI systems as a central element is a key factor in ensuring respect for human autonomy.

Although they have the potential to bring countless benefits, including enabling fundamental rights, AI systems are also capable of negatively affecting fundamental rights. If that is the case, an impact assessment should be conducted, prior to developing the system. Such an impact assessment should include information regarding whether it is possible to reduce these risks or whether these can be

[50] While at the moment there are no AI-specific legislations in force yet, some are in development, such as the AI Act Proposal in the EU, and there are many relevant binding rules under the European, national and international level. The most relevant of those will be explored in the next chapter concerning the legal frameworks.
[51] ibid II.
[52] One of the most important key policy documents in relation to AI, the European Commission's White Paper on AI also builds on these seven key principles. The White Paper on AI will be explored below in Section 2.3.2.

justified as necessary to respect the rights and freedoms of other individuals. There should also be an external oversight and feedback mechanisms to further assess the risks to fundamental rights.

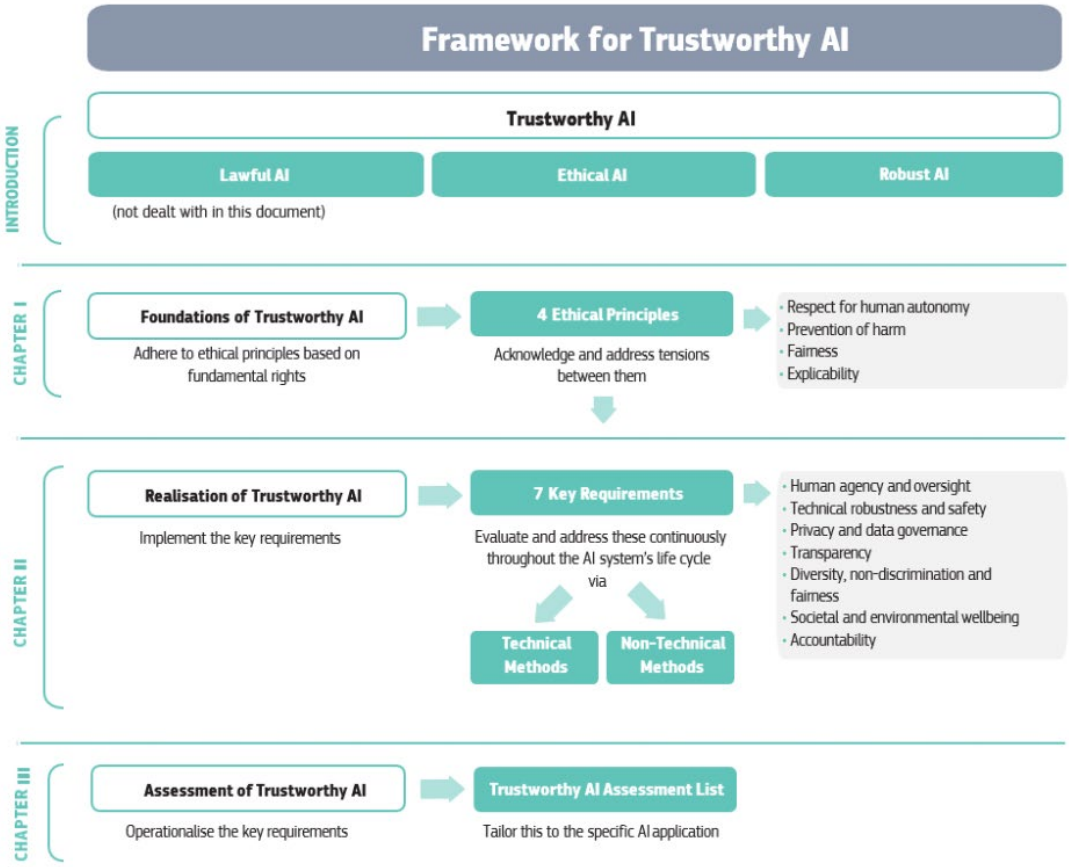

Figure 1: A graphical summary of the framework established by the Ethics Guidelines for Trustworthy AI[53]

To ensure human autonomy, the users of the AI system should be able to make informed and autonomous decisions about the system, as well as have the sufficient knowledge and the means to understand and interact with the AI. Individuals should also be able to assess and challenge the system, if needed. Due to their technical capabilities, there is a potential for AI systems to be used for manipulating human behaviour through methods that may be difficult to detect and identify. Such uses would violate the principle of human autonomy.

In line with the human autonomy principle, AI systems must respect users' right *"not to be subject to a decision solely on automated processing when this produces legal effects on or similarly significantly affects them."*[54]

With regard to human oversight, the guidelines refer to various governance mechanisms,[55] and accordingly oversight should vary in function of the other existing safety and control measures, as well

[53] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (n 49) 8.
[54] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (n 49) 16.
[55] Such as human-in-the-loop, human-on-the-loop or human-in-command approaches.

as the potential risk of the specific AI system. If the availability of human oversight options are limited, the guidelines require more extensive testing and stricter governance.[56]

TECHNICAL ROBUSTNESS AND SAFETY – The technical robustness and safety principle is explained with four main components: 1) resilience to attack and security; 2) fallback plan and general safety; 3) accuracy; and 4) reliability and reproducibility.

The guidelines link the technical robustness requirement to the principle of prevention of harm: AI systems should be developed with an aim to prevent risks, behave in a reliable manner, following the intentions of the developers and thus minimising possible unintended and unexpected harm, and completely preventing unacceptable harm.

To consider an AI system to be secure, it is necessary to take into account potential unintended applications (such as dual-use applications) and potential abuse by malicious actors, such as data-targeted attacks (data poisoning), model-targeted attacks (model leakage), or software and hardware attacks. Suitable measures must be implemented to prevent and reduce these dangers.

AI systems should also have protections that allow for a backup strategy. It must be guaranteed that the system will perform its intended function without causing harm to individuals or the environment.

In the context of the guidelines, accuracy refers to *"an AI system's ability to make correct judgments, for example to correctly classify information into the proper categories, or its ability to make correct predictions, recommendations, or decisions based on data or models".*[57] To prevent inaccurate outcomes, the guidelines recommend the adoption of an explicit development and evaluation process. When it is not possible to prevent inaccurate outcomes, it is beneficial to provide an indication of the likelihood of errors. Accuracy is especially crucial in cases where AI systems have direct consequences on human lives.

Moreover, AI systems' outcomes should be reliable and reproducible. Reliability is necessary to be able to scrutinize the system and minimise the risk of unintended harmful results. Reproducibility means that the AI mechanism should lead to the same results with the same inputs and under the same conditions, which allows third parties to accurately describe the function of an AI system.

PRIVACY AND DATA GOVERNANCE – Privacy is closely related to the prevention of harm: AI systems should protect privacy and data protection at all stages of their development, deployment and use. This includes data that is fed to an AI system, as well as the data that is generated about the users of an AI system. Accordingly, the quality and the integrity of the data must be ensured. The safeguard of privacy and data protection is even more critical considering the potential risks of unfair and unlawful discrimination presented by certain AI systems. Lastly, an organisation that manages personal data should establish protocols to regulate data access, which should include information about the

[56] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (n 49) 16.
[57] ibid 17.

conditions to allow data access. Only specific personnel who are qualified to access the data and who actually needs them for their role should be granted access.

TRANSPARENCY – The transparency requirement is strongly related to the principle of explicability and involves the transparency of the data, the system, and the business models important to an AI system. The guidelines explain this requirement with three distinct characteristics, namely traceability, explainability and communication.

Traceability requires a detailed documentation of the datasets and the processes leading to the AI system's decision, as well as of the resulting decisions. The goal behind such documentation is to be able to identify the reasons behind the errors made by the AI system, and therefore to improve its decision-making in the future.

Explainability refers to the ability to explain various components of an AI system, including the technical processes and the decisions made by humans which had a relevant effect on the algorithm. Due to the inherent characteristics of AI systems, in many cases, enhancing a system's explainability may lead to reducing its accuracy and vice versa. An appropriate balance must be struck depending on the possible impacts of the AI.

Due to the communication component of transparency, people must be provided with the right to know whether they are interacting with an AI system. They should have the possibility to opt for an interaction with a human instead of an AI application. Finally, people interacting with an AI system should be clearly and appropriately informed about its capabilities and limitations.

DIVERSITY, NON-DISCRIMINATION AND FAIRNESS – There is always a risk that the data used in the training and operation of AI systems may include historic biases, may be incomplete and the AI system may be inadvertently designed in a manner to provide biased and discriminatory outputs. This could lead to unintended direct or indirect discrimination against certain people or groups of people and could ultimately contribute to the prejudice and marginalisation they already suffer from. The guidelines underline the need to avoid identifiable and discriminatory biases, in the stage where data are collected. Oversight mechanisms should be established to analyse and resolve potential biases in the design and programming of the AI systems.

To ensure accessibility and universal design, the guidelines suggest that the AI systems shall be designed to allow everyone to use them, whatever their age, gender, abilities etc. may be. Persons with disabilities should also be taken into account to ensure accessibility to the highest extent possible.

To avoid unfair discrimination, the guidelines also emphasise the need of participation of the stakeholders who may be affected by AI systems, by soliciting their feedback throughout the whole life cycle of the AI systems.

SOCIETAL AND ENVIRONMENTAL WELL-BEING – The guidelines underline the importance of sustainability, stating that AI systems shall be assessed for all stages of their development, deployment and use on whether they are sustainable and environmentally friendly. Similarly, the impact of AI systems in all

areas of social life such as education, work, care or entertainment, on people's physical and mental health, as well as on the society and democracy should be duly taken into account.

ACCOUNTABILITY – Pursuant to the requirement of accountability set forth under the guidelines, various systems should be established to guarantee the responsibility and accountability of AI systems and their outcomes throughout their life cycle, including all stages of development, deployment and use.

Accordingly, the AI systems shall be auditable, in a manner to allow the assessment of various components of an AI system, such as algorithms, data and design. These audits may be undertaken by internal or external auditors and reports concerning the outcome of such audits must be made available to the extent possible and in line with intellectual property rights.

In supporting accountability, paramount importance is given to the use of impact assessments. The potential negative impacts of AI systems shall be duly identified, assessed and documented and efforts shall be put in place to limit negative consequences, as much as possible. The guidelines identify red teaming and algorithmic impact assessment forms as potential methods to do this. The higher risk an AI system presents, the higher the importance of such impact assessments and measures to minimise the negative impact.

The guidelines also acknowledge that there may be conflicts and tensions between these requirements. In these cases, ethically acceptable trade-offs should be identified, based on clear reasoning and well documented, so to establish the accountability of the developers of AI systems. Finally, adequate and accessible redress mechanisms should be laid down, especially for vulnerable people or groups.[58]

The guidelines further identify technical and non-technical methods to incorporate the identified key requirements into the AI systems, in all stages of their design, development and deployment. In its last chapter, the guidelines provide methods and best practices to assess the trustworthiness of an AI system.

The other three deliverables produced by AI HLEG similarly aim to facilitate the implementation of these principles, with a number of concrete policy and investment recommendations, practical assessment lists and sector-specific recommendations.[59]

[58] ibid 20.

[59] See High-Level Expert Group on AI, 'Policy and Investment Recommendations for Trustworthy Artificial Intelligence' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence> accessed 12 July 2022; High-Level Expert Group on AI, 'Futurium | European AI Alliance - ALTAI - The Assessment List on Trustworthy Artificial Intelligence' <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence> accessed 12 July 2022; High-Level Expert Group on AI, 'Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI' <https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-sectoral-considerations-policy-and-investment-recommendations-trustworthy-ai> accessed 12 July 2022.

2.3.2 European Commission – White Paper on Artificial Intelligence

On February 2020, the European Commission adopted a white paper, titled *White Paper on Artificial Intelligence - A European approach to excellence and trust*[60] (White Paper). The White Paper has a two-fold aim: promoting the uptake of AI, while also addressing the risks associated with it. To this end, it provides concrete policy options that now are embedded in the Commission's AI Act Proposal [Section 3.2.4].

ECOSYSTEM OF EXCELLENCE – A primary aim while regulating AI has to be that of mobilising resources in both the private and public sector, and along the entire value chain, to stimulate the adoption of new AI solutions. To achieve this objective, the White Paper proposes specific supporting economic actions to Member States, the research and innovation community, and the private and public sector.

ECOSYSTEM OF TRUST – While regulating AI, compliance with EU fundamental rights is of paramount importance, to both give citizens the confidence to take up AI applications and give companies and public organisations the legal certainty to be able to innovate.

The White Paper recognises that AI technologies bring both opportunity and risks, especially as for individuals' fundamental rights and (physical) safety. To address these risks, the White Paper welcomes the principles already identified by the AI HLEG [Section 2.3.1] and proposes some possible adjustments to the existing EU legislative framework applicable to AI solutions, including both the product safety legislation and the data protection legislation.

Of particular relevance in this context, is the risk-based approach adopted in the White Paper, which is addressed more in detail below in the section specifically dedicated to the AI Act Proposal [Section 3.2.4]. In short, the White Paper distinguishes between 'high-risk' AI applications and other, non-high-risk, AI applications. To be qualified as high-risk, an AI application has to meet two cumulative criteria: it has to be employed in a sector where significant risks are expected to occur and it has to be used in such a manner that significant risks are likely to arise. In case an AI application is qualified as high-risk, as similarly done by the guidelines drafted by the AI HLEG [for a more detailed explanation, see Section 2.3.1], the White Paper identifies specific mandatory legal requirements to be implemented. They concern, in particular:

1) Training data, which should be sufficiently broad and representative, while also ensuring compliance with privacy and data protection standards.
2) Records of data relating to the programming of the algorithm and training data, to verify compliance and enforce the applicable rules.
3) Information provision on the AI system's capabilities and limitations and, in case the AI is intended to interact with natural persons, on the existence of this automated interaction.

[60] European Commission, 'White Paper on Artificial Intelligence - A European Approach to Excellence and Trust (COM(2020) 65 Final)' <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 12 July 2022.

4) Robustness and accuracy, to ensure reproducible outcomes and the possibility to address errors and inconsistencies.
5) Human oversight, implying the need to human intervention in the design phase and in the evaluation of the outputs of the algorithms, including the possibility to intervene in real time.
6) Biometric identification, which should only be allowed when duly justified, proportionate and subject to adequate safeguards.

By providing specific policy recommendations and technical requirements for high-risk AI systems, the Commission's White Paper served mostly as a solid basis for then developing a concrete proposal for a binding AI Regulation, which aims to horizontally govern the AI applications deployed in the EU. A tailored assessment of the Proposal is contained below in Section 3.2.4.

3 Legal framework

This section identifies the most relevant legal instruments in the context of policing, specifically in scenarios where police and law enforcement authorities deploy AI-based technologies for prevention, detection, investigation and prosecution of criminal behaviours. It has to be noted that there is no concrete legal framework by the CoE or in the EU which primarily focuses on AI in law enforcement. Nevertheless, there are many pieces of existing legislation that, while focusing specifically on broader fundamental rights and establishing obligations accordingly, still apply to the use of AI tools by LEAs.

First, the section explores the most important human rights instruments in Europe and addresses how AI tools may affect several fundamental rights of individuals, such as the right to a fair trial, right to privacy and to data protection, right to non-discrimination and freedom of expression [Section 3.1]. Subsequently, the section explores the relevant European secondary legislation, including various instruments establishing the rights and obligations that are relevant both for individuals and law enforcement authorities in the deployment of AI technologies, such as the privacy and data protection legislation [Section 3.2.1], the Regulation on the free flow of non-personal data [Section 3.2.2], the EU directives on criminal procedural rights [Section 3.2.3], the proposed AI Regulation [Section 3.2.4], and the framework governing the lawfulness of evidence [Section 3.2.5].

3.1 Human rights relevant for the use of AI systems by LEAs

This first section provides an overview of the most important human rights, as defined within both the ECHR and the Charter, that are susceptible to be affected by the use of AI systems in the law enforcement field. Particular attention is paid to: the right to a fair trial and an effective remedy [Section 3.1.1]; the presumption of innocence and right to defence [Section 3.1.2]; freedom of expression and information [Section 3.1.3]; the right to non-discrimination [Section 3.1.4]; the right to respect for private and family life and the right to the protection of personal data [Section 3.1.5].

It is worth noting that, in light of how human rights are closely connected to each other, the use of AI tools in the context of policing has the potential to affect almost all of them. The overview provided in this section is thus only a general introduction, focusing on the most relevant and fundamental rights. Depending on the scenarios to be developed under ALIGNER and the relevant AI technologies identified in that context, more detailed analyses will be provided in the future deliverables.

3.1.1 Right to a fair trial (ECHR Art. 6) and the right to an effective remedy (Charter Art. 47)

Article 6 of the ECHR titled "*Right to a Fair Trial*", and Article 47 of the Charter titled "*Right to an effective remedy and to a fair trial*", provide certain standards and principles to ensure fair and balanced proceedings. To begin with, the defendant should be clearly informed about the charges

against them (ECHR Art 6(3)(a)).[61] Once informed about what they are being accused with, every person is entitled to a fair and public hearing in the process of determination of a criminal charge against them. This right also includes the requirement that the public hearings should take place within a reasonable time and be undertaken by an independent and impartial tribunal established by law.[62]

The defendant has the right to participate effectively in the proceedings. This means that the defendant should be provided with enough time and necessary means to defend their case. According to the adversarial principle, each party has the right to attend the process in its entirety and observe procedural actions as much as feasible. Being able to attend and observe the whole process enables them to contradict the accusations and the evidence submitted by the other party.

At this stage, the principle of equality of arms is also relevant as one of the inherent components of the right to a fair trial. In line with this principle, both parties shall be given a reasonable opportunity to bring to the proceedings their arguments and evidence, without being put in a disadvantaged situation compared to their counterpart.[63] The defence shall have the possibility to conduct investigations simultaneously with the prosecution.

Both parties should be informed about the submissions the other party makes to the court and, thanks to the confrontational right granted by the ECHR under its Article 6(3)(d),[64] have the opportunity to scrutinise and counteract witnesses, which helps to maintain a fair balance between the parties.[65] While this article specifically refers to witnesses, which could potentially have a limiting effect with regard to examining other types of evidence, the ECtHR interprets broadly the notion of witness[66] and deems that all of the evidence, including AI-based evidence, that is presented can be deemed witness and be a basis for conviction, and therefore any and all types of evidence falls under the protection of the confrontational clause.[67]

According to the right to confrontation, the defendant shall be able to confront the evidence presented against them, not only the probity and credibility of the evidence but also the truthfulness and reliability thereof.[68]

Once the court makes its decision, the reasons on which this decision is based should be adequately stated and made accessible to the defendant, so that the latter is enabled to challenge it. Although these rights are not absolute and can be limited to a certain extent when necessary, they are vital

[61] See also Marquenie (n 3).
[62] Piero Leanza and Ondrej Pridal, *The Right to a Fair Trial: Article 6 of the European Convention on Human Rights* (Wolters Kluwer Law & Business : Kluwer Law International 2014).
[63] Dombo Beheer BV v Netherlands App no 14448/88 (ECtHR, 27 October 1993) para 33. This approach is also taken by the CJEU, see Case C-199/11 EU v Otis and others [2012] ECLI:EU:C:2012:684 para 71.
[64] Stefan Trechsel, *Human Rights in Criminal Proceedings* (Oxford University Press 2006).
[65] European Court of Human Rights, 'Guide on Article 6 of the European Convention on Human Rights, Right to a Fair Trial (Criminal Limb)' (2022) <https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf> accessed 12 July 2022.
[66] See Mika v Sweden App no 31243/06 (ECtHR, 27 January 2009); Lucà v Italy App no 33354/96 (ECtHR, 27 February 2001), where the Court considered that the original sources of hearsay evidence, police informants and expert witnesses and related individuals were also to be deemed "witness".
[67] Thomas Marquenie and others, 'MAGNETO D9.1 Ethical and Legal Guidelines for the Use and Development of MAGNETO Tools' (2019) 32–33.
[68] Al-Khawaja and Tahery v the United Kingdom [GC] App no 26766/05 and 22228/06 (ECtHR, 15 December 2011).

safeguards to make sure that the entire proceedings can be conducted in a fair manner and that the right to a fair trial of the accused person is respected.[69]

As the name suggests, the right to a fair trial is closely connected to the principle of fairness, which is a key criminal procedure principle concerning the defence rights of the individuals. According to the case law of the ECtHR, fairness is of crucial importance in a democratic society.[70] Moreover, fairness is not only required during the trial stage, but during all previous and subsequent stages of the criminal proceeding.[71]

The right to a fair trial as provided under the ECHR and the Charter has a limited scope of application and its wording mainly concerns criminal proceedings. However, the pre-trial and trial stages are closely connected, considering how the procedural actions undertaken by the LEAs in the pre-trial stage can affect the fairness of the later stages. In line with this, the ECtHR adopts a broad interpretation and awards certain rights to individuals during the pre-trial phases as well.[72] Similarly, even though they may not be used specifically during the criminal proceeding phase, the LEAs' deployment of AI technologies can create considerable risks towards the fairness of all related procedures. Moreover, violations of other fundamental rights, such as the rights to privacy and data protection or the right to equal treatment and non-discrimination, can also harm the right to a fair trial.[73]

The right to a fair trial and the related principles mentioned above become relevant for the AI technologies deployed to determine patterns and make predictions as well as to gather or analyse evidence during criminal investigations. Especially in cases where decisions about suspects or defendants are made by the use of AI-based tools, the right to a fair trial may be violated.

PROBLEMS WITH THE AI-BASED SYSTEM ITSELF – The AI-driven tools used in these contexts are not infallible. They may contain errors or may not function as intended, negatively affecting the accuracy of the outputs of the tool.[74] The factors identified to decide the output of the AI system may be inaccurately selected or they may not be comprehensive enough. For instance, a recidivism prediction tool which bases its decisions on gender, age and socio-economic background of an offender may neglect other influential factors such as the family or job situation of that person. This may lead to unfair results among different people.

---

[69] Marquenie (n 3) 112; Nuala Mole and Catharina Harby, *The Right to a Fair Trial, A Guide to the Implementation of Article 6 of the European Convention on Human Rights*, vol 3 (Directorate General of Human Rights, Council of Europe 2006).
[70] Airey v Ireland App no 6289/73 (ECtHR, 9 October 1979) para 24; Stanev v Bulgaria App no 36760/06 (ECtHR, 6 November 2012) para 231.
[71] Moreira de Azevedo v Portugal App no 11296/84 (ECtHR, 23 October 1990) para 66.
[72] Victor Tadros, 'Rethinking the Presumption of Innocence' (2006) 1 Criminal Law and Philosophy 193; (as cited in Marquenie [n 3] 112).
[73] Marquenie and others (n 67) 33.
[74] Francesca Palmiotto, 'The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings' in Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges* (Springer International Publishing 2021) 53ff <https://doi.org/10.1007/978-3-030-50559-2_3> accessed 16 May 2022; It is also argued in the literature that it is not prudent to assume that any computer program is reliable by default, and rather tests should be conducted to prove that the program is accurate, precise and reliable. See Christian Chessman, 'A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution' (2017) 105 California Law Review 179.

PROBLEMS WITH THE DATA – The data that is fed into the AI system may be inaccurate or contain biases, which would lead to inaccurate outputs as well. Indeed in many instances it has been proven that although the data may be accurate, it inevitably reflects the inequalities inherent in the society. Therefore, there is a high likelihood that AI systems making decisions based on historical data may result in biased outputs. The COMPAS tool widely used in the US to predict recidivism rates is an infamous example of biased outputs based on historical data. The tool was consistently inaccurate in its predictions and severely biased against black people.[75] Facial recognition tools are also prone to erroneous results, usually due to the datasets used in developing the tool, and in many instances they fail to accurately identify women and people with darker skin colours.[76]

In this context, for instance, the use of predictive policing tools to detect crime patterns and hotspots or to identify individuals who are considered to present a higher risk of committing crimes could easily undermine the right to a fair trial. As explained above, even if the predictive policing tools are used only in a function to support the decisions made by human officers and judges, this would not guarantee a fair outcome. Due to the opaque nature of an AI system, it may not be easy for human officers to understand how a decision was made by the AI system. They may also not have a full grasp of how biased the results may be. Moreover, human officers may be reluctant to challenge the decisions made by the AI-driven tools. Challenging the decisions of the AI system may be more burdensome than simply accepting these decisions. In the end, this situation may lead to *"judgmental atrophy"*,[77] where majority of decisions are based on the assessments made by the imperfect and unfair AI systems.[78] In light of the above, the risk posed by certain AI systems against the right to a fair trial is considerably high.

Additionally, it was explained above that the right to a fair trial includes right to participate effectively in the proceedings, as well as understanding and confronting evidence and arguments presented by the other parties. Opaque AI-driven systems will create significant challenges for these requirements. For instance, suspects or defendants may not have access to the evidence used against them. Even if they have access to the evidence, they may not be able to examine it in-depth or obtain information about how the relevant conclusions are reached. While the ECtHR does not deem itself competent to comment on evidence-related matters and the admissibility of evidence specifically, in cases where the defendant is not given a chance to challenge the authenticity and the use of unlawfully obtained evidence, the ECtHR may deem that the overall fairness of the proceedings was tainted and that the right to a fair trial was violated. This is very well applicable to the evidence that is obtained with the use of AI-driven systems. [see also Section 3.2.5]

---

[75] Julia Angwin and others, 'Machine Bias' *ProPublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=TiqCeZIj4uLbXl91e3wM2PnmnWbCVOvS> accessed 8 June 2022.

[76] For relevant examples, see Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' 15 and Paul Marks, 'Can the Biases in Facial Recognition Be Fixed; Also, Should They?' (2021) 64 Communications of the ACM 20.

[77] Mireille Hildebrandt, 'Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics' (2018) 68 University of Toronto Law Journal 12, 31.

[78] Marion Oswald and others, 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and "Experimental" Proportionality' (2018) 27 Information & Communications Technology Law 223.

Moreover, as algorithms behind the AI tools are protected with IP rights and trade secrets, even experts may not be allowed to conduct a proper assessment of the accuracy and the reliability of the system. The opacity of the AI tools would limit the suspects' and defendants' capacity to understand and challenge the evidence and to appeal the court decisions based on the output delivered by the AI technologies, overall significantly harming the right to a fair trial.[79]

As summarized by Palmiotto, opaque algorithms create significant challenges for the right to a fair trial, due to their negative effects on *"the adversarial principle when the parties cannot contradict the opponent's allegations; the equality of arms principle when it creates a knowledge asymmetry between parties; the right to confrontation, when algorithms cannot be examined by the defence, and the right to have a reasoned judicial decision when algorithms do not explain or justify how a particular decision has been reached."* [80] In light of the above, to ensure the right to a fair trial, AI systems to be adopted and deployed by LEAs shall have effective transparency and explainability features.[81]

RIGHT TO EFFECTIVE REMEDY – Another relevant right is the right to an effective remedy. According to Article 47 of the Charter, anyone "*whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal*". The right to an effective remedy naturally encompasses the right to a fair trial as well. In addition to the right to a fair trial, this right can also provide a ground to challenge decisions of the LEAs, including those that are informed by AI-driven law enforcement technologies.[82]

The data collected and analysed by the AI tools deployed by the LEAs have the potential to influence the criminal proceedings as well as be used as incriminating evidence against individuals. To ensure that the right to a fair trial is respected, LEAs must pay attention to the above mentioned principles in relation to the collection and management of data that are used in connection with the AI-driven technologies. Crucially, the individuals who are investigated or prosecuted should be informed about the nature of the suspicions and charges against them grounded on or influenced by the use of AI-based tools. They should have the opportunity to observe the various stages of criminal proceedings, including how the accusations against them are shaped with the use of AI tools. They should be able to collect the supporting evidence similarly to how the prosecution collects evidence, and contradict the allegations and evidence presented using the AI tools involving automated processing and data analysis. In line with the above-mentioned principles, the prosecution shall be able to provide and

---

[79] For more information, see Marquenie (n 3); Katherine Quezada-Tavárez, Plixavra Vogiatzoglou and Sofie Royer, 'Legal Challenges in Bringing AI Evidence to the Criminal Courtroom' (2021) 12 New Journal of European Criminal Law 531; Palmiotto (n 74); Gloria González Fuster, 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights' (2020).

[80] Francesca Palmiotto, 'The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings' in Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and Governance of Algorithms: Legal and Ethical Challenges* (Springer International Publishing 2021) 61 <https://doi.org/10.1007/978-3-030-50559-2_3> accessed 16 May 2022;

[81] For a discussion about the explainable AI, see Martin Ebers, 'Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework(s)' [2021] Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence <https://papers.ssrn.com/abstract=3901732> accessed 8 June 2022.

[82] Council of Europe Commisioner for Human Rights, 'Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights' (Council of Europe 2019) 13 <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64> accessed 31 May 2022; as cited in European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (2019) 31 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> accessed 31 May 2022.

explain in court the reports and conclusions reached by means of the use of such AI-based methods. These requirements may be difficult to achieve when opaque AI systems are used. If possible, AI systems which include explainability as a main feature should be preferred.

Compliance of the AI-driven technologies with the national criminal procedure laws are also important to protect the right to a fair trial and due process as well as the right to an effective remedy of the suspects or accused.

3.1.2 Presumption of innocence (ECHR Art 6(2)) and the right to defence (ECHR Art. 6.2, Charter Art. 48)

Article 6(2) of the ECHR and Article 48 of the Charter stipulate that *"everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law"*. Accordingly, the legal burden of proof is on the prosecution and it must prove that the person charged with a criminal offence is guilty, by collecting and presenting sufficient evidence to the court. In order to prevent wrong conviction of an innocent individual, this right also includes the guarantee that the members of a court conducting the criminal proceedings should not commence the criminal proceedings with any previous notion that the accused person has committed the offence in question.[83]

Article 6(2) of the ECHR on the presumption of innocence has a limited wording which mainly concerns criminal proceedings.[84] This means that the presumption of innocence applies in criminal proceedings only after a person has been charged with a crime, and the pre-trial stages are excluded from the scope of this article. However, the pre-trial and the trial stages are closely connected, as the procedural actions undertaken by LEAs in the pre-trial stages can equally affect the fairness of the trial stage. Based on this close connection, the ECtHR interprets the principle of presumption of innocence broadly and deems it to award certain rights to individuals during the pre-trial phases as well.[85]

Predictive policing practices present a higher risk of violating the presumption of innocence. This is mainly because of their dependence on historical data and potential inherent biases that these datasets may contain. In a manner, predictive policing tools are targeting and profiling people as potential criminals before they commit the crime. They thereby have the potential of reversing the burden of proof, obliging innocent people to prove their innocence rather than being treated as innocent until proven guilty by criminal justice.

ProKid 12-SI – The ProKid 12-SI tool used by the Dutch police is a relevant example where the presumption of innocence may be significantly violated. In order to assess the potential criminality of kids between the ages of 0 and 12 years, ProKid 12-SI uses existing police data about the previous instances where the child has come into contact with the police, including the address where the child

[83] Marquenie and others (n 67) 34.
[84] Antonella Galetta, 'The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the Use of Surveillance Technologies?' (2013) 4 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/221> accessed 12 July 2022; (as cited in Marquenie [n 3] 112).
[85] Tadros (n 72); (as cited in Marquenie [n 3] 112).

lives, the child's living situation, relationships, and whether the child has been a victim of violence. On the basis of this information, the system analyses whether the children are under risk of committing a crime in the future, whether a child should be monitored or referred to youth care services.[86] It also analyses the risk and the eventual bad influence of family members and other people living at the same address with the child. Such a system may be useful to protect the children from potential harm they may suffer from the people in their living environment, as well as to protect others from the potential harm that may be caused by the children in question. However, it also labels children as potential criminals, even if they have not committed any crimes yet, simply on the basis of their surroundings and whether they have been victim of a crime. Labeling a child in this manner clearly violates the presumption of innocence.

Nevertheless, presumption of innocence does not entirely preclude the use of algorithms or AI-driven technologies during the criminal proceedings. When using these technologies, LEAs should strive to strike a balance between the pursuit of the truth and the fairness of the proceedings. For ALIGNER, this indicates the necessity of identifying AI-driven technologies which do not contain systemic biases and similar errors in the machine learning or the subsequent reasoning processes. It is also crucial to adopt measures to ensure that the system is sufficiently accountable and explainable. On a more practical level, it is important to adequately train analysts and investigators concerning the prejudices and concepts such as confirmation bias that may be introduced into the criminal proceedings through the use of AI-driven tools.[87]

In this context, it would be beneficial for ALIGNER to identify AI technologies which will enable the LEAs to ensure the fairness of the outcomes of the AI technology, in a manner which guarantees that no unfair assumptions or biases will be embedded in the datasets or the algorithms within the scope of the deployed AI technology. Similarly, the LEAs should make sure that any evidence obtained through the use of the AI technology will not be detrimental to the presumption of innocence of the identified or targeted individuals. An important factor here is that the factual elements should not be considered as proven and included into the final decision of the AI system, unless these factual elements are supported by solid evidence. Moreover, to ensure that the principle of presumption of innocence is protected, the AI systems should be always supported by the presence of a human overseeing the decision-making process and the LEAs should refrain from considering the decisions made by the AI system as being final without such human input. Finally, measures to strengthen accountability and explainability of the AI system would decrease its opacity, minimize inherent biases and ultimately guarantee that the presumption of innocence is respected.[88]

---

[86] European Digital Rights (EDRi), 'Use Cases: Impermissible AI and Fundamental Rights Breaches' (European Digital Rights (EDRi) 2020) 11 <https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf> accessed 8 June 2022; Karolina La Fors-Owczynik, 'Profiling "Anomalies" and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), *Under Observation: The Interplay Between eHealth and Surveillance* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-48342-9_7> accessed 8 June 2022.
[87] Quezada-Tavárez, Vogiatzoglou and Royer (n 79).
[88] Marquenie and others (n 67) 33–34.

3.1.3 Freedom of expression and information (ECHR Art. 10, Charter Art. 11)

Freedom of expression is one of the fundamental pillars of a democratic society, as well as a vital ingredient for its growth and the self-fulfilment of each person.[89] Both Article 10 of the ECHR and Article 11 of the Charter protect the freedom of expression.

Freedom of expression consists of three components: the freedom to hold opinions, the freedom to acquire information and ideas, and the freedom to communicate information and ideas without State interference. The ECtHR has granted a high level of protection to freedom of expression and information through its case law, where this right is found to entail not only a prohibition on interference by state authorities, but also a positive obligation for States to create an adequate legal framework for its protection.

In this context, ensuring the freedom of expression requires a balancing of opposing interests, which complicates safeguarding this freedom, from the perspective of LEAs. Nonetheless, this right may be restricted when there is a legitimate purpose for such restriction, such as national security, territorial integrity or public safety, protection of health or morals, prevention of disorder or crime, protection of the reputation or rights of others, prevention of the disclosure of confidential information. To make such restrictions compatible with the Convention, they should also be mandated by law and necessary in a democratic society (ECHR Article 10). On the other hand, it is important to mention that the ECHR imposes a positive obligation on state authorities, including LEAs, to take particular actions to facilitate the exercise of rights by individuals,[90] which is a more comprehensive requirement compared to merely prohibiting the States from interfering with the rights.

The freedom of expression is also essential for exercising some of the other fundamental rights, such as the freedom of assembly.[91] It would indeed not be possible to benefit from the freedom of assembly without the freedom of expression. However, when competent authorities must protect public interests such as national security, territorial integrity, public safety, or the prevention of disorder or crime, freedom of expression can conflict with other rights such as the right to a fair trial, to privacy, and to freedom of conscience and religion.

On the other hand, the operations of law enforcement are also related with various dangers to freedom of expression. For instance, recording of telecommunications information and subsequent analysis thereof, as well as pervasive monitoring and surveillance, can lead to a chilling effect for individuals. Knowing that they may be observed or listened to by state authorities at any point, individuals may refrain from exercising their freedom of expression.[92] Accordingly, the awareness of government

[89] Stoll v Switzerland App no 69698/01 (ECtHR, 10 December 2007) para 101.
[90] Jim Murdoch and Ralph Roche, *The European Convention on Human Rights and Policing, A Handbook for Police Officers and Other Law Enforcement Officials* (Council of Europe Publishing 2013).
[91] Dominika Bychawska-Siniarska, *Protecting the Right to Freedom of Expression under the European Convention on Human Rights, A Handbook for Legal Practitioners* (2017).
[92] Big Brother Watch and Others v the United Kingdom App no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021). See also Sarah Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An in-Depth Review of La Quadrature Du Net and Others and Privacy International' (2022) 8 European Data Protection Law Review 143.

surveillance may result in fewer minority opinions being expressed, as individuals self-censor on social networks and are less willing to speak when they disagree with the majority. In consequence, the chilling effect that monitoring may have on speech may also have an impact on the freedom of assembly and association. Individuals who are reluctant to speak up in their personal circles would be even more hesitant to participate in groups or public demonstrations.

The freedom of expression also includes the freedom to receive information. The access to information which is sought for the purpose of participating in the public debate has a significant importance for the society. Consequently, the ECtHR has ruled that such material should be easily available to the public.[93]

AI-driven technologies that will be identified by ALIGNER should enable the individuals to exercise their rights and freedoms. To ensure respect for the right to information, the AI-driven technologies should store and keep records of data in a manner that would allow an individual who exercises their right to information before a LEA, where possible and allowed under the law, to access the requested information. Hence, the information within the AI-based tool should be readily available in the system and be able to be easily exported.

Furthermore, ALIGNER should pay utmost attention to ensure that the AI-driven technologies deployed by LEAs will not lead to chilling effects, deterring individuals from exercising their rights. In order to prevent the occurrence of such chilling effects, the AI-driven technology should not be used to target minorities or marginalised communities in an unfair manner. Otherwise, the individuals from these groups may choose to avoid expressing their opinions. Similarly, ALIGNER should avoid AI tools that have biased datasets or algorithms, as these would have a disproportionate negative impact on marginalised communities and beyond, and limit their freedom of expression.[94]

3.1.4 The right to equality and non-discrimination (ECHR Art 14, Charter Art 20 & 21, the International Convention on the Elimination of All Forms of Racial Discrimination (CERD))

Discrimination occurs when the outcome of an action constitutes a distinction, exclusion or preference which nullifies or impairs the equality of opportunity or treatment of individuals based on personal characteristics such as race, sex, ethnicity or religion. According to the right to equal treatment and non-discrimination, all individuals must be treated equally under the law and protected from such discriminatory decisions or policies[95] (ECHR Article 14, Charter Article 21).

[93] Magyar Helsinki Bizottság v Hungary App no 18030/11 (ECtHR, 8 November 2016) para 180.
[94] Marquenie and others (n 67) 35–37.
[95] Federico Casolari and Lucia Serena Rossi (eds), *The Principle of Equality in EU Law* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017). It is worth noting that the prohibition of discrimination under Article 14 of the ECHR is not a stand-alone right, it originally only protects individuals against discrimination when enjoying the rights accorded under the ECHR. However, the Protocol 12 of the ECHR has established a wider prohibition of discrimination: the enjoyment of any right set forth by law shall be secured without discrimination on any ground, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status and no one shall be discriminated against by any public authority on any ground (ECHR Protocol 12, Article 1).

Similarly, the International Convention on the elimination of all forms of Racial Discrimination (CERD), a UN convention ratified by all EU Member States, prohibits discrimination. According to the CERD, discrimination is any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life (CERD Article 1(1)). The Member States are prohibited from engaging in any act or practice of racial discrimination against persons, groups of persons or institutions and to ensure that all public authorities and public institutions, national and local act in line with the convention (CERD Article 2(1)). Nevertheless, as long as the Member States do not discriminate against any particular nationality, they can apply distinctions, exclusions, restrictions or preferences made between citizens and non-citizens (CERD Article 1(2)), as well as establish legal provisions concerning nationality, citizenship or naturalization (CERD Article 1(3)).

Within the context of the EU, according to the Charter, any discrimination on grounds of nationality shall be prohibited (Charter Article 21(2)). The Charter also guarantees equality between women and men in all areas, including employment work and pay (Charter Article 23).

Additionally, the LED also explicitly prohibits discrimination, more specifically discriminatory profiling and automated decision-making based on protected attributes, which are explored below in Section 3.2.1.1.v.

According to the principle of equality, similar cases cannot be treated differently, and different cases cannot be treated equally. In the event two categories are treated differently, two questions must be answered: whether those categories are similar or not, and whether it would be wrong to treat them differently. If there is no justification to explain the different treatment between two or more categories, that would be considered discrimination.[96]

The possibility of bias and inequality[97] in algorithmic systems is high. The historical data used in AI systems may not fully reflect the actual criminality in the society. It is a record of the crimes, areas and groups of people which are monitored by LEAs. It is a direct result of the operational choices made by LEAs, concerning which areas and people will be monitored more closely. Areas where more crimes are committed may be more closely monitored, which is a natural choice. Also, these are choices that LEAs are forced to make due to the limitations of their technical, financial and human resources and do not automatically indicate a bias. Nevertheless, the data resulting from these activities will inevitably be more focused on these selected areas and people, and as a result will automatically include these implicit biases. Moreover, the data included in these datasets may not always be free of mistakes, sometimes erroneous information may also be included into the datasets. In these cases where the training data is derived from incorrect or biased information, the resulting models and

[96] European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe, *Handbook on European Non-Discrimination Law* (Publications Office of the European Union 2018) <https://data.europa.eu/doi/10.2811/58933> accessed 13 July 2022; Marquenie and others (n 67) 37.

[97] Victor Demiaux, 'How Can Humans Keep the Upper Hand? Report on the Ethical Matters Raised by Algorithms and Artificial Intelligence' (2017) <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf> accessed 12 July 2022.

decisions are very well capable of reflecting and repeating the biases in practice. At that point, it is possible to talk about 'feedback loops' that proliferate patterns of inequality[98] and prolong discriminatory and exclusive policing tactics by legitimising them through their inclusion in advanced analytical systems, such as the AI-driven tools that ALIGNER will identify.

Academic research pointed out to potential discriminatory outcomes caused by data mining and machine learning, based on certain sensitive characteristics such as gender, ethnicity, religion, etc.[99] AI tools can find new patterns in databases, match these patterns with certain outcomes and on the basis of their findings, place individuals in previously non-existing categories. Subsequently, these categories can be used as proxies for sensitive attributes, with equally negative effects as discrimination based on the sensitive characteristics mentioned above. For instance, an AI tool may detect that, on the basis that a poorer neighbourhood has a higher crime rate, individuals who live in that area may be more likely to commit crime. This could easily lead to over-policing of these areas and thus a greater number of convictions for the individuals who live there, harming the right to equality and non-discrimination. Moreover, location may be used as a proxy for ethnicity, as it is not uncommon for minority communities to reside within common areas. These risks are inherent to analytical systems that are trained on data which has human biases incorporated in it. These flaws are replicated in the systems which are used to analyse data, make predictions, assess evidence, and guide LEAs' practices.

Furthermore, the potential discrimination that AI systems may cause exacerbates the already existing legal shortcomings concerning discrimination. A recent report published by the European Commission, titled "*Algorithmic discrimination in Europe - Challenges and opportunities for gender equality and non-discrimination law*"[100] lists these existing shortcomings as, "*the uneven material scope of EU discrimination law, the exceptions to gender equality in the field of goods and services, the comparator problem, the lack of recognition for intersectional discrimination, the exhaustive nature of the list of protected grounds, and uncertainties in the distinction between direct and indirect discrimination*" and emphasizes the urgent necessity to address these gaps, concerning how AI technologies may spread discrimination at an unprecedented scale and speed.[101]

Such risks must be taken into account and prevented as much as possible. ALIGNER should pay utmost attention to ensure that its AI-based technologies do not discriminate individuals on the basis of social origin, ethnicity, gender, religious or political opinion, or on the basis of other categorizations that may be used as proxies for these sensitive characteristics. Beyond data collection, AI systems may lead to

---

[98] Fair Trials, 'Briefing Paper on the Communication on Digitalisation of Justice in the European Union' (2021) 8 <https://policehumanrightsresources.org/content/uploads/2021/10/BRIEFING-PAPER-ON-THE-COMMUNICATION-ON-DIGITALISATION-OF-JUSTICE-IN-THE-EUROPEAN-UNION.pdf?x19059> accessed 13 July 2022.

[99] See for instance Laurens Naudts, 'Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?' in Anton Vedder and others (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) <https://papers.ssrn.com/abstract=3508020> accessed 13 July 2022; and Rosamunde van Brakel and Paul De Hert, 'Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies.' (2011) 20 Journal of Police Studies 163.

[100] Janneke Gerards and Rapha Xenidis, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law : A Special Report* (2021).

[101] ibid 152.

biased or discriminatory practices through, for example, profiling. Thereby, AI-based systems should strive to prevent and mitigate any discriminatory effects of profiling or similar techniques.[102]

One solution that is suggested to prevent discrimination by AI-driven tools is to have these systems tested by independent bodies both before and after they are deployed in the criminal justice systems.[103] Moreover, from a different perspective, it is also possible to instrumentalise AI-driven tools can to detect and prevent discrimination. Visualisation and measuring capabilities provided by certain AI tools can indeed provide countless benefits in this regard.[104]

To effectively address potential discrimination by algorithms, it is important to support interdisciplinary collaboration, ensuring a dialogue between computer and data scientists and law makers and policy experts.

3.1.5 The right to respect for private and family life (ECHR Art. 8, Charter Art. 7 and 52) and the right to protection of personal data (Charter Art. 8)[105]

The right to respect for private life and the right to personal data protection provide individuals with a private domain in which they are free to develop their personalities, as well as to establish relations with others without external intrusions. Therefore, these rights are necessary preconditions for exercising other fundamental freedoms.[106][107] The main difference between the two is in their formulation and scope: the right to privacy entails a general prohibition on interference by public and private bodies, which may be subject to some public interest criteria that allows interference in some cases, whereas the right to data protection establishes a system of checks and balances with the goal of protecting individuals whenever their data is processed.[108] Moreover, both can be seen as broader than one another, as the right to privacy encompasses aspects that are irrelevant to data processing, and data protection is applicable whenever processing activities are involved regardless of whether the information relating to the individual may be considered as private or not.[109]

These rights are laid down in Article 8 of the ECHR and Articles 7 and 8 of the Charter. According to the right to private life as enshrined under both Charter and ECHR, everyone has the right to respect for their private and family life, their home and their communications. According to the ECtHR, the concept of 'private life' should be understood in a broad sense and cannot be interpreted in an exhaustive

---

[102] Marquenie and others (n 67) 37–38. CoE Commissioner for Human Rights also emphasizes the risks of using AI tools for the rights to non-discrimination and equality in its recommendation titled "Unboxing Artificial Intelligence: 10 steps to protect human rights". The recommendation specifically states the need to "apply the highest level of scrutiny when using AI systems in the context of law enforcement, especially to avoid profiling of individuals belonging to specific groups". See Council of Europe Commisioner for Human Rights (n 82) 21.
[103] Fair Trials (n 98) 9.
[104] Gerards and Xenidis (n 100) 152.
[105] Marquenie and others (n 67).
[106] European Union Agency for Fundamental Rights and others, *Handbook on European Data Protection Law: 2018 Edition* (Publications Office 2018) <https://data.europa.eu/doi/10.2811/343461> accessed 2 June 2022.
[107] ibid.
[108] Marquenie and others (n 67) 38.
[109] Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" Of A Right To Data Protection In The EU Legal Order' (2014) 63 International & Comparative Law Quarterly 569.

manner.[110] This concept pertains not only to the integrity of an individual but also to the integrity of the relationships between different people. It was also established by the ECtHR that there is an undeniable connection between an individual's private life and their physical and moral integrity, and their sexual lives.[111] Moreover, the interactions, associations, and relationships with other people that occur in a person's life are considered to be part of that individual's private life.[112] The right to private life is highly relevant to the activities that LEAs may pursue using AI-driven tools, considering the close relation between the concept of 'private life' and its importance for an individual's relationships, associations and networks. Furthermore, both the ECtHR and the CJEU consider that the right to privacy is interfered with by personal data processing activities.

Additionally, as opposed to the ECHR, the Charter addresses the right to the protection of personal data under a separate article. This is welcomed by some scholars, as such a separation may emphasize the importance of both rights and offer individuals a stronger control over their personal data, going beyond the control provided by the right to privacy.[113] In any event, these two rights require a joint interpretation, due to their strong relationship, and they need to be read and considered together.[114]

According to the Charter, personal data must be processed in a fair manner and aim to accomplish specific purposes. It shall be based either on the consent of the concerned person or on another legitimate legal ground, which must be established by the law. Moreover, it states that individuals have the right to access to their personal data and the right to have it rectified. Last but not least, an independent authority shall have oversight and control to ensure that these rules are complied with (Charter Article 8).

On the other hand, it should be noted that the right to privacy and data protection under the Charter are not absolute rights and Member States can interfere with these rights as long as they comply with certain limitations laid down under the Charter. According to Article 52 of the Charter, such limitations must:

- be provided for by law;
- respect the essence of the right to data protection;
- be subject to the principle of proportionality and necessity; and
- genuinely meet objectives of general interest recognised by the Union or the need to protect rights and freedoms of others.

Similarly, according to the ECHR Article8(2), there shall be no interference with the right to privacy by a public authority, unless such interference is imposed in accordance with a law, justified by the

[110] Costello-Roberts v the United Kingdom App no 13134/87 (ECtHR, 25 March 1993).
[111] X and Y v the Netherlands App no 8978/80 (ECtHR, 26 March 1985), para 22.
[112] Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992).
[113] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 11.
[114] Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector, WP 211' <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 13 July 2022.

requirements of a democratic society and serves vital and legitimate public interests such as the national security, public safety or the economic well-being of the country.

The activities to be undertaken by the LEAs using the AI-driven tools that will be identified by ALIGNER must also comply with the requirements above. The majority of such activities indeed concern the protection of national security and the prevention of crime, which would justify an interference with the rights to privacy and to data protection.[115] Still, the other requirements listed above must be respected.

Overall, a careful assessment is necessary to ensure the lawfulness and the necessity of such interferences by LEAs using the AI-driven technologies that will be identified and recommended by ALIGNER.

Some of the AI technologies that may be deployed by LEAs, such as facial recognition, criminal profiling and predictive policing tools, require large datasets developed with personal data [see also Section 3.2.1.1.i.], and therefore may unduly cause risks to the rights to privacy and to data protection. The majority of AI tools deployed in policing scenarios involve the processing of not only personal but also sensitive data. Considering the ubiquity of technology in an individual's daily life, a great amount of data can be easily collected, in a manner to provide a clear, very detailed picture of that individual's life, habits, personality, beliefs and relationships. Combined with the advancing AI-based policing technologies, many types of information relating to individuals can find its way into LEAs' databases used for the development and functioning of AI-based tools, inevitably creating risks towards the rights to privacy and data protection.

Not all AI-driven technologies deployed by LEAs will present risks as high as these examples; yet, it is likely that the majority of such technologies will need to process immense amounts of data collected from various sources with the aim of identifying individuals, networks, groups and events that are suspected to be connected to criminal offences. Furthermore, LEAs are in a position of greater power in relation to citizens. Citizens are likely to have little or no control over their personal information. As a result, the less risky AI-driven tools are still likely to have a significant impact on the right to privacy and data protection. This situation requires a strict adherence to respect with the conditions for the limitation of these rights, as well as to the data protection requirements, as elaborated upon in secondary legislation [Section 3.2.1]. The AI technologies in question shall include the measures to minimize the interferences with the private lives of individuals.

To summarise, the concepts of privacy and data protection allow individuals to have a private, internal sphere where they can think freely and develop their identities. As a result, the rights to privacy and data protection are indispensable for the exercise of other fundamental rights and freedoms. This is the key reason why they are always strongly emphasized in the EU when it comes to the adoption and

[115] European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights - Right to Respect for Private and Family Life, Home and Correspondence' (Council of Europe 2021) 8 <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> accessed 13 July 2022.

deployment of AI-based technologies. Especially the activities that will be undertaken by LEAs have a greater risk to undermine these rights, due to the significant power asymmetry between the individuals that will be subject to the AI-driven LEAs technologies and the substantial results that the use of such tools may lead to.

THE RIGHT TO PRIVACY AND DATA PROTECTION AND UNLAWFUL EVIDENCE – According to the case law of the ECtHR, problematic cases of evidence collection can also lead to the violation of the right to privacy and data protection. In this regard, the ECtHR distinguishes systems that are specifically developed and deployed for surveillance purposes from systems that do not have a primary aim of surveillance. Systems that have a primary surveillance purpose are usually strictly regulated under the law. As long as their use complies with the requirements and specific procedures stipulated under the relevant laws, the use of such systems and the evidence obtained through these do not violate the right to privacy. On the other hand, when a system's primary purpose is not surveillance, but it is being repurposed for it, then the use of such systems are deemed to violate the right to privacy, based on the fact that individuals will not be able to foresee that the system could be used for surveillance.[116]

When evidence is extracted from devices that are not built for surveillance purposes, such as smart-phones or other personal devices where electronic communications are conducted, the ECtHR requires that appropriate safeguards should be established against abuses of right to privacy and data protection, in function of the way surveillance is conducted.[117] The data may be extracted directly from the citizens or obtained from an electronic service provider, it may be obtained through targeted collection or in bulk through untargeted collection activity, all being activities where the intervention of AI-driven tools is possible. According to the ECtHR's case law, if the surveillance on such devices is conducted on the basis of a legal framework, the legal framework should include clear specifications when and under which conditions the surveillance takes place, so that individuals can have a clear idea concerning when they may be subjected to surveillance.[118] Moreover, these surveillance activities should be based on prior authorisation.[119]

In the context of ALIGNER, this means that any interference with people's personal devices and communications where they would not normally expect to be under surveillance, including tapping into these devices and collection of evidence via the use of AI-driven tools, should be based on prior authorisation with a clear legal ground foreseen under the relevant laws. Moreover, the individuals should be clearly informed of the details of potential surveillance they may be under, such as the conditions under which LEAs may access their data. Considering the current lack of clear and AI-specific regulations in the EU, the use of AI tools for such surveillance and evidence extraction purposes may

[116] P.G. and J.H. v the United Kingdom App no 44787/98 (ECtHR, 25 December 2001 Final), paras 37-38; Vetter v France App no 59842/00 (ECtHR, 31 May 2005); Wisse v France App no 71611/01 (ECtHR, 22 December 2005) (as cited in Quezada-Tavárez, Vogiatzoglou and Royer [n 79] 537, fn 32).
[117] For relevant examples, see Klass and others v Germany App no 5029/71 (ECtHR, 6 September 1978); Bykov v Russia App no 4378/02 (ECtHR, 10 March 2009); Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015); Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016); Big Brother Watch and others v the United Kingdom App no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) (n 92); P.N. v Germany App no 74440/17 (ECtHR, 11 June 2020) (as cited in ibid 537, fn 35.).
[118] Ibid.
[119] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 537.

become challenging. The principles laid down by the case law mentioned above should be kept in mind while assessing the lawfulness of the use of such AI-driven tools as well as the evidence obtained through their use.

EXAMPLE OF AI IN POLICING INTERFERING WITH THE RIGHT TO PRIVACY – The recent Bridges case[120] concerning the use of automated facial recognition technology by the South Wales police in the UK could provide some guidance to interplay between the right to privacy and data protection and the facial recognition technologies. The Bridges case has significance as the first case where the use of facial recognition technologies deployed by LEAs were considered by a court.

For a duration of over two years, the South Wales Police deployed an automated facial recognition technology known as 'AFR Locate', once in a shopping streets before Christmas and another time at a technology exhibition. The AFR Locate compared the images of people passing by with the images of people who are in a watchlist of around 400 to 800 people, curated by the South Wales Police.[121] Around 500000 faces were checked against this watchlist in total throughout three years. While the South Wales Police paid great attention to keeping the practice as overt as possible, informing the individuals who entered the area where the technology was deployed, by handing out postcards with URL addresses directing people to websites where they could obtain more information. The watchlist was also published. The images that were not matched with any from the watchlist were immediately deleted. More importantly, any decision made by the facial recognition system was checked by a police officer before any action was taken, making sure that the system was not fully automated and a human was involved in the process. However, there were certain problems with the deployment as well: the watchlist not only included people who were suspected of criminal offences but also vulnerable people such as missing children. There was no minimum threshold of severity of crimes that justified and limited inclusion of people into the list. People who were not directly under suspicion but had a connection to the suspects were also included in the watchlist.

A privacy campaigner, Ed Bridges, brought the case before the Divisional Court. He argued that he had not seen any signage in the area that the technology was being deployed by the South Wales Police. His claims included, among others, that this practice breached Article 8 of the ECHR (as well as ss 35 and 6491) of the Data Protection Act 2018 and the s 149 of Equality Act 2010, especially concerning the false positives detected by the technology).[122]

The Divisional Court, assessing Bridges' claims, emphasized the critical importance of the facial recognition technology compared to other forms of biometric surveillance, stating that *"facial biometrics can be procured without requiring the co-operation or knowledge of the subject or the use*

[120] R (Bridges) v Chief Constable of South Wales Police and Secretary of State for the Home Office [2019] EWHC 2341 (Admin) ("Divisional Court decision"), Bridges v Chief Constable of South Wales Police and Other [2020] EWCA CIV 1058 ("Court of Appeal decision").
[121] The details of how the AFR Locate functioned was detailed in paragraph 24 of the judgment and its deployment in paragraph 32 ff.
[122] L Woods, 'Automated Facial Recognition in the UK: The Bridges Case and Beyond' (2020) 6 European Data Protection Law Review 455, 456.

of force, and can be obtained on a mass scale".[123] With this emphasis on the importance of the technology, the Divisional Court found that even if this practice was taking place in a public space, it could have significant impacts on the right to privacy, therefore the claimant's rights under the Article 8 of the ECHR could indeed be breached. Assessing the lawfulness of the measure, the Divisional Court held that the measure was foreseeable and predictable, and therefore lawful, as well as proportionate, as the measures were necessary in a democratic society.[124] Moreover, it decided that the deployment of the technology was in line with the domestic data protection regime in the UK, the South Wales Police had taken the necessary measures and the processing was proportionate. The trial was conducted for a limited time, in a limited geographic area and used a specific, limited watchlist.

However, the judgment of the Divisional Court was appealed and in contrast to that judgment, the Court of Appeal found that certain legal requirements concerning privacy, data protection and equality were not complied with. With regard to privacy concerns, the Court of Appeal stated that *"the more intrusive the act complained of, the more precise and specific must be the law said to justify it"*.[125] It did not declare the technology inherently unlawful, but stated that certain requirements that were not complied with rendered the practice unlawful. For instance, the South Wales Police had neglected to investigate the impact of this technology on equality. Overall, the decision concerns how to better construct the watchlist by introducing some constraints and limits as to who can be included, how to justify the locations where the technology is deployed, as well as how the police should have provided more transparency. In a sense, this decision adopts an approach that is similar to that adopted by the AI Act Proposal. In other words, rather than banning the facial recognition technology, it incentivizes certain administrative specifications.[126]

CONCLUSION – In developing the policy roadmaps and identifying potential AI-based technologies that could benefit LEAs, ALIGNER should focus on technologies that would include measures to minimise the interference with the rights to privacy and data protection and limit such interferences only to absolutely necessary processing activities. Further requirements concerning the right to privacy and data protection as foreseen under secondary legislation in the EU are addressed in Section 3.2.1 below.

3.2 Secondary legislation

This second section provides an overview of the most important European secondary legislation, including various instruments establishing the rights and obligations that are relevant both for individuals and law enforcement authorities in the deployment of AI technologies, such as the privacy and data protection legislation [Section 3.2.1], the Regulation on the free flow of non-personal data

[123] See paragraph 43 of the Divisional Court decision and paragraph 23 of the Court of Appeal decision.
[124] The court conducted this assessment on the basis of the four part test established in the Bank Mellat case (Bank Mellat v Her Majesty's Treasury (No 2) [2014] AC 700). See L Woods, 'Automated Facial Recognition in the UK: The Bridges Case and Beyond' (2020) 6 European Data Protection Law Review 455, 457.
[125] See paragraphs 82-83 of the Court of Appeal decision.
[126] For more information on the case, see Woods (n 122).

[Section 3.2.2], the EU directives on criminal procedural rights [Section 3.2.3], the proposed AI Regulation [Section 3.2.4], and the framework governing the lawfulness of evidence [Section 3.2.5].

3.2.1 Privacy and data protection legislation

As already seen above [Section 3.1.5], the rights to privacy and data protection are among the fundamental rights of individuals primarily affected by AI systems used in policing contexts. The present section provides an overview of the main European instruments established by both the CoE and the EU with the aim of safeguarding these important instrumental rights. To this aim, the section addresses the Law Enforcement Directive [3.2.1.1], the e-Privacy Directive and the e-Privacy Regulation [3.2.1.2], the framework on the collaboration between LEAs and EU agencies [3.2.1.3] and the relevant CoE instruments [Section 3.2.1.4].

3.2.1.1 Law Enforcement Directive (LED)

In May 2016, the EU co-legislators adopted the so-called 'data protection package', a set of legal instruments with the scope to adapt the European framework on data protection to the digital age. The package consists of the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions.

While GDPR regulates, in general, the processing of personal data and their free movement, the LED is specifically aimed to govern personal data processing operations within the law enforcement context. Therefore, the LED is the data protection instrument of paramount importance for ALIGNER.

i. Scope of application and definitions

The LED has a two-fold aim: protecting the fundamental rights and freedoms of natural persons, especially as for the right to data protection, while also ensuring the exchange of personal data for law enforcement purposes.[127] Each of these objectives is crucial to ensure effective judicial and police cooperation in criminal matters. Therefore, the Directive harmonises the legal framework in all EU Member States, to strengthen both the rights of natural persons whose personal data are processed for law enforcement purposes and the obligations of those who carry out these processing activities.[128]

Article 2 of the LED defines the material scope of application of the Directive. The legal instrument applies 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, including the safeguarding against and the prevention of threats to public security. To better understand the precise scope of application of the directive, it is important to first introduce some key definitions.

[127] LED Article 1.
[128] LED Recital 7.

PERSONAL DATA – Personal data means any information relating to an identified or identified natural person, namely a living individual labelled as 'data subject'.

The concept of 'personal data' has to be interpreted broadly. The nature of the information can, indeed, consists of any sort of statement about a natural person, including objective and subjective information. Also, for being considered personal data, the content of the information does not necessarily have to cover a topic touching the natural person's private life, but it can also relate to any kind of activity undertaken by the data subject. Finally, the information can be available in any format.[129]

For an information to amount to 'personal data', it has to relate to a natural person. In other words, the data has to be about an individual. It is understood that an information can relate to a natural person for either its content, purpose or result. Clearly, the content element is present where the information is about a particular person. The purpose element exists when the information is used with the purpose to evaluate or treat in a certain way a particular person. The result element applies when the information has an impact on a particular person's rights or interests.[130]

Finally, the information has to relate to a natural person who has to either be identified or identifiable. A natural person is 'identified' when they are singled out from a group, not necessarily via their name; on the contrary, a natural person is 'identifiable' when they are not yet singled out from a group, but it is anyway possible to do so, through the means of an additional piece of information called 'identifier'. A direct identifier is a person's name, while indirect identifiers are, for instance, identification numbers, location data, telephone numbers or a combination of significant criteria.[131] When determining whether a natural person is identifiable, the criterion is that of "*all the means reasonably likely to be used*" for singling that person out. This evaluation should take into account all the possible objective factors, including the costs and the amount of time required for the identification and the available technology.[132] It is not necessary that all the relevant pieces of information necessary for identifying the natural person are retained by the same entity, as long as they can still be combined.[133]

It follows from the above that, while fully anonymised data will not overcome the threshold of the identifiability and, therefore, cannot be considered personal data, the opposite holds for pseudonymised information. Pseudonymised data are, indeed, data processed in such a manner that it can no longer be attributed to a specific natural person without relying on additional information, which is kept separately and subject to technical and organisational measures to ensure that the data

[129] Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 13 July 2022.
[130] ibid.
[131] ibid 4.
[132] LED Recital 21.
[133] Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.

are not attributed to an identified or identifiable natural person.[134] Therefore, the processing of pseudonymised data is still subject to the LED.

The majority of data processed within the scope of the use of AI-driven tools by LEAs is personal data. This may create significant compliance burdens for the developers of AI-driven systems, especially considering how certain characteristics of AI-driven tools, such as opacity and biased outcomes, clash with the legal requirements under the GDPR and LED. In order to alleviate this burden, developers may intend to develop such AI-based systems in a manner where only anonymised data will be processed. However, it is difficult in practice to ensure full anonymity of the data and there is almost always a re-identification risk.[135] As stated by the Spanish data protection supervisory authority,

"A robust anonymisation process aims to reduce the re-identification risk below a certain threshold. Such threshold will depend on several factors such as the existing mitigation controls (none in the context of public disclosure), the impact on individuals' privacy in the event of re-identification, the motives and the capacity of an attacker to re-identify the data. Although a 100% anonymisation is the most desirable goal from a personal data protection perspective, in some cases it is not possible and a residual risk of re-identification must be considered."[136]

In many cases, there is a significant risk of re-identification, for instance when the total number of individuals included in a dataset is too small, when the categories relating to the individuals are too different in a manner to allow singling out of the individuals from the rest, or when a dataset contains a significant amount of demographic attributes or location data.[137] Therefore, in the face of statements claiming full anonymity of the data fed into an AI-driven system, and that a specific system does not fall into the scope of the LED, it is of utmost importance to scrutinize these statements closely.

PERSONAL DATA PROCESSING – Processing means any operation that can be performed on personal data, whether or not by automated means. The definition provided by the LED is voluntarily so broad that it covers virtually any type of activity that can be carried out on data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[138]

COMPETENT AUTHORITIES – Competent authorities are defined by the LED as:

---

[134] LED Article 3(5).
[135] Agencia Española de Protección de Datos and European Data Protection Supervisor, '10 Misunderstanding Related to Anonymisation' 5 <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf> accessed 13 July 2022. In this context, the European Data Protection Board (EDPB) also has ongoing research on anonymisation and pseudonymisation and an opinion is expected to be published in 2022.
[136] ibid.
[137] Luc Rocher, Julien M Hendrickx and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069; Fengli Xu and others, 'Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data', *Proceedings of the 26th International Conference on World Wide Web* (2017) <http://arxiv.org/abs/1702.06270> accessed 13 July 2022; (as referred to in Agencia Española de Protección de Datos and European Data Protection Supervisor [n 135] 4, fn 8–9).
[138] LED Article 3(2).

(a) any public authority competent for law enforcement purposes; or
(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for law enforcement purposes.[139]

An authority is competent for law enforcement purposes if it is established by either a EU or Member State law determining its structure and mandates. Alternatively, another (private) body or entity can be considered as a competent authority, if a Member State law entrusts it to exercise law enforcement powers. Therefore, if personal data are processed by (private) body or entities which do not have law enforcement powers, the GDPR will apply. However, the question has also been raised to what extent such private entities may still be subject to the LED as processors.[140] This point may be important to consider for ALIGNER, with regard to the involvement of private entities or authorities that are not entitled to exercise law enforcement powers in the deployment or development of the AI-driven technologies that will be used by the LEAs.

LAW ENFORCEMENT PURPOSES – The LED contains an explicit list of law enforcement purposes. These are: the 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.[141] Therefore, if personal data are processed by competent authorities for purposes other than the ones listed above, the GDPR will apply. While not within the scope of ALIGNER, this would include the research and development stages of the AI-based tools that will be used by LEAs.

ii. Key actors: controllers and processors

The LED establishes precise obligations for the actors involved in the processing of personal data. However, not all the entities involved are equally responsible: the Directive allocates, indeed, the responsibilities on the basis of the different roles assumed during the carrying out of the processing activities.

The LED distinguishes between two types of actors: controllers and processors. The precise meaning of these two terms are clarified by Article 3 of the Directive.

DEFINITION OF 'CONTROLLER' – Data controllers are the competent authorities which, alone or jointly with others, determine the purposes and means of the processing of personal data. In case the purposes and means of the processing are explicitly determined by EU or national law, the same law can also identify the controller or the criteria for their identification.[142]

The definition of 'controller' consists of five main building blocks:[143]

[139] LED Article 3(7).
[140] Mireille M Caruana, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33 International Review of Law, Computers & Technology 249.
[141] LED Article 1.
[142] LED Article 4(8).
[143] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0' (2021) <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf> accessed 23 May 2022.

1. ‘competent authorities’, as defined in the previous paragraph. Under the Directive, only competent authorities (so, normally, LEAs) can assume the legal status of controllers.
2. ‘alone or jointly with others’. More than one data controllers can be involved in the processing operations. In this case there is a situation of ‘joint controllership’ and the responsibilities are shared between the two (or more) competent authorities involved.
3. ‘determine’. This requirement concerns the capacity of the competent authority to exercise decision-making powers over the processing, influencing its key elements. These powers can, in general, stem from two different occasions: a EU or domestic legal provision, usually also determining the purposes of the processing; or a factual assessment of the situation. In the case of LEAs, is generally a law that determines (at least) the criteria for the identification of the competent authority to be considered as controller and the purposes of the processing operations. In case this is not legally predetermined, then a factual assessment of the context is in which the processing happens is necessary.
4. ‘the purposes and means’, namely the ‘why’ and ‘how’ of the data processing activities. Generally, data controllers must decide on both the purposes and means of the processing; some margin of manoeuvre as regards technical aspects of the processing can be left to the processor. In the case of the LED, this threshold is anyway less stringent: it is generally for the EU or the national law to determine the law enforcement purpose for which the processing by the competent authority is allowed.
5. ‘of the processing of personal data’, as defined in the previous paragraph.

The controller is the entity primarily responsible for ensuring and demonstrating compliance with the requirements and obligations set in the LED.[144] Therefore, it has a duty to choose only processors which offer sufficient guarantees to implement technical and organisational measures to meet the requirements of the Directive.[145]

DEFINITION OF ‘PROCESSOR’ – Processors are any natural or legal persons, public authorities, agencies or other bodies, which process personal data on behalf of the controller.

The LED definition of ‘processor’ is so broad that, virtually, any entity can assume this legal status. However, two cumulative conditions must be fulfilled:

1. The concerned entity has to be a completely separate one from the controller. Therefore, the competent authority must have decided to externalise (parts of) the processing to a different organisation.
2. The processor must process the data on the controller’s behalf, meaning that it was delegated by the controller and does not pursue its own purposes, but it only acts according to the instructions received.

[144] LED Article 4(4).
[145] LED Article 22.

In this way, public or private entities to whom processing operations have been delegated by LEAs, for instance a cloud service provider providing storage capacities to a LEA, could act as processor under the LED. The processor is not responsible to ensure full compliance with the LED, but it has a duty to assist the controller in this sense.[146]

iii. Data protection principles

The LED prescribes a set of legal principles that must be observed while carrying out personal data processing activities, which largely mirror the GDPR data protection principles. According to Article 4 of the LED, personal data must be:

(a) processed lawfully and fairly;
(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; and
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles are further analysed below.

LAWFULNESS AND FAIRNESS – The processing of personal data must be lawful, fair and transparent.[147]

The principle of lawfulness addresses the legality of the processing activities, which is further clarified by Article 8 of the LED. According to this, the processing is lawful only if and to the extent that it is necessary for the performance of a task carried out by a competent authority acting for law enforcement purposes and if based on either EU or Member State law. In the latter case, the national law must specify at least the objective and purposes of the processing, as well as the personal data involved.

The LED identifies special categories of personal data, also referred to as sensitive data. These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union memberships; as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. For these special categories of personal data a higher lawfulness threshold is foreseen: the processing is allowed under appropriate safeguards for the right and freedoms of the

[146] LED Article 22.
[147] LED Recital 26.

data subjects and only where strictly necessary, if authorized by law or to protect the vital interests of a natural person, or where the data was manifestly made public by the data subject.[148]

The principles of fairness and transparency aim to ensure that the data subject is made aware of the risks, rules, safeguards and rights in relation to the data processing activities.[149] These principles also reflect the fairness and transparency requirements included in ethics frameworks that govern the use of AI-driven technologies by the LEAs. These principles are further implemented in the LED via the establishment of certain data subject rights, such as the right to information access [see paragraph iv. of this section].

In the context of ALIGNER, to ensure transparency, attention shall be paid to identify tools that will allow reviewing and understanding the technical core and working mechanism, as well as potential outcomes of the algorithms. One way of allowing such review and analysis would be disclosing the source code, system reports and the documentation concerning the features of the AI-technologies to the supervisory authorities, to the extent the intellectual property rights over the said technology and LEAs' internal procedures allow it.

Nevertheless, complying with the transparency requirement does not refer to a full transparency towards all stakeholders. For instance, the LEAs can undertake various actions that are not transparent, such as covert investigations, provided that these are justified under the law and also comply with the requirements of necessity and proportionality in a democratic society.[150]

PURPOSE LIMITATION – The principle of purpose limitation aims to ensure that data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

As for the data collection, the principle entails three different requirements.[151] First, the purposes must be specified, meaning that the LEAs must carefully consider and identify the law enforcement-related purposes of the collection and must not collect unnecessary, inadequate or irrelevant data. Second, the purposes must be made explicit without vagueness and ambiguity. Last, the purposes must be legitimate, so to comply with the lawfulness requirement.

As for the further processing, this is allowed insofar as it is compatible with the purposes specified at the collection. A further processing for a different purpose does not have to necessarily be considered as incompatible, but the compatibility has to be assessed on a case-by-case basis,[152] especially in the context of the LED which does not provide further guidance on compatibility between purposes. It has been pointed out that *"law enforcement, per se, shall not be considered as one specified, explicit and*

[148] LED Article 10.
[149] LED Recital 26.
[150] LED Recital 26.
[151] Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation, WP 203' (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 13 July 2022.
[152] ibid.

legitimate purpose".[153] Instead, every individual purpose of processing should be detailed, while two law enforcement purposes should not be *de facto* considered compatible because they belong in the same field.[154]

In the context of the AI technologies explored by ALIGNER, particular attention must be paid to a potential function creep, that is the deployment of AI beyond its originally specified, explicit and legitimate purposes.[155] For example, AI systems intended for specific crime prevention goals might gradually be repurposed for unwarranted surveillance activities not originally considered merely prompted by having the technical possibility of achieving such repurposing. In this way, predictive policing tools may for instance be gradually turned into mass surveillance tools by gradually extending the purposes for which collected data may be used, the connectivity with new databases as well as through the evolution of big data techniques.[156]

DATA MINIMISATION – The principle of data minimisation entails that data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. Therefore, seen the purposes of collection and further processing, LEAs must collect and process only the least amount of data which is necessary for achieving the aforementioned purposes.

The principle of data minimisation is strongly linked to the principles of data protection by design and default, enshrined by Article 20 of the LED. Accordingly, LEAs must implement appropriate technical and organisational measures, in the design and development stage of the processing operations, to effectively implement data protection principles and process only the necessary data.

Moreover, according to Article 5 of the LED, the national law must foresee appropriate time limits for the erasure or a period review of the need for storage of personal data, so to avoid the data to be kept longer than necessary. This means that the AI-based tools that will be identified by ALIGNER must allow the personal data to be removed from the system after a certain time, when the storage of the relevant personal data is not necessary anymore. This could be guaranteed through various methods, such as erasing or anonymising the data. However, complying with this requirement may not always be straightforward, especially for certain AI-based technologies, where it may be difficult to selectively delete certain data from the relevant datasets or anonymise it.

DATA QUALITY – The principle of data quality ensures that the data collected are accurate and kept up to date; inaccurate data must be erased or rectified without delay. The principle is further implemented by Article 7 of the LED, which requires LEAs to take all the reasonable steps to ensure that inaccurate,

---

[153] Article 29 Data Protection Working Party, 'Opinion 03/2015 on the Draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, WP 233' (2015) 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf> accessed 13 July 2022.
[154] European Data Protection Supervisor, 'Opinion on the Data Protection Reform Package' (2012) <https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 13 July 2022.
[155] Stefano Fantin and others, 'Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence', *UNICRI Special Collection on AI in Criminal Justice* (2020) <http://www.unicri.it/sites/default/files/2020-08/Artificial%20Intelligence%20Collection.pdf,> accessed 13 July 2022.
[156] ibid.

incomplete or no longer up to date personal data are not transmitted or made available before a verification of their quality.

STORAGE LIMITATION – The principle of storage limitation provides that data must be kept in a form which allows the identification of data subjects for no longer than is necessary for the purposes for which they are processed. As a consequence, LEAs are obliged to implement appropriate technical measures, such as anonymisation techniques, to ensure that the data can no longer be linked to the concerned natural person after the time required for the purpose of processing passes. Article 5 LED on time limits for storge and periodic review thereby reinforces the storage limitation principles, and should be further read in conjunction with Article 6 LED on data subject categories distinction.[157] Thereby different timeframes should be envisaged for the different categories of data subjects, as further clarified below.

DATA SECURITY – The principle of data security aims to guarantee that personal data are processed in such a manner that ensures their security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Accordingly, Article 29 of the LED requires LEAs to implement technical and organisational measures to ensure an appropriate level of security, seen the possible risks of the processing. Such measures may be designed to, for instance, deny unauthorised persons to access the processing equipment and the personal data and prevent the unauthorised reading, copying, modification or removal of data. Also, LEAs have to keep the logs of the processing operations entailing collection, alteration, consultation, disclosure, combination and erasure of data.[158]

OTHER RELEVANT PRINCIPLES – Aside from those listed in Article 4, the LED contains other principles which are relevant in the present context.

According to Article 6 of the LED, LEAs must make a clear distinction between personal data of different categories of data subjects, and in particular of:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence (e.g., witnesses).

Additionally, according to Article 7 of the LED, personal data based on facts must be distinguished from personal data based on personal assessments.

[157] Article 29 Data Protection Working Party, 'Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), WP258' (2017) 3–6 <https://ec.europa.eu/newsroom/article29/items/610178/en> accessed 13 July 2022.
[158] LED Article 25.

iv. Rights of the data subject

The LED confers data subjects specific and actionable rights; these are: right to information, right to access, right to rectification or erasure of personal data and restriction of processing.

While the concrete modalities of exercise of these rights are largely based on Member States' laws,[159] the Directive provides for some common mandatory requirements. In general, LEAs must make any communication to the data subject in a concise, intelligible and easily accessible form and by using clear and plain language. The information must be provided by appropriate means (i.e., in the same form as the received request), including electronic ones. LEAs must facilitate data subjects in the exercise of their rights: they should address the request without undue delay and provide information free of charge.[160]

RIGHT TO INFORMATION – Article 13 of the LED grants data subjects the right to information. This applies at least as regards to the identity and contact details of the data controller and their data protection officer; the purposes of the processing; the right to lodge a complaint with a supervisory authority and the existence of the right to request access to, rectification or erasure of personal data and restriction of processing. Member States can implement in national law additional mandatory information requirements, as concerns for instance the legal basis of the processing, the storage period, the categories of data recipients. The right to information can be delayed, restricted or omitted if such a measure constitutes a necessary and proportionality measure in a democratic society, with due regard for the rights and freedoms of the natural persons involved, where the information, if provided, would obstruct or prejudice the LEAs activities.

RIGHT TO ACCESS – Pursuant to Article 14 of the LED, data subjects have the right to obtain confirmation on whether their personal data are being processed and, if this is the case, obtain access to the personal data and the information foreseen in Article 13 of the LED. Similarly to the case of the right to information, the right to access can be restricted if such a measure constitutes a necessary and proportionality measure in a democratic society, with due regard for the rights and freedoms of the natural persons involved, where the information, if provided, would obstruct or prejudice the LEAs activities.

RIGHT TO RECTIFICATION OR ERASURE – Article 16 of the LED confers data subjects the right to obtain from LEAs without undue delay the rectification of inaccurate personal data. Where the undertaken processing activities do not comply with the binding principles relating to the processing of personal data, data subjects have the right to request the erasure of the unlawfully processed information. However, LEAs can instead opt for a restriction to the processing when the alleged inaccuracy of the personal data cannot be ascertained or the personal data must be maintained for evidentiary purposes.

[159] LED Article 18.
[160] LED Article 12.

v. Automated decision-making and profiling

Article 11 of the LED provides for a specific discipline applicable to the case of decisions solely based on automated processing (for instance, through the means of AI systems). Even though the Article aims to cover all possible automated decisions solely based on automated means, the immediate referral is that of profiling, defined by the Directive as any form of automated processing of personal data to evaluate or predict certain aspects of a natural person, such has their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[161]

Profiling techniques are widely used in the criminal context. Criminal profiling has been defined by Kocsis as the process in which *"exhibited criminal behaviours are evaluated for the purpose of making some prediction concerning the characteristics of the probable offender, in order to provide information that can assist in criminal investigations"*.[162] Profiling techniques can be implemented in the context of predictive policing, as well as for real-time or post-fact investigative purposes.[163]

Some problematic aspects of profiling were already outlined above, especially as concerns the presumption of innocence [Section 3.1.2] and the right to non-discrimination [Section 3.1.4]. The LED addresses particularly the latter, establishing a series of prohibitions. It must be preliminarily noted that these prohibitions apply only when the final outcome of the automated processing is solely based on it; therefore, whenever a human intervenes in the decision-making process, the safeguards provided by Article 11 of the LED will not be mandatory.

First, automated decisions based solely on automated processing producing an adverse legal effect for the data subject or anyway significantly affecting them are, in principle, prohibited. On the one hand, it is apparent that, for this prohibition to apply, it is not necessary that the outcome of the solely automated processing affects a legal right of an individual: any other significant effects, similar to the legal ones, will trigger its application.[164] On the other hand, this first prohibition suffers an important exception: the automated decision-making is allowed if authorised by a law which provides appropriate safeguards for the rights and freedoms of the data subject and, at least, for the right to obtain human intervention. However, the extent of human intervention, and to what extent it should be substantially meaningful, can be challenging in an environment whereby AI is considered as more objective and reliable than a human being.

Second, automated decisions based solely on automated processing, even if allowed by a law providing for sufficient safeguards, cannot be based on sensitive data. Again, this prohibition suffers of an exception, i.e., that of measures suitable to safeguard the data subjects' rights, freedoms and legitimate interests.

---

[161] LED Article 3(4).
[162] Richard N Kocsis, *Criminal Profiling* (Humana Press 2006) 9 <https://link.springer.com/book/10.1007/978-1-59745-109-3> accessed 13 July 2022.
[163] Naudts (n 99).
[164] For a more detailed overview of the concept of 'significance', see Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01' (2018) <https://ec.europa.eu/newsroom/article29/items/612053/en> accessed 13 July 2022.

Finally, profiling that results in discrimination against natural persons on the basis of sensitive data is prohibited, as already demanded by the principle of non-discrimination [Section 3.1.4]. However, as seen therein, data processing practices like profiling can lead to discrimination even when sensitive data are not used as such, but only through proxies.

Other than being allowed by the LED, criminal profiling can also be considered as a legitimate technique, especially if based on specific intelligence to help identify individual suspects.[165] For ALIGNER, this means that the technologies that will be identified will have to avoid profiling based on data mining techniques, aimed at identifying profiles of individuals susceptible of committing a potential future crime. Also, the technologies identified by ALIGNER will have to take into due account the fundamental rights highlighted above and specifically assess the risk of discriminatory biases and the possibility to further explain and challenge the outcome of the algorithm, so to safeguard the presumption of innocence and right to non-discrimination. Finally, any decision provided by AI technologies identified by ALIGNER should be meaningfully subject to being challenged by the responsible officer who has to take the final decision.

vi. Data protection impact assessment

Among the technical and organisational measures that competent authorities can implement to be able to ensure and demonstrate compliance to the data protection legislation, data protection impact assessments (DPIAs) have a prominent function.

A DPIA is aimed at describing the data processing operations, assessing their necessity and proportionality and helping managing the risks cause by the processing itself.[166] According to Article 27 of the LED, data controllers are obliged to carry out a DPIA whenever the type of processing activities the intend to undertake, especially if these involve the use of new technologies (such as AI tools) are likely to result in a high risk for the rights and freedoms of the individuals involved. It is, therefore, important to underline here that, while DPIAs are generally targeted mostly on the data subjects' data protection rights, they must evaluate and assess the impact on the broader fundamental rights of the individuals, as identified in Section 2 of this work. For fully mitigating the risks caused by the personal data processing, the LED prescribes that DPIAs must be conducted before engaging in the processing activities.

The Directive prescribes the minimum requirements that a DPIA has to fulfil.[167] First, it must contain a general description of the envisaged processing; hover, as also prescribed by the GDPR, seen the potential impact that AI tools used for law enforcement purposes may have on the affected individuals, a systematic description of the intended processing operations is advisable. Second, a DPIA must contain a full and punctual assessment of the risks to the rights and freedoms of the individuals. Finally,

---

[165] European Union Agency for Fundamental Rights, *Towards More Effective Policing : Understanding and Preventing Discriminatory Ethnic Profiling : A Guide* (Publications Office of the European Union 2010) <https://data.europa.eu/doi/10.2811/40252> accessed 13 July 2022.
[166] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP248 Rev.01' (2017) <https://ec.europa.eu/newsroom/article29/items/611236> accessed 13 July 2022.
[167] LED Article 27.

it must enlists the specific measures that LEAs intend to implement for addressing and mitigating the risks previously identified. Even though it seems to be not mandatory in the context of the LED to include in the DPIA an assessment of the proportionality and necessity of the processing in respect to the law enforcement purposes pursued by the LEAs, it is anyway strongly advised to do so.

Conducting a DPIA is an iterative process.[168] It starts with describing the general processing operations and the measures already envisaged for safeguarding the relevant fundamental rights; then, the impact on the rights and freedoms of the individuals is assessed and new mitigating measures are envisaged; finally, this process is continuously monitored and reviewed, when necessary.

Currently, several different methodologies for conducting DPIAs (or more broad human rights impact assessments) have been proposed by both data protection supervisory authorities and legal scholars. The available guidance is mostly focused on the requirements and safeguards established by the GDPR and none of them is specifically tailored on the law enforcement context. However, AI systems used for law enforcement purposes carry specific risks for the rights and freedoms of the individuals (e.g., inaccurate, biased or inexplicable outputs), that are susceptible to impact important fundamental rights of the individuals, including the necessary due process guarantees. While the state-of-the-art can still help LEAs in conducting their DPIAs, more specific and relevant guidance is needed. For this reason, one of the ALIGNER's aim is to design a specific impact assessment methodology to address ethical and legal issues related to the use of AI tools in the context of law enforcement. This methodology will be further illustrated in WP4's D4.2.

3.2.1.2 ePrivacy Directive & ePrivacy Regulation

Adopted in 2002 and undergoing significant changes in 2009, the e-Privacy Directive focuses on privacy and data protection matters in the electronic communications sector, more specifically the processing of personal data within the scope of the provision of publicly available electronic communications services[169] in public communications networks in the EU (Article 3 e-Privacy Directive). It complements and particularises the GDPR, and supplements the issues that fall outside the GDPR's scope, such as the protection of the content of communications and information stored or accessed on a personal device.

The scope of the Directive includes traffic data, location data, content of the communications, as well as cookies placed on people's personal electronic devices.

---

[168] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP248 Rev.01' (n 166).

[169] Article 2 of the Directive describes electronic communications service as "a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

The e-Privacy Directive does not apply to *"activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law"* (Article 1(3) e-Privacy Directive). Nevertheless, the CJEU has confirmed that the scope of the e-Privacy Directive extends to the collection and processing of traffic and location data by electronic communications services providers even in the context of security. The e-Privacy Directive thereby applies when the security authorities ask for these data collected by electronic communications service providers.[170] Therefore, due to the fact that electronic communications data may be quite relevant for the development and functioning of the AI-based tools that will be identified under ALIGNER, the e-Privacy Directive should be taken into account.

It shall be noted that the Directive is in the process of being replaced with an e-Privacy Regulation. The proposal for the e-Privacy Regulation[171] has been published in 2017, with the aim of modernising e-privacy and aligning it with the GDPR. The new Regulation aims to cover a wider range of communication services, going beyond the traditional telecommunications operators. As a result, the Regulation will include machine to machine communications (for instance via Internet of Things devices) and modern voice-over-IP services such as Whatsapp, Zoom, Skype, Gmail and Viber, as well as communications on publicly accessible networks, such as public Wi-Fi networks. Like in the case of the e-Privacy Directive, due to the CJEU's case law, the Regulation will be applicable[172] when the security authorities ask for the relevant data collected by electronic communications service providers.

While the proposal has been subject to heated discussions in the five years that followed, undergoing many changes, without seeing much progress, its heavily revised text was adopted in February 2021 for negotiations with the European Parliament.[173]

3.2.1.3 Legal framework on the collaboration between LEAs and EU Agencies[174]

The EU Agencies focusing on cybercrime and security, namely Europol, Eurojust and European Public Prosecutor's Office (EPPO) play an important role in the data exchange among LEAs and other relevant

[170] For more information, see Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2020] ECLI:EU:C2020:790, and Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others [2020] ECLI:EU:C:2020:791.
[171] Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 Final - 2017/03 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> accessed 13 July 2022; see also Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for Negotiations with EP, 10 February 2021, No 6087/2.
[172] Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2020] ECLI:EU:C2020:790, and Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others [2020] ECLI:EU:C:2020:791 (n 170).
[173] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for Negotiations with EP, 10 February 2021, No 6087/2 (n 171).
[174] F Coudert, 'The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to ... What Exactly?' (2017) 3 European Data Protection Law Review 313; T Quintel, 'European Union · The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation' (2022) 8 European Data Protection Law Review 90.

institutions across Europe. The data shared between LEAs and EU Agencies has a significant potential for the development and deployment of the AI-based tools that LEAs may benefit from. Whereas Regulation 2018/1725 concerning the processing of personal data by the Union institutions, bodies, offices and agencies provides the broader framework for operational data similar to the LED, a few additional distinct instruments regulate this operational data sharing between LEAs and certain EU agencies.

One of the instruments, the Regulation 2016/794 (Europol Regulation),[175] specifies the role of Europol and the modalities of the data exchange between Member States, Europol and relevant authorities. According to the Europol Regulation, when organized crime, terrorism and other specific forms of serious crime affect two or more Member States, Europol supports the competent authorities of the Member States to prevent and combat crime (Article 3 Europol Regulation). It acts as an information hub for the affected States, helps them exchange information, as well as analyse and assess the intelligence and the threats they receive (Article 4(1)(a)), with the help of the Europol Information System.

The Europol Information System is a database which allows Member States to exchange criminal intelligence and share information among themselves, especially relating to individuals who *"are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence"* (Annex II of the Europol Regulation, A-1(a)) or *"persons regarding whom there are factual indications or reasonable grounds* […] *that they will commit such offences"*.[176] Overall, there are strict conditions to the personal data transfers by and to Europol. For instance, Europol can transfer personal data to EU authorities only to the extent that such transfer is necessary for the performance of the task of Europol or the EU authority. Exchange of personal data in this context can have a significant role in the development of AI-driven tools to be deployed by LEAs, therefore the requirements set forth under the Europol Regulation are relevant within the scope of ALIGNER and will be monitored in line the project activities.[177]

Whether Europol complies with the data protection and privacy legal framework within the scope of its personal data processing activities is monitored by the European Data Protection Supervisor (EDPS). The EDPS investigates complaints regarding Europol's data processing activities and also advises Europol (Articles 43 and 44 Europol Regulation).

Following a recent investigation, in January 2022, the EDPS ordered Europol to delete all personal data it held on individuals who were not previously involved in or had any connection to a criminal activity. The EDPS' inquiry demonstrated that the agency had been receiving great amounts of personal data from national authorities and processing the said data violating a number of data protection and

[175] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and Replacing and Repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135/53.
[176] European Union Agency for Fundamental Rights and others (n 106) 301.
[177] ibid 300–301.

privacy obligations they had. For instance, Europol was processing the data without specifying whether it concerned innocent individuals or those linked to a criminal activity, which violates the requirement according to which Europol should categorize its data subjects indicating what role they may have in a criminal proceedings. Moreover, the agency engaged in data processing in this manner for at least six years, and stored the relevant data without a clear and valid legal basis, breaching the data minimization and storage limitation principles under the Europol Regulation. Europol argued that, due to the great quantity of data received from national authorities, it was very difficult to analyse it and determine what category each individual that is included in the database belongs to in a period of six months as required by the EPDS.[178]

The order by the EDPS requiring Europol to delete all such data received significant attention, as it clearly pointed to the severe violations of the privacy and data protection framework by Europol. Pointedly, following this order, the draft regulation amending the Europol Regulation, which has been in the works since 2020, underwent swift changes. These changes introduced new data processing capabilities for Europol, in a manner to retroactively allow the storage and processing of personal data of which the EDPS had ordered the deletion (Article 18a of the recast Europol Regulation). These swift changes were met with concern and criticism among academics and civil society.[179] The developments surrounding the EDPS' order and the Recast Europol Regulation may shed light into the potential pitfalls of data processing activities by LEAs by using the AI-driven tools, as well as provide some clues regarding capability enhancement needs to speed up data analysis by LEAs. Therefore, these developments require close attention and will be followed throughout the project.

The recast Europol Regulation also includes requirements for a close cooperation with Eurojust and the European Public Prosecutor's Office. With regards to the cooperation with EPPO, the recast regulation stipulates that Europol will support EPPO in its investigations, upon EPPO's request, and it will report to EPPO any criminal conduct that falls within its competence. EPPO will also be able to access data held by Europol, following the requirements stipulated under the recast Europol Regulation (Article 20a).

3.2.1.4 Relevant CoE privacy and data protection instruments

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe (CETS No. 108),[180] (Convention 108) was drafted by the CoE in 1980 and adopted in 1981. Convention 108 aims to protect individuals in relation to the automatic processing of their personal data and covers all aspect of it, including the data processing activities taking place in the field of police and criminal justice. Another important aim is to ensure the free flow of data

[178] Quintel (n 174).
[179] ibid.
[180] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe (CETS No. 108), Adopted on 28.01.1981, as Amended by Protocol CETS No. 223, 2018.

between the signatories while limiting the flow to countries that do not protect personal data on an equivalent level.

Although there had been instruments before which included similar principles, such as the OECD Guidelines, Convention 108 differs from those previous ones thanks to its legally binding nature. It signalled the beginning of a new phase in European data protection and had a significant influence over the subsequent data protection laws in the CoE states.[181] Its resounding influence can be observed in the repealed Data Protection Directive 95/46/EC, as well as the GDPR and the LED.

According to Convention 108, data should be collected and processed in a fair and lawful manner. This processing shall be based on specific and legitimate purposes; in other words, the data should not be processed for other non-compatible purposes. The data collection and processing should not be excessive, the data shall be adequate, relevant and accurate and not stored for longer than necessary. Convention 108 prohibits processing sensitive data unless national laws provide adequate safeguards. In this context, sensitive data include a person's race, religion, health, politics, sexual life and criminal record. The convention also includes data security measures and certain rights for individuals whose data are processed. Accordingly, individuals shall have the right to know that their personal data is stored and, where applicable, to have it corrected, except for the cases when the reasons of public security prevents it.

In line with the changing needs in the 21st century, the Convention 108 underwent a modernisation process in May 2018, with the amending protocol CETS No. 223. The aim was to provide stronger protection of privacy and ensure that the Convention's follow up and enforcement mechanisms are effective. The resulting modernised instrument, Convention 108+[182] closely resembles the current EU data protection framework and embodies equivalent principles, already explored above in Section 3.2.1.1.

Another relevant instrument relating to the Convention 108 is the CoE's Recommendation (87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector[183] (CoE Police Recommendation). Adopted in 1987, it provides recommendations in the form of principles, tailored to more specific problems that may be experienced by LEAs within the scope of their activities, especially about the collection, storage, use and communication of personal data. It aims to help LEAs strike a balance in the face of clashing interests of national security and prevention of crime and the rights to privacy and data protection.

---

[181] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014) 93 <http://link.springer.com/10.1007/978-3-319-05023-2> accessed 13 July 2022. Gonzalez Fuster emphasizes the particular influence of the Convention for the adoption of the Act on the automated processing of data in the United Kingdom on 1984, of the Irish and Finnish Data Protection Acts in 1988.

[182] Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 13 July 2022.

[183] Committee of Ministers of the Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector' <https://rm.coe.int/168062dfd4> accessed 13 July 2022.

The CoE Police Recommendation went through a number of updates in 1993, 1998 and 2002 to ensure its effective application and relevance. Even with the fast-paced developments of the 2010s, it continued to be relevant in guiding and clarifying national regulations concerning the police use of personal data. Moreover, the CoE Police Recommendation was supplemented with a "Practical guide on the use of personal data in the police sector" in 2018.[184] As its name suggests, this guide mainly aims to provide practical guidance to LEAs, with concrete examples as to how a balance may be struck between the rights to data protection and privacy and the public interests through the broad range of activities undertaken by LEAs.

More recently, CoE's Consultative Committee of Convention 108 provided "Guidelines On Artificial Intelligence And Data Protection".[185] Taking the modernised Convention 108+, these guidelines include some minimum measures that can be adopted to ensure protection of human dignity, fundamental rights and freedoms, especially concerning data protection-related aspects of the use of AI technologies. The guidelines are divided into three sections, including a section with general guidance points, another one tailored towards AI developers, manufacturers and service providers, and a final section with specific guidelines for legislators and policy makers.[186]

The guidelines repeat the importance of "*lawfulness, fairness, purpose specification, proportionality of data processing, privacy-by-design and by default, responsibility and demonstration of compliance (accountability), transparency, data security and risk management*"[187] as key elements. They state that the efforts in this direction should not be limited to protecting human rights and fundamental freedoms, but also include democratic, social and ethical values.

The guidelines reiterate the concerns expressed in similar documents, emphasising the importance of impact assessments, human rights by-design approach, avoiding biases and discrimination, quality of data, dialogue and consultation between stakeholders, preventative approaches etc. A few of the more original points raised by the guidelines concern the suggestion for the use of synthetic data for data minimisation, the potential adverse impacts of de-contextualised data and algorithmic models on individuals and society, the need for cooperation between different supervisory authorities, such as data protection, consumer protection, competition, anti-discrimination, sector regulators and media regulatory authorities and the importance of the independence of oversight committees.

---

[184] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Practical Guide on the Use of Personal Data in the Police Sector' <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> accessed 13 July 2022.

[185] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 'Guidelines on Artificial Intelligence and Data Protection' <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> accessed 13 July 2022.

[186] Another guideline document by the same consultative committee has been published, with a focus on facial recognition. Due to its specific focus it wasn't included in this deliverable, nevertheless it can be a valuable source in guiding LEAs for the use of facial recognition technologies. For more information, see Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 'Guidelines on Facial Recognition' <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> accessed 13 July 2022.

[187] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (n 185) 1.

3.2.2 The Regulation on the Free Flow of Non-Personal Data

The Regulation on the free flow of non-personal data[188] (NPDR), was adopted in November 2018 and entered into force on 19 June 2019. Significantly, it is the first legislation which focuses on non-personal data, positioned opposite the GDPR and the LED. The reason behind its adoption was to benefit from various types of machine-generated data that falls out of the scope of the definition of personal data, and as a result, foster the digital economy and innovation.[189] The NPDR defines non-personal data as any data other than personal data as defined in the GDPR. It stipulates provisions concerning data localisation requirements; the availability of data to competent authorities, including the LEAs;[190] and the porting of data for professional users.[191]

The NPDR introduces rules prohibiting data localisation (Article 4 NPDR). According to the Regulation, data localisation requirements are prohibited, *"unless they are justified on grounds of public security in compliance with the principle of proportionality"* (Article 4(1) NPDR). As a result, companies and individuals have the opportunity to freely move data across EU borders. The same applies to the competent authorities, which shall be able to request or obtain access to data for the performance of their duties, even if the data is processed in another Member State (Article 5(1) NPDR).

The competent authorities may request data from other competent authorities as well as other natural or legal persons. If a competent authority has difficulties obtaining access to the requested data, it may ask for the assistance of another competent authority from a different Member State, by following the procedures set out under the NPDR, especially if there are no other specific cooperation mechanisms[192] between the two Member States. (Article 5(2) NPDR). Accordingly, the requesting Member State contacts the single contact point designated by the other Member State, and submits a request which contains the reasons behind the request and the justifying legal grounds (Article 7(2) NPDR). Upon receiving this request, the single contact point identifies the relevant competent authority in the receiving Member State and transmits the request to that authority (Article 7(3) NPDR), which must respond as quickly as possible, either sending the requested data or explaining why it cannot do so. (Article 7(4) NPDR). Finally, a principle similar to purpose limitation is identified under Article 7(5) of the NPDR, and accordingly, the data received through these requests cannot be used for purposes other than the ones explained in the request.

---

[188] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 ("Non-personal data Regulation", "NPDR").
[189] European Parliamentary Research Service and Mar Negreiro, 'Briefing - EU Legislation in Progress - Free Flow of Non-Personal Data in the European Union' <https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614628/EPRS_BRI(2017)614628_EN.pdf> accessed 29 October 2021.
[190] NPDR Article 3(6).
[191] NPDR Article 1.
[192] Such as Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1, the Convention on Cybercrime of the Council of Europe, CETS No 185, Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters [2001] OJ L 174/1, Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax [2006] OJ L 347/1, and Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax [2010] OJ L 268/1.

Within the scope of ALIGNER, the NPDR facilitates the LEAs' access to non-personal data which they need to develop specific AI-driven tools, and which may be found in another Member State, either with another LEA, a different authority or another natural or legal person.

3.2.3 EU Directives concerning the procedural rights of the suspected and accused persons

In 2009, the European Union adopted a roadmap aiming to strengthen the procedural rights of suspected or accused persons in criminal proceedings,[193] which led to the adoption of six binding directives regarding certain procedural rights in criminal proceedings: the right to information;[194] the right to interpretation and translation;[195] the right to have a lawyer;[196] the right to be presumed innocent and to be present at trial;[197] special safeguards for children suspected and accused in criminal proceedings;[198] and the right to legal aid.[199] The rules and safeguards established under these directives also have binding force on member states through the national laws that implementing them.

RIGHT TO INFORMATION – One of the most relevant directives in this context for ALIGNER is the Directive 2012/13,[200] which focuses on the right to information. It is applicable from the moment an individual is made aware by competent authorities that they are a suspect or accused of a criminal offence, and up to the conclusion of the criminal proceedings.[201] The right to information also encompasses other rights and freedoms, such as the right to legal assistance (in other words, the right of access to a lawyer and the entitlement of free legal assistance), the right to receive information about the charges against them, the right to an interpreter and translation of legal documents, and the right to remain silent. According to Directive 2012/13, the information in this context must be provided expeditiously and in a manner to enable the individual to effectively exercise their rights. For ALIGNER, this Directive appears to be particularly relevant in all the occasions in which AI-driven tools are used by LEAs for their decision-making processes and an individual requests information about the reasons of suspicion or accusations against them.

---

[193] Resolution of the Council of 30 November 2009 on a Roadmap for Strengthening Procedural Rights of Suspected or Accused Persons in Criminal Proceedings [2009] OJ C 295/1.
[194] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the Right to Information in Criminal Proceedings [2012] OJ L 142/1.
[195] Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the Right to Interpretation and Translation in Criminal Proceedings [2010] OJ L 280/1.
[196] Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the Right of Access to a Lawyer in Criminal Proceedings and in European Arrest Warrant Proceedings, and on the Right to Have a Third Party Informed upon Deprivation Of liberty and to communicate with third persons and with consular authorities while deprived of liberty [2013] OJ L 294/1.
[197] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 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 [2016] OJ L 65/1.
[198] Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on Procedural Safeguards for Children Who Are Suspects or Accused Persons in Criminal Proceedings [2016] OJ L 132/1.
[199] Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on Legal Aid for Suspects and Accused Persons in Criminal Proceedings and for Requested Persons in European Arrest Warrant Proceedings [2016] OJ L 297/1.
[200] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the Right to Information in Criminal Proceedings [2012] OJ L 142/1 9 (n 194).
[201] A criminal proceeding is understood to be finished when the question regarding the suspicion or accusation of the individual has been solved by way of a final judgement or resolution. See Marquenie and others (n 67) 36.

RIGHT TO BE PRESUMED INNOCENT – Another relevant directive in the context of ALIGNER is the Directive 2016/343 on the right to be presumed innocent and to be present at the trial,[202] considering how AI-driven technologies, especially predictive policing tools present significant risks for the presumption of innocence. The Directive applies to suspects or accused persons throughout the duration of criminal proceedings, from the moment a suspicion arises or an accusation is made, until the moment the decision about whether that person has committed the crime becomes final.[203] Importantly, the Directive strengthens the presumption of innocence with rules concerning, among others, the burden of proof, the right to remain silent and the right not to incriminate oneself.

3.2.4 AI Act Proposal

In April 2021, the European Commission published its proposal for a regulation laying down harmonised rules on artificial intelligence[204] (AI Act Proposal). With the proposed Regulation, the Commission aimed to enhance and foster the development of a single market for AI applications, while at the same time laying down specific safety requirements, capable of ensuring and effectively enforcing EU values and fundamental rights safeguards. To achieve this two-fold objective, the Proposal adopts a horizontal regulatory approach, providing for a flexible and future-proof legal framework which is applicable, in principle, to all 'AI systems' throughout their whole lifecycle. This new piece of legislation is meant to complement the already existing sectoral legislation, such as the LED.

i. Scope of application

The AI Act Proposal provides for a definition of 'AI systems' that aims to both ensure legal certainty and be flexible, so to be applicable to future technological developments.[205] To this end, the benchmark is the key functional characteristic of an AI software, namely its ability to generate different outputs (e.g., content, prediction, recommendations or decisions) for different given sets of human-defined objectives.[206] Annex I to the proposed Regulation enlists several techniques that can be used to develop AI systems, such as supervised and unsupervised machine learning, logic- and knowledge-based approaches and, finally, statical approaches.

The proposed AI Act has a broad scope of application, both from a material and territorial perspective.[207] As for the first, the AI Act Proposal applies to two categories of subjects:

[202] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 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 [2016] OJ L 65/1 (n 197).
[203] Directive 2016/343 (n 197) Article 2.
[204] 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, 2021/0106(COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> accessed 13 July 2022 ('AI Act Proposal').
[205] AI Act Proposal Recital (4).
[206] AI Act Proposal Article 3(1).
[207] AI Act Proposal Article 2.

a. ‘providers’, meaning any natural or legal persons, public authorities, agencies or bodies that develop or own AI systems to place them on the market or put them into service, whether against payment or for free; and
b. ‘users’, meaning any natural or legal persons, public authorities, agencies or bodies that use AI systems under their authorities, unless they are carrying out a non-professional activity.

As for the second, the AI Act Proposal applies to users located within the EU; providers established both in the EU and in third countries, as long as they are targeting the internal market; and providers and users located in third countries, if the output produced by the AI system is used in the EU.

Importantly in ALIGNER context, the Proposal does not apply to AI systems developed or used exclusively for military purposes nor to public authorities located in third countries or international organizations, if in the framework of international agreements for law enforcement and judicial cooperation.

ii. Risk-based approach

To ensure a high-level of protection for fundamental rights and EU values, the AI Act Proposal adopts a risk-based regulatory approach, as similarly done within the context of the data protection legislation.

The underlying assumption is that AI systems may generate risks and cause material and immaterial harm to public interest and rights protected by EU law, depending on the circumstances and their specific uses.[208] The type and content of the obligations and requirements introduced by the Regulation are, therefore, based on a sector-by-sector and case-by-case approach, taking specifically into account the intensity of the possible risks generated by AI systems.[209] To this end, the AI Act Proposal distinguishes between AI uses that create an unacceptable risk, a high risk and a low or minimal risk.

AI USES CREATING AN UNACCEPTABLE RISK – Article 5 of the AI Act Proposal prohibits certain AI practices which create an unacceptable risk, as they contravene EU values by violating fundamental rights. The prohibition covers four specific use cases.

The first two prohibitions tackle the misuse of AI systems with the aim of (a) deploying subliminal techniques beyond a person’s consciousness; or (b) exploiting vulnerabilities of specific group of persons, both in order to materially distorting their behaviour to cause physical or psychological harm. These uses are, indeed, contradicting several values protected by other already existing pieces of EU legislations, such as human dignity, right to non-discrimination, democracy, right to data protection and privacy.

[208] AI Act Proposal Recital (4).
[209] AI Act Proposal Recital (14).

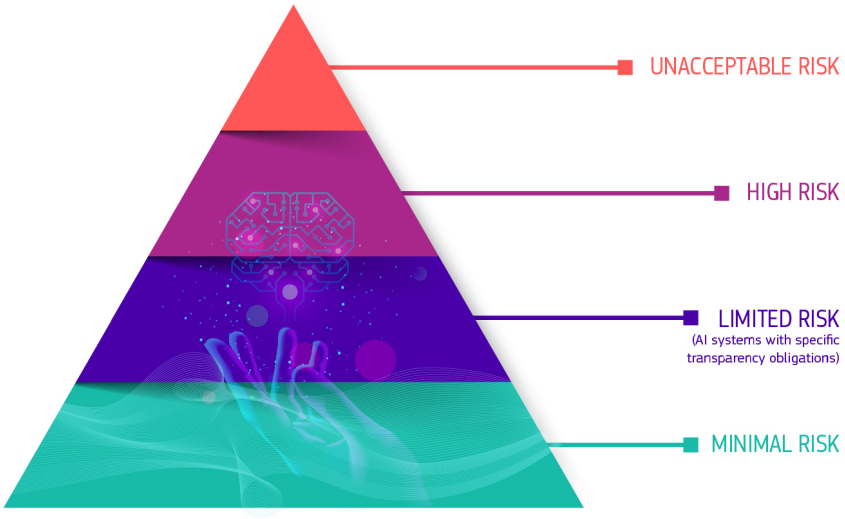

Figure 2: Risk levels specified under the AI Act Proposal[210]

The third prohibition covers AI applications used by public authorities to evaluate the trustworthiness of a natural person on the basis of their social behaviour or personality characteristics (i.e., the so-called 'social scoring'), when this evaluation leads to a detrimental treatment either in an unrelated context or of a disproportionate gravity. These practices may violate the right to dignity and non-discrimination and, if used in a judicial context, also the right to a fair treatment and due process.

Of particular relevance for ALIGNER is the fourth and last prohibition, which addresses the use of 'real-time' remote biometric identification systems in public accessible spaces for the purpose of law enforcement. To fall within the prohibition, the AI system has to fulfil four conditions:

(1) The AI tool has to be designed specifically with the purpose of identifying natural persons at a distance, by matching their biometric data (as defined in the LED) with those contained in a reference database;
(2) The identification process, from the moment of the collection of data to that of the identification in itself, has to occur in real time, or without any significant delay;
(3) The AI tool has to be deployed in any physical place which is accessible to the public; and
(4) The AI tool has to be used for law enforcement purposes.

As a consequence, the prohibition foreseen in the AI Act Proposal does not cover 'post' remote biometric identification systems, where the identification process occurs with a significant delay. 'Post' remote biometric identification tools are, instead, to be considered as high-risk AI applications [see next paragraph of this section].

[210] European Commission, 'Regulatory Framework Proposal on Artificial Intelligence' (Shaping Europe's Digital Future) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 2 June 2022.

AI systems allowing 'real-time' remote biometric identification, especially if deployed in publicly accessible areas and for law enforcement purposes, are capable of having numerous fundamental rights implications. They are considered to be particularly intrusive in the fundamental rights and freedoms of the natural persons involved and they are capable of having a severe chilling effects, due to the risk of mass surveillance they invoke. For this reason, the Proposed Regulation introduces this specific prohibition, which should apply as *lex specialis* to the regime already provided by Article 10 LED (meaning that the Proposed Regulation would override the LED in case of conflicting rules).

Nevertheless, this last prohibition suffers major exceptions which significantly undermine its effectiveness, in favour of reasons of public interest. The use of 'real-time' remote biometric identification tools is allowed, if strictly necessary, for the targeted search of specific potential victims of crime; for the prevention of a specific, substantial and imminent threat to the physical safety of natural persons or in case of a terrorist attack; and for the detection, identification or prosecution of a perpetrator or suspect of one of the offences listed in Article 2(2) of the Council Framework Decision 2002/584/JHA.[211] In assessing the strict necessity to use these AI tools, LEAs should consider both the harm caused in the absence of the use of the system and the consequences of its use for the rights and freedoms of all individuals concerned, by taking also into account the mandatory safeguards and conditions imposed by the other relevant legislation. In particular, the use should be subject to limits in time and space and circumscribed to specific threats, victims or (suspect) perpetrators. The use of AI tools for 'real-time' identification should be preceded by a judicial authorisation, issued upon reasoned request and in accordance with national law. However, in case of a situation of urgency, the authorisation can also be requested after the use has started, or even after it.

AI USES CREATING A HIGH-RISK – Article 6 of the AI Act Proposal identifies two different categories of high-risk AI systems, based on their intended purposed and modalities of use.

The first category of high-risk AI applications covers AI systems that fulfil two cumulative conditions:

(a) The AI system is intended to be used as a safety component of a product, or is itself a product, covered by harmonised EU product safety legislation;[212] and
(b) Before being placed on the market, the aforementioned product has to go under a third-party conformity assessment.

---

[211] The criminal offences therein listed are the following: participation in a criminal organisation; terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; corruption; fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests; laundering of the proceeds of crime; counterfeiting currency, including of the euro; computer-related crime; environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties; facilitation of unauthorised entry and residence; murder, grievous bodily injury; illicit trade in human organs and tissue; kidnapping, illegal restraint and hostage-taking; racism and xenophobia; organised or armed robbery; illicit trafficking in cultural goods, including antiques and works of art; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery of administrative documents and trafficking therein; forgery of means of payment; illicit trafficking in hormonal substances and other growth promoters; illicit trafficking in nuclear or radioactive materials; trafficking in stolen vehicles; rape; arson; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; sabotage.

[212] As enlisted by AI Act Proposal Recital (30), these are: machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.

These AI systems are particularly susceptible of causing severe risks to the health and safety of persons. For this reason, the Proposed Regulation seeks specifically to mitigate these risks, as similarly done by the already existing product safety legislation in the case of non-digital products. The Regulation, therefore, aims to also complement the latter instruments so to adapt the legal framework to the AI specificities.

The second category of high-risk AI applications consists of stand-alone AI systems with fundamental rights implications, as listed by Annex III to the Proposed Regulation. The Annex currently consists of eight areas of application, of which the most relevant for ALIGNER are:

(1) Biometric identification and categorisation of natural persons, including 'real-time' and 'post' remote biometric identification;
(2) Law enforcement, including predictive policing tools, polygraphs or similar instruments, tools to detect deep fakes, systems used to evaluate the reliability of criminal evidence and, in general, profiling tools and systems used for crime analytics using large datasets to identify unknown patterns;
(3) Migration, asylum and border control management; and
(4) Administration of justice and democratic processes.

AI systems operating in these areas are particularly susceptible of leading to surveillance, arrest or discrimination.[213] They can also harm the exercise of other fundamental rights, such as the right to fair trial or the presumption of innocence.

The EU Commission can further expand this list, always within the same areas of application, when it finds new AI systems posing equivalent or greater risks of harm in comparison with the uses already referred to in the Annex. The specific criteria informing the Commission's evaluation are provided by Article 7 of the Regulation, and they stem from a risk-based methodology.[214] However, these criteria have been subject to some criticisms, according to which they are not specific enough and are not based on a concrete rationale, which would eventually enable political choices to have an undue influence on the determination of the new high risk AI systems.[215]

The AI Act Proposal foresees specific horizontal legal requirements for high-risk AI systems. These requirements are not to be considered a novelty in themselves, as they were already part of the state-of-the-art represented, for instance, by the Ethics Guidelines for Trustworthy AI issued by the High-Level Expert Group on Artificial Intelligence [Section 2.3.1]. Nonetheless, the importance of the AI Act stands in transposing these ethical principles in a legally binding end enforceable act. The Proposed Regulation establishes, indeed, the obligation for AI providers to ensure full compliance with the legal requirements provided in the same act.[216] Providers are also subject to a conformity assessment before

[213] AI Act Proposal Recital 38.
[214] For instance, the Commission has to take into account the intended purpose of the AI system, the extent to which it is used, the extent to which it has already caused harm along with its intensity and ability to affect a plurality of persons.
[215] Ilina Georgieva, Tjerk Timan and Marissa Hoekstra, 'Regulatory Divergences in the Draft AI Act - Differences in Public and Private Sector Obligations' (European Parliamentary Research Service 2022) IV–V.
[216] AI Act Proposal Article 16.

an independent third party (i.e., the notified body), designated in accordance to the Regulation. While AI users are, in general, mainly responsible for using AI systems in accordance with the instruction of use accompanying the systems,[217] they may assume the same obligations as of the provider, if they place on the market the AI application under their name; or if they modify the intended purpose or anyway make substantial modifications to the AI application.[218]

Preliminarily, providers have to establish, implement, document and maintain a risk management system.[219] This is a continuous iterative process run during the whole AI system lifecycle, which consists of four steps:

(1) Identify and analyse the known and foreseeable risks;
(2) Estimate and evaluate the risks that may emerge from both normal use and foreseeable misuse;
(3) Evaluate other possible risks, on the basis of information collected after the placing on the market; and
(4) Taking into account the state of the art, adopt suitable risk management measures.

High-risk AI systems are subject to higher data quality standards.[220] Training, validation and testing datasets must be relevant, representative, free of errors and complete. To this aim, providers should implement appropriate data governance practices, such as relevant labelling, formulation of relevant assumptions, prior assessment of the datasets and examination in view of possible biases. Also, high-risk AI systems must be developed so to ensure an appropriate level of accuracy, robustness and cybersecurity during their whole lifecycle.[221]

The development of high-risk AI systems must ensure a sufficient degree of transparency, so that users can interpret their outputs.[222] Finally, high-risk AI systems must include an appropriate human-machine interface that allows natural persons to oversee their use and minimise the risks, by monitoring their operation, interpreting the output and eventually deciding to override it.[223]

AI USES CREATING LIMITED OR MINIMAL RISKS – Article 52 of the AI Act Proposal establishes minimal transparency obligations for AI systems creating limited risks. Whenever AI applications are intended to interact with natural persons or generate content (e.g., chatbots) and this may pose specific risks of impersonation or deception, providers are obliged to ensure that system acts in such a way that natural persons are informed they are interacting with AI, unless this appears to be obvious from the circumstances or context of use. This obligation does not apply to AI systems deployed in a law enforcement context.

[217] AI Act Proposal Article 28.
[218] AI Act Proposal Article 29.
[219] AI Act Proposal Article 9.
[220] AI Act Proposal Article 10.
[221] AI Act Proposal Article 15.
[222] AI Act Proposal Article 13.
[223] AI Act Proposal Article 14.

Finally, AI systems creating minimal or no risks, such as AI-enabled videogames or spam filters, can be designed and used freely.

iii. Current developments and criticisms towards the proposal

When adopted, the AI Act will have a broad impact on the activities of LEAs. According to the Commission's draft, the use of AI systems in the field of law enforcement has to be considered as a high-risk application; LEAs will, therefore, be obliged to ensure and demonstrate compliance with the enhanced legal requirements established by the Regulation. In addition, LEAs will have to comply with the ban on 'real-time' biometric identification, unless one of the foreseen exemptions applies.

The exact extent of the impact the AI Act will have on LEAs will be, anyway, known only after the European Parliament and the Council of the European Union will have agreed on a common position. The co-legislators are now still finalising their respective positions and negotiations will start immediately afterwards.

In the meantime, there have been various criticisms towards the proposal.[224] A joint opinion of the European Data Protection Board (EDPB) and of the EDPS underlines the important data protection implication of the Proposal, thus calling for a stronger alignment with the rights and principles established by the EU data protection framework. In particular, the EDPB and the EDPS suggest to explicitly enlist as a mandatory requirement in the Proposal the compliance with the GDPR and the LED. Moreover, the two authorities invoke a stricter approach to the issue of remote biometric identification, by suggesting a more general ban on any use of AI systems for the automated recognition of human features in publicly accessible spaces.

Also, a recent report by the European Parliamentary Research Service highlights some of the problematic aspects of the AI Act, more specifically the diverging approaches the proposal adopts towards public and private actors.

First, the report addresses the different treatment of risk levels of manipulative AI systems such as deepfakes, when these systems are deployed by public and private actors. The AI Act categorizes deepfakes themselves as low-risk, whereas it categorizes the deepfake detection tools used by LEAs to prevent online manipulation as high-risk systems. As a result of this categorization, ironically, the actors who deploy these manipulative AI systems are faced with far less burdens compared to the those trying to prevent the harms that may be caused by these systems.[225] This point is reminiscent of the criticisms according to which there is no evident criteria or concrete reasoning to be used when categorizing AI systems in different risk levels.[226] The classification of risk levels is seemingly not evidence based and

---

[224] European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (2021) <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 13 July 2022; Tambiama Madiega and European Parliamentary Research Service, 'Briefing - EU Legislation in Progress - Artificial Intelligence Act' <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>.
[225] Georgieva, Timan and Hoekstra (n 215) III.
[226] ibid IV–V.

could be amended on the basis of political choices, which can create uncertainties for the users and producers of these AI systems.

Second, when it comes to social scoring a distinction between public and private authorities using the AI system is observed. However, due to the ever increasing influence of the private actors (as can be observed in the cases of Google, Meta and Amazon), the power asymmetry between these private actors and citizens has reached levels comparable to those between public actors and citizens. Therefore, the AI systems deployed by private authorities have the potential to be equally harmful. Making a distinction between public and private actors may leave gaps in the protection that the AI Act aims to provide.

Finally, another criticism towards the AI Act is that the transparency obligations in the Proposal do not go beyond being mere "policy aspiration", as they are not directly stipulated through subjective rights. Moreover, the LEAs are exempted from the disclosure obligations, which can be problematic as this exemption limits the chances of the individuals to become aware of the AI systems deployed that may affect them and protect themselves accordingly. In light of this, the authors of the report suggest "*to clarify and directly stipulate in the AIA's provisions how GDPR rights and remedies are applicable to the addressees of AI systems, especially so when data rights are involved; and 2) to further critically assess the connection between the AIA's transparency obligations and redress mechanisms by strengthening information and disclosure obligations with withdrawal rights.*"[227]

3.2.5 Lawfulness of evidence [228]

In criminal proceedings, both the prosecution and defence use evidence to prove the facts of the case and the validity of their claims. One definition for evidence is *"information by which facts tend to be proved"*.[229] Both parties can prove or refute contentious points raised in the criminal proceedings by evaluating the evidence presented. Therefore, evidence plays a vital role in criminal proceedings,[230] to establish various elements of the crime as well as to identify the perpetrator or the victim.

AI-driven tools have a great potential to benefit LEAs by enhancing their capabilities when it comes to collecting, preserving, using and exchanging, in other words 'processing' evidence. They can enable police forces to quickly process vast amounts of data, which would normally be a taxing effort for the human officers, and therefore, these tools can ease the burden on human resources.[231] The AI-driven tools can also uncover evidence that are undetectable to humans, by searching for clues in images to

[227] ibid V.
[228] Quezada-Tavárez, Vogiatzoglou and Royer (n 79). See also, EVIDENCE project; Balázs Garamvölgyi and others, 'Admissibility of Evidence in Criminal Proceedings in the EU' [2020] eucrim - The European Criminal Law Associations' Forum 201.
[229] Olivier Leroux, 'Legal Admissibility of Electronic Evidence' (2004) 18 International Review of Law, Computers & Technology 193, 196.
[230] Mark Valport and Elizabeth Surkovic, 'Annual Report of the Government Chief Scientific Adviser 2015. Forensic Science and Beyond: Authenticity, Provenance and Assurance' 16.
[231] Considering the explanations above in Section 3.2.1.3, concerning Europol's difficulties in analyzing the vast amounts of data sent to them by national authorities, such tools would provide many benefits and enhance LEAs capabilities significantly.

detect faces and various objects, identifying patterns and matching various information in datasets.[232] Through collecting and analysing pieces of information that may initially not make sense to humans analysts, these tools can reveal meaningful information, which can subsequently become pivotal evidence in a criminal proceeding.[233]

LEAs need to comply with various legal requirements and criminal procedural rules in order to make sure that the evidence they obtain during criminal investigations can be lawfully used during a trial.[234] Like other types of evidence, the evidence gathered, handled or processed by AI-driven tools (in short, AI evidence) also needs to be lawfully obtained. For this reason, any data that is encountered during a criminal investigation must be treated in line with these procedural rules, for the whole duration of the investigation. If not, it may not be possible to present such data as adducible evidence before the court.

The legal frameworks that relate to the lawfulness of evidence regulate various stages of the lifecycle of evidence, namely the collection, storage, disclosure, interpretation, challenging by the defendant and evaluation by the judge. Throughout all these stages, evidence shall be handled in a manner respectful of the applicable national, international and supranational criminal rules. To assess the lawfulness of evidence, these different levels of legal frameworks present three main elements: admissibility, reliability of digital evidence and interpretability of evidence.[235] Challenging by the defendant and evaluation by judge may also be added to the list. The following paragraphs will have a brief look at these elements.

i. Divergent national laws and lack of an EU level harmonising regulation

As mentioned above, in order for evidence to be admissible within the scope of a criminal jurisdiction before national courts, it should be lawfully obtained, and this rule also applies to AI evidence. However, the legal setting which regulates the lawfulness of evidence in Europe is indeed complicated. The strong link between criminal law and the concept of state sovereignty leads to criminal law matters usually being addressed on the national level rather than on the Union level. As a result, typically, the rules concerning the lawfulness of evidence diverge from one another in each Member state. Compounding the situation, at the moment there is no harmonised EU framework specifically regulating the admissibility of evidence.[236]

The lack of a common framework and the divergence of national criminal procedure laws concerning the admissibility of evidence can raise issues when evidence is produced in one State and then is involved in a criminal procedure in another State. The AI-driven technologies used in handling and producing the evidence may have been developed in more than one jurisdiction, with different laws

[232] See, for instance, '4NSEEK' (INCIBE, 16 January 2019) <https://www.incibe.es/en/european-projects/4nseek> accessed 2 June 2022; Austin Davis, 'German Authorities Turn to AI to Combat Child Pornography Online | DW' (DW.COM, 8 May 2019) <https://www.dw.com/en/germany-new-ai-microsoft-combat-child-porn/a-49899882> accessed 2 June 2022.
[233] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 532–533.
[234] Geert Corstens and Jean Pradel, *European Criminal Law* (Kluwer law international 2002).
[235] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 535ff.
[236] Garamvölgyi and others (n 228).

concerning the lawfulness of the evidence. Moreover, because of the inherent characteristics of AI-driven technologies, such as their opacity, lack of explainability and their automated nature, it may be difficult to detect the origin of evidence or how the evidence was handled and produced by these technologies, greatly complicating the assessment of its lawfulness.

At the moment, the similar standards observed in many national criminal legal orders can be helpful in the face of the complicated situation in Europe. European human rights law and the relevant principles formulated in the case law of the ECtHR also provide some clarity.[237] These common standards and the case law of the ECtHR bring an illuminating perspective which is used to explore the common elements identified above. In addition, this paragraph also briefly addresses some other relevant international and European law instruments, such as the Budapest Convention, European Investigation Order,[238] the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union[239] and the LED.

ii. Admissibility of evidence

EXCLUSIONARY PRINCIPLE - Evidence that is gathered illegally or, in other words, by violating the relevant legal requirements (including a wide range of laws and regulations, such as fundamental rights, criminal procedure or data protection rules) or gathered via methods that violate a person's rights, is deemed to be unlawfully obtained. In addition to national criminal rules, the most notable legal rules the violation of which would lead to the inadmissibility of evidence are the violation of fundamental rights, such as the right to fair trial, right to privacy and data protection explained above, and right to life, prohibition of torture and inhuman or degrading treatments.[240]

The commonly accepted 'exclusionary' principle kicks in and leads to the exclusion of the unlawfully obtained evidence from criminal proceedings, barring it from being taken into deliberation by the court or constituting a basis for judgment in the proceedings. However, it is worth noting that this rule is not absolute, and while it is generally accepted, it does not have a universal reach.[241] Indeed, in exceptional cases, many jurisdictions allow unlawfully obtained evidence to be included in criminal proceedings and give the judges the discretion to decide whether such evidence can become admissible.[242] For

[237] 'Rights of Suspects and Accused' (*European Commission*) <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/rights-suspects-and-accused_en> accessed 13 July 2022.
[238] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1 (n 192) Article 9.
[239] The Convention established by the Council in accordance with art 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C197/1.
[240] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 535.
[241] Anne Weyembergh and Elodie Sellier, 'Criminal Procedural Laws across the European Union – A Comparative Analysis of Selected Main Differences and the Impact They Have over the Development of EU Legislation' (European Parliament Policy Department for Citizens' Rights and Constitutional Affairs 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604977/IPOL_STU(2018)604977_EN.pdf>.
[242] Quezada-Tavárez, Vogiatzoglou and Royer (n 79).

instance, in Canada, the UK and Germany, unlawfully obtained evidence is excluded only in very specific cases, such as when its inclusion would severely violate certain rights.[243]

Concerning the violations of fundamental rights that lead to the exclusion of evidence, and especially the right to a fair trial, the ECtHR deems itself non-competent to decide specifically on the admissibility of evidence but it nevertheless comments on the topic when problems with the admissibility of evidence lead to significant problems in a manner to violate the fairness of the proceedings. As explained above, in Section 3.1.1 concerning the right to a fair trial, a defendant should be able to challenge the authenticity and inclusion into the proceedings of unlawfully obtained evidence when this evidence is the sole or deciding element for the conviction, otherwise the ECtHR finds that the right to a fair trial to be violated.[244]

Violations of privacy and data protection laws can also taint the lawfulness of evidence. As explained above, the Convention 108+ and the LED require that the LEAs collect personal data for *"specified, explicit and legitimate purposes"*[245] and they should limit data collection and processing to the extent that is necessary for the performance of a task.[246] Not complying with these requirements could equally lead to exclusion of evidence.

When it comes to the lawfulness and admissibility of AI evidence, according to the case law of the ECtHR, as explained above in Section 3.1.5, for the extraction of evidence including personal data through the use of various surveillance methods there should be clear legal grounds regulating the use of the specific surveillance technologies and establishing clear safeguards. On the other hand, as explained above in Section 3.1.5, when evidence is extracted from devices that are not built for surveillance purposes, the ECtHR requires that appropriate safeguards should be established against abuses of right to privacy and data protection.[247] If the surveillance on such devices is conducted on the basis of a legal framework, the legal framework should include clear specifications when and under which conditions the surveillance takes place, so that individuals can have a clear idea concerning when they may be subjected to surveillance.[248] Moreover, these surveillance activities should be based on prior authorisation. [249]

In the context of ALIGNER, countless AI-driven tools could facilitate such evidence extraction practices. Such practices should be based on prior authorisation with a clear legal ground foreseen under the relevant laws. The individuals should be clearly informed of the details of potential surveillance they may be under, such as the conditions under which LEAs may access their data. However, at the

[243] Garamvölgyi and others (n 228) 204.
[244] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 536.
[245] Convention 108+ Article 5(4)(b) and LED Article 4(1)(b).
[246] LED Article 8(1).
[247] For relevant examples, see Klass and others v Germany App no 5029/71 (ECtHR, 6 September 1978); Bykov v Russia App no 4378/02 (ECtHR, 10 March 2009); Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015); Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016); Big Brother Watch and Others v the United Kingdom App no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021); P.N. v Germany App no 74440/17 (ECtHR, 11 June 2020) (as cited above in [n 117] and in Quezada-Tavárez, Vogiatzoglou and Royer [n 79] 537, fn 35.).
[248] Ibid.
[249] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 537.

moment, there is no clear AI-specific regulation in the EU focusing on surveillance and extraction of evidence by the use of AI tools. This makes the lawfulness of evidence obtained via the use of AI-driven tools extremely challenging. In any case, the principles laid down by the case law mentioned above should be kept in mind while assessing the lawfulness of the use of such AI-driven tools as well as the evidence obtained through their use.

There are ongoing efforts in Europe to establish clear legal rules concerning the admissibility of evidence, especially with the upcoming e-Evidence Package (including a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters,[250] and a Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings)[251] and the Second Additional Protocol to the Cybercrime Convention.[252] When finalized, these ongoing efforts will have the potential to clarify the questions surrounding the admissibility of evidence. Nevertheless, due to the inherent characteristics of AI-driven tools, and potential risks they pose towards fundamental rights, clearer and AI evidence-specific legislation will be required with regard to the use of AI tools to obtain evidence, in order to satisfy the requirements set forth so far under the case law of the ECtHR and the CJEU.

RELIABILITY OF DIGITAL EVIDENCE – In order to consider the evidence as reliable, there should be no doubt concerning its authenticity (meaning that the LEAs need to establish the source of the evidence) and integrity (the evidence should remain intact and should not be tampered with throughout the proceedings by the LEAs).[253] In its case law, the ECtHR usually has a high threshold and considers the evidence to be unreliable only when the flaws in its handling and processing are manifest. Therefore, as stated by Quezeda-Tavarez et al, *"National courts* […] *have a considerable margin of appreciation when assessing the reliability of evidence, which boils down to a case-by-case approach"*.[254]

The reliability of evidence is closely related to the quality of data used by LEAs as evidence, and the LED and Convention 108+ also have principles to ensure the quality of data, such as accuracy of processing and keeping the data up to date.[255] As a result, as data controllers, LEAs have the responsibility to ensure the quality and reliability of the personal data they process to be used as evidence within the proceedings [see also Section 3.2.1.1 concerning the LED].

The reliability of evidence that is obtained through the use of AI-driven tools can be challenging from a few points. First of all, huge datasets are used in the development and deployment of the AI-driven tools and the data included in those datasets may be originating from numerous different sources.

---

[250] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for Electronic Evidence in Criminal Matters COM/2018/225 Final - 2018/0108 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN> accessed 12 December 2021.
[251] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal COM/2018/226 Final - 2018/0107 (COD) < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:226:FIN> accessed 13 July 2022.
[252] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) < https://rm.coe.int/1680a49dab> accessed 13 July 2022.
[253] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 539.
[254] ibid.
[255] LED Article 4(1)(d) and Convention 108+ Article 5(4).

Moreover, data included in those datasets may not always be based on objective facts, it may be speculative, include mistakes or have inherent historical biases. When these far-from-perfect data are used by the AI-driven tools to obtain and handle evidence, assessing the authenticity and the integrity of the outcomes becomes a challenge. The inherent opaque characteristics of AI-driven tools also bring significant challenges to the assessment of the reliability of the data. Another problem in this regard is the interaction of human experts with the AI systems, considering the fact that personal experiences and choices of human experts who operate the AI systems can affect the outcomes.[256]

In light of the risks presented by AI-driven tools concerning the lawfulness of evidence, chain of custody is also a vital element. The term chain of custody is defined as "*the chronological documentation of evidence as it is processed during the investigation (i.e., seizure, custody, transfer, and analysis)*".[257] If the chain of custody is breached, evidence becomes unreliable starting from the moment of breach. There are no specific legislations concerning AI evidence, as mentioned above, however, the specific guidelines developed for LEAs with the aim of protecting the chain of custody could provide some level of clarity.[258] Moreover, recording all the details concerning the source of the evidence and how the evidence is handled can ensure the reliability of the evidence. This includes recoding all human and digital factors that came into contact with the evidence, with their respective times and dates, including "a detailed account of issues such as location, time and date of evidence recovery, as well as a description of each evidence item".[259]

INTERPRETABILITY OF EVIDENCE – As explained above in Section 3.1.1, the defendants should be able to assess the incriminating evidence and challenge its use and authenticity. Similarly, judges should have sufficient information and understanding as to how the decisions that influence the proceedings were made by the AI-driven tools.

However, when it comes to the use of AI-driven tools for AI evidence, the opacity of the AI systems and lack of explainability will lead to problems for not only the defendants to challenge the evidence but also for the judges and other experts who may be involved in the criminal proceedings. To counteract potential problems in this regard, it is important for ALIGNER to focus its efforts on identifying explainable, transparent AI tools which will allow the defendants, experts and judges involved in the case to understand the factors that play a role in the outcomes of the AI mechanism which is used to obtain and handle the evidence. They must be able to question different steps that the AI system

[256] Nina Sunde and Itiel E Dror, 'A Hierarchy of Expert Performance (HEP) Applied to Digital Forensics: Reliability and Biasability in Digital Forensics Decision Making' (2021) 37 Forensic Science International: Digital Investigation 301175.
[257] Thomas J Holt, Adam M Bossler and Kathryn C Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (Second edition, Routledge, Taylor & Francis Group 2018) 498.
[258] See, for example, Nigel Jones and others, 'Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges (Version 2.0)' (Council of Europe Directorate General of Human Rights and Rule of Law, Cyber Crime Division 2014) <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf> accessed 13 July 2022; see also 'Electronic Evidence - a Basic Guide for First Responders' (European Union Agency for Cybersecurity (ENISA) 2015) Report/Study <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders> accessed 13 July 2022.
[259] Quezada-Tavárez, Vogiatzoglou and Royer (n 79) 541. ISO also provides standards with regard to digital forensics and chain of custody, which may support ensuring the reliability of AI evidence. See for instance, ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

passes through to reach the specific outcome and the effects of those steps on the evidence and the fact-finding process of the criminal proceedings.[260]

[260] Ibid, 547.

Conclusion

As the first output of ALIGNER Work Package 4, this deliverable identified the relevant legal and ethical frameworks, as well as best practices and guidelines for the use of AI tools in the police and law enforcement sector. With a strong focus on the instruments adopted by the Council of Europe and the European Union, this deliverable presented the existing knowledge in a systematised manner, with the aim of building among LEAs a common understanding of the relevant ethical and legal challenges relating to issues further examined by other ALIGNER Work Packages.

As expressly identified under this deliverable, the AI-driven technologies and tools used in the police and law enforcement sector create substantial ethical problems, as well as significant risks towards a number of fundamental rights, such as the right to a fair trial, non-discrimination as well as the right to privacy and data protection. Respect towards these fundamental rights, as well as careful compliance with the requirements set forth under relevant laws identified above is of utmost importance to ensure safe and acceptable development and deployment of AI tools by the police and the law enforcement sector. Our research concerning the relevant legal frameworks also clarified the need for a specific legal instrument addressing this area. While the proposed AI Act provides some clarity, a legal instrument that is tailored for the needs of the police and law enforcement sector could prove to be more efficient to address the ethical and legal risks of AI-driven tools that are already in use, as well as the ones that are to be adopted in the near future, by the LEAs.

In light of the identified legal and ethical concerns, this deliverable also provides suggestions to ensure compliance with the ethical and legal requirements listed above. Rather general at the moment, these suggestions will be further developed and specified under roadmap deliverables, in light of the scenarios to be developed under ALIGNER as well as future workshops. In addition to raising awareness within the LEA community and helping them understand the current and emerging debates on the risks arising from their use of AI, the findings of this deliverable will support the following tasks of Work Package 4.

4 Bibliography

4.1 Legislation

Charter of Fundamental Rights of the European Union [2000] OJ C 364/1

Consolidated Version of the Treaty on European Union [2008] OJ C115/13

Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C 115/47

Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data

Convention established by the Council in accordance with art 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C197/1

Convention for the Protection of Human Rights and Fundamental Freedoms

Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe (CETS No. 108), Adopted on 28.01.1981, as Amended by Protocol CETS No. 223, 2018

Convention on Cybercrime of the Council of Europe, CETS No 185

Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax [2006] OJ L 347/1

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386/89

Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters [2001] OJ L 174/1

Council Regulation (EU) No 904/2010 of 7 October 2010 on administrative cooperation and combating fraud in the field of value added tax [2010] OJ L 268/1

Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the Right to Interpretation and Translation in Criminal Proceedings [2010] OJ L 280/1

Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the Right to Information in Criminal Proceedings [2012] OJ L 142/1

Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the Right of Access to a Lawyer in Criminal Proceedings and in European Arrest Warrant Proceedings, and on the Right to Have a Third Party Informed upon Deprivation Of liberty and to communicate with third persons and with consular authorities while deprived of liberty [2013] OJ L 294/1

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 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 [2016] OJ L 65/1

Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on Procedural Safeguards for Children Who Are Suspects or Accused Persons in Criminal Proceedings [2016] OJ L 132/1.

Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on Legal Aid for Suspects and Accused Persons in Criminal Proceedings and for Requested Persons in European Arrest Warrant Proceedings [2016] OJ L 297/1

International Convention on the elimination of all forms of Racial Discrimination

Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) [2016] OJ L 119/89 (“LED”)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal COM/2018/226 Final - 2018/0107 (COD)

Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 Final - 2017/03 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010> accessed 13 July 2022

Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for Negotiations with EP, 10 February 2021, No 6087/2.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for Electronic Evidence in Criminal Matters COM/2018/225 Final -

2018/0108 (COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN> accessed 12 December 2021

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 ('AI Act Proposal')

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ("GDPR")

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and Replacing and Repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135/53

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303/59 ("NPDR")

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)

4.2 Jurisprudence

Airey v Ireland App no 6289/73 (ECtHR, 9 October 1979)

Al-Khawaja and Tahery v the United Kingdom [GC] App no 26766/05 and 22228/06 (ECtHR, 15 December 2011)

Bank Mellat v Her Majesty's Treasury (No 2) [2014] AC 700

Big Brother Watch and Others v the United Kingdom App no 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021)

Bridges v Chief Constable of South Wales Police and Other [2020] EWCA CIV 1058 ("Court of Appeal decision")

Bykov v Russia App no 4378/02 (ECtHR, 10 March 2009)

Case C-199/11 EU v Otis and others [2012] ECLI:EU:C:2012:684

Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779

Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others [2020] ECLI:EU:C2020:790

Costello-Roberts v the United Kingdom App no 13134/87 (ECtHR, 25 March 1993)

Dombo Beheer BV v Netherlands App no 14448/88 (ECtHR, 27 October 1993)

Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others v Premier ministre and Others [2020] ECLI:EU:C:2020:791

R (Bridges) v Chief Constable of South Wales Police and Secretary of State for the Home Office [2019] EWHC 2341 (Admin) ("Divisional Court decision")

Klass and others v Germany App no 5029/71 (ECtHR, 6 September 1978)

Lucà v Italy App no 33354/96 (ECtHR, 27 February 2001)

Magyar Helsinki Bizottság v Hungary App no 18030/11 (ECtHR, 8 November 2016)

Mika v Sweden App no 31243/06 (ECtHR, 27 January 2009)

Moreira de Azevedo v Portugal App no 11296/84 (ECtHR, 23October 1990)

Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992)

P.G. and J.H. v the United Kingdom App no 44787/98 (ECtHR, 25 December 2001 Final)

P.N. v Germany App no 74440/17 (ECtHR, 11 June 2020)

Stanev v Bulgaria App no 36760/06 (ECtHR, 6 November 2012)

Stoll v Switzerland App no 69698/01 (ECtHR, 10 December 2007)

Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016)

Vetter v France App no 59842/00 (ECtHR, 31 May 2005)

Wisse v France App no 71611/01 (ECtHR, 22 December 2005)

X and Y v the Netherlands App no 8978/80 (ECtHR, 26 March 1985)

Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015)

4.3 References

'4NSEEK' (*INCIBE*, 16 January 2019) <https://www.incibe.es/en/european-projects/4nseek> accessed 2 June 2022

Ad Hoc Committee on Artificial Intelligence (CAHAI), 'Feasibility Study' <https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da> accessed 8 July 2022

——, ‘Possible Elements of a Legal Framework on Artificial Intelligence, Based on the Council of Europe’s Standards on Human Rights, Democracy and the Rule of Law’ <https://rm.coe.int/cahai-2021-09rev-elements/1680a6d90d> accessed 8 July 2022

Agencia Española de Protección de Datos and European Data Protection Supervisor, ‘10 Misunderstanding Related to Anonymisation’ <https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf> accessed 13 July 2022

‘AI Initiatives’ <https://www.coe.int/en/web/artificial-intelligence/national-initiatives> accessed 8 July 2022

‘ALIGNER’ <https://aligner-h2020.eu/> accessed 8 July 2022

Angwin J, Larson J, Mattu S and Kirchner L, ‘Machine Bias’ *ProPublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing?token=TiqCeZIj4uLbXl91e3wM2PnmnWbCVOvS> accessed 8 June 2022

Article 29 Data Protection Working Party, ‘Opinion 4/2007 on the Concept of Personal Data’ (2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 13 July 2022

——, ‘Opinion 03/2013 on Purpose Limitation, WP 203’ (2013) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 13 July 2022

——, ‘Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector, WP 211’ <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf> accessed 13 July 2022

——, ‘Opinion 03/2015 on the Draft Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, WP 233’ (2015) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf> accessed 13 July 2022

——, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679, WP248 Rev.01’ (2017) <https://ec.europa.eu/newsroom/article29/items/611236> accessed 13 July 2022

——, ‘Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680), WP258’ (2017) <https://ec.europa.eu/newsroom/article29/items/610178/en> accessed 13 July 2022

——, ‘Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01’ (2018) <https://ec.europa.eu/newsroom/article29/items/612053/en> accessed 13 July 2022

Brakel R van and De Hert P, 'Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies.' (2011) 20 Journal of Police Studies 163

Buolamwini J and Gebru T, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' 15

Bychawska-Siniarska D, *Protecting the Right to Freedom of Expression under the European Convention on Human Rights, A Handbook for Legal Practitioners* (2017)

Caruana MM, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) 33 International Review of Law, Computers & Technology 249

Casolari F and Rossi LS (eds), *The Principle of Equality in EU Law* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Chessman C, 'A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution' (2017) 105 California Law Review 179

CILEVIČS B, 'Justice by Algorithm – the Role of Artificial Intelligence in Policing and Criminal Justice Systems (Report - Doc. 15156)' <https://pace.coe.int/en/files/28723/html> accessed 8 July 2022

Committee of Ministers of the Council of Europe, 'Explanatory Memorandum to Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector' <https://rm.coe.int/168062dfd4> accessed 13 July 2022

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 'Practical Guide on the Use of Personal Data in the Police Sector' <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5> accessed 13 July 2022

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 'Guidelines on Artificial Intelligence and Data Protection' <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> accessed 13 July 2022

——, 'Guidelines on Facial Recognition' <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> accessed 13 July 2022

Cormen TH, Leiserson CE, Rivest RL and Stein C (eds), *Introduction to Algorithms* (3rd ed, MIT Press 2009)

Corstens G and Pradel J, *European Criminal Law* (Kluwer law international 2002)

Coudert F, 'The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to ... What Exactly?' (2017) 3 European Data Protection Law Review 313

Council of Europe, 'Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems' <https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154> accessed 8 July 2022

——, 'Terms of Reference of the Committee on Artificial Intelligence (CAI)' <https://rm.coe.int/terms-of-reference-of-the-committee-on-artificial-intelligence-for-202/1680a4ee36> accessed 8 July 2022

Council of Europe Commisioner for Human Rights, 'Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights' (Council of Europe 2019) <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64> accessed 31 May 2022

'Council of Europe's Work in Progress' <https://www.coe.int/en/web/artificial-intelligence/work-in-progress> accessed 8 July 2022

Davis A, 'German Authorities Turn to AI to Combat Child Pornography Online | DW' (*DW.COM*, 8 May 2019) <https://www.dw.com/en/germany-new-ai-microsoft-combat-child-porn/a-49899882> accessed 2 June 2022

Demiaux V, 'How Can Humans Keep the Upper Hand? Report on the Ethical Matters Raised by Algorithms and Artificial Intelligence' (2017) <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf> accessed 12 July 2022

Devillé R, Sergeyssels N and Middag C, 'Basic Concepts of AI for Legal Scholars' in Jan de Bruyne and Cedric Vanleenhove (eds), *Artificial intelligence and the law* (Intersentia 2021)

Ebers M, 'Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework(s)' [2021] Nordic Yearbook of Law and Informatics 2020: Law in the Era of Artificial Intelligence <https://papers.ssrn.com/abstract=3901732> accessed 8 June 2022

'Electronic Evidence - a Basic Guide for First Responders' (European Union Agency for Cybersecurity (ENISA) 2015) Report/Study <https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders> accessed 13 July 2022

Eskens S, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An in-Depth Review of La Quadrature Du Net and Others and Privacy International' (2022) 8 European Data Protection Law Review 143

European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe (COM/2018/237 Final)' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN> accessed 8 July 2022

——, ‘White Paper on Artificial Intelligence - A European Approach to Excellence and Trust (COM(2020) 65 Final)’ <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 12 July 2022

——, ‘A European Approach to Artificial Intelligence | Shaping Europe’s Digital Future’ <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 8 July 2022

——, ‘Regulatory Framework Proposal on Artificial Intelligence’ (*Shaping Europe’s Digital Future*) <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 2 June 2022

European Commission for the Efficiency of Justice (CEPEJ), ‘European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment’ <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> accessed 8 July 2022

European Court of Human Rights, ‘Guide on Article 8 of the European Convention on Human Rights - Right to Respect for Private and Family Life, Home and Correspondence’ (Council of Europe 2021) <https://www.echr.coe.int/documents/guide_art_8_eng.pdf> accessed 13 July 2022

——, ‘Guide on Article 6 of the European Convention on Human Rights, Right to a Fair Trial (Criminal Limb)’ (2022) <https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf> accessed 12 July 2022

European Data Protection Board, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0’ (2021) <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf> accessed 23 May 2022

European Data Protection Board and European Data Protection Supervisor, ‘EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)’ (2021) <https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf> accessed 13 July 2022

European Data Protection Supervisor, ‘Opinion on the Data Protection Reform Package’ (2012) <https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 13 July 2022

European Digital Rights (EDRi), ‘Use Cases: Impermissible AI and Fundamental Rights Breaches’ (European Digital Rights (EDRi) 2020) <https://edri.org/wp-content/uploads/2021/06/Case-studies-Impermissible-AI-biometrics-September-2020.pdf> accessed 8 June 2022

European Parliamentary Research Service and Negreiro M, ‘Briefing - EU Legislation in Progress - Free Flow of Non-Personal Data in the European Union’ <https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614628/EPRS_BRI(2017)614628_EN.pdf> accessed 29 October 2021

European Union Agency for Fundamental Rights, *Towards More Effective Policing : Understanding and Preventing Discriminatory Ethnic Profiling : A Guide* (Publications Office of the European Union 2010) <https://data.europa.eu/doi/10.2811/40252> accessed 13 July 2022

——, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> accessed 31 May 2022

——, *Handbook on European Data Protection Law : 2018 Edition* (Publications Office 2018) <https://data.europa.eu/doi/10.2811/343461> accessed 2 June 2022

European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe, *Handbook on European Non-Discrimination Law* (Publications Office of the European Union 2018) <https://data.europa.eu/doi/10.2811/58933> accessed 13 July 2022

Fair Trials, 'Briefing Paper on the Communication on Digitalisation of Justice in the European Union' (2021) <https://policehumanrightsresources.org/content/uploads/2021/10/BRIEFING-PAPER-ON-THE-COMMUNICATION-ON-DIGITALISATION-OF-JUSTICE-IN-THE-EUROPEAN-UNION.pdf?x19059> accessed 13 July 2022

Fantin S, Emanuilov I, Vogiatzoglou P and Marquenie T, 'Purpose Limitation By Design As A Counter To Function Creep And System Insecurity In Police Artificial Intelligence', *UNICRI Special Collection on AI in Criminal Justice* (2020) <http://www.unicri.it/sites/default/files/2020-08/Artificial%20Intelligence%20Collection.pdf,> accessed 13 July 2022

Galetta A, 'The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the Use of Surveillance Technologies?' (2013) 4 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/221> accessed 12 July 2022

Garamvölgyi B, Ligeti K, Ondrejova A and von Galen M, 'Admissibility of Evidence in Criminal Proceedings in the EU' [2020] eucrim - The European Criminal Law Associations' Forum 201

Georgieva I, Timan T and Hoekstra M, 'Regulatory Divergences in the Draft AI Act - Differences in Public and Private Sector Obligations' (European Parliamentary Research Service 2022)

Gerards J and Xenidis R, *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law : A Special Report* (2021)

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014) <http://link.springer.com/10.1007/978-3-319-05023-2> accessed 13 July 2022

——, 'Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights' (2020)

High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 12 July 2022

——, 'Policy and Investment Recommendations for Trustworthy Artificial Intelligence' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence> accessed 12 July 2022

——, 'Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI' <https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-sectoral-considerations-policy-and-investment-recommendations-trustworthy-ai> accessed 12 July 2022

——, 'Futurium | European AI Alliance - ALTAI - The Assessment List on Trustworthy Artificial Intelligence' <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence> accessed 12 July 2022

Hildebrandt M, 'Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics' (2018) 68 University of Toronto Law Journal 12

Holt TJ, Bossler AM and Seigfried-Spellar KC, *Cybercrime and Digital Forensics: An Introduction* (Second edition, Routledge, Taylor & Francis Group 2018)

'INCIBE' (*INCIBE*) <https://www.incibe.es/> accessed 8 July 2022

Jones N, George E, Merida FI, Rasmussen U and Völzow V, 'Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges (Version 2.0)' (Council of Europe Directorate General of Human Rights and Rule of Law, Cyber Crime Division 2014) <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf> accessed 13 July 2022

Kaltheuner F and Narayanan A, 'AI Snake Oil, Pseudoscience and Hype - an Interview with Arvind Narayanan', *Fake AI* (Meatspace Press 2021) <https://ia804607.us.archive.org/3/items/fake-ai/Fake_AI.pdf>

Kocsis RN, *Criminal Profiling* (Humana Press 2006) <https://link.springer.com/book/10.1007/978-1-59745-109-3> accessed 13 July 2022

La Fors-Owczynik K, 'Profiling "Anomalies" and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), *Under Observation: The Interplay Between eHealth and Surveillance* (Springer International Publishing 2017) <https://doi.org/10.1007/978-3-319-48342-9_7> accessed 8 June 2022

Leanza P and Pridal O, *The Right to a Fair Trial: Article 6 of the European Convention on Human Rights* (Wolters Kluwer Law & Business : Kluwer Law International 2014)

Leroux O, ‘Legal Admissibility of Electronic Evidence’ (2004) 18 International Review of Law, Computers & Technology 193

Lynskey O, ‘Deconstructing Data Protection: The “Added Value” Of A Right To Data Protection In The EU Legal Order’ (2014) 63 International & Comparative Law Quarterly 569

——, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

Madiega T and European Parliamentary Research Service, ‘Briefing - EU Legislation in Progress - Artificial Intelligence Act’ <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>

Marks P, ‘Can the Biases in Facial Recognition Be Fixed; Also, Should They?’ (2021) 64 Communications of the ACM 20

Marquenie T, ‘Legal and Ethical Challenges in Algorithmic Policing and Law Enforcement AI’ in Marie-Amélie Bourguignon and others (eds), *Technology and society: the evolution of the legal landscape* (Gompel & Svacina 2021)

——, ‘MAGNETO D9.1 Ethical and Legal Guidelines for the Use and Development of MAGNETO Tools’ (2019)

Ministerie van Justitie en Veiligheid, ‘Home - Forensischinstituut.nl’ (27 January 2021) <https://www.forensischinstituut.nl/> accessed 8 July 2022

Mole N and Harby C, *The Right to a Fair Trial, A Guide to the Implementation of Article 6 of the European Convention on Human Rights*, vol 3 (Directorate General of Human Rights, Council of Europe 2006)

Murdoch J and Roche R, *The European Convention on Human Rights and Policing, A Handbook for Police Officers and Other Law Enforcement Officials* (Council of Europe Publishing 2013)

Narayanan A, ‘How to Recognize AI Snake Oil’ (2019) <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>

Naudts L, ‘Criminal Profiling and Non-Discrimination: On Firm Grounds for the Digital Era?’ in Anton Vedder and others (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia 2019) <https://papers.ssrn.com/abstract=3508020> accessed 13 July 2022

Oswald M, Grace J, Urwin S and Barnes GC, ‘Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and “Experimental” Proportionality’ (2018) 27 Information & Communications Technology Law 223

Palmiotto F, ‘The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings’ in Martin Ebers and Marta Cantero Gamito (eds), *Algorithmic Governance and*

Governance of Algorithms: Legal and Ethical Challenges (Springer International Publishing 2021) <https://doi.org/10.1007/978-3-030-50559-2_3> accessed 16 May 2022

Parliamentary Assembly of the Council of Europe, 'Justice by Algorithm – The Role of Artificial Intelligence in Policing and Criminal Justice Systems (Recommendation 2182 (2020))' <https://pace.coe.int/en/files/28806/html> accessed 8 July 2022

——, 'Justice by Algorithm – The Role of Artificial Intelligence in Policing and Criminal Justice Systems (Resolution 2342 (2020))' <https://pace.coe.int/en/files/28805/html> accessed 8 July 2022

Quezada-Tavárez K, Vogiatzoglou P and Royer S, 'Legal Challenges in Bringing AI Evidence to the Criminal Courtroom' (2021) 12 New Journal of European Criminal Law 531

Quintel T, 'European Union · The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation' (2022) 8 European Data Protection Law Review 90

'Rights of Suspects and Accused' (*European Commission*) <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/rights-suspects-and-accused_en> accessed 13 July 2022

Rocher L, Hendrickx JM and de Montjoye Y-A, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069

Sunde N and Dror IE, 'A Hierarchy of Expert Performance (HEP) Applied to Digital Forensics: Reliability and Biasability in Digital Forensics Decision Making' (2021) 37 Forensic Science International: Digital Investigation 301175

Tadros V, 'Rethinking the Presumption of Innocence' (2006) 1 Criminal Law and Philosophy 193

Trechsel S, *Human Rights in Criminal Proceedings* (Oxford University Press 2006)

Valport M and Surkovic E, 'Annual Report of the Government Chief Scientific Adviser 2015. Forensic Science and Beyond: Authenticity, Provenance and Assurance' 16

Weyembergh A and Sellier E, 'Criminal Procedural Laws across the European Union – A Comparative Analysis of Selected Main Differences and the Impact They Have over the Development of EU Legislation' (European Parliament Policy Department for Citizens' Rights and Constitutional Affairs 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604977/IPOL_STU(2018)604977_EN.pdf>

'Why Do We Need the Charter?' (*European Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/why-do-we-need-charter_en> accessed 8 July 2022

Woods L, 'Automated Facial Recognition in the UK: The Bridges Case and Beyond' (2020) 6 European Data Protection Law Review 455

Xu F, Tu Z, Li Y, Zhang P, Fu X and Jin D, 'Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data', *Proceedings of the 26th International Conference on World Wide Web* (2017) <http://arxiv.org/abs/1702.06270> accessed 13 July 2022