A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights

D2.2: Legal framework and casework taxonomy: emerging trends and scenarios

Grant Agreement ID	101022001	**Acronym**	pop AI
Project Title	A European Positive Sum Approach towards AI tools in support of Law Enforcement and safeguarding privacy and fundamental rights		
Start Date	01/10/2021	**Duration**	24 Months
Project URL	https://www.pop-ai.eu/		
Contractual due date	30/09/2022	**Actual submission date**	30/09/2022
Nature	R = Document, report	**Dissemination Level**	PU = Public
Author	Francesca Trevisan (ETICAS)		
Contributors	Gemma Galdon Clavell (ETICAS), Gerardo Steta Perea (CREMADES), Ezgi Eren (KU Leuven)		
Reviewers	Dimitra Papadaki (KEMEA), Galateia Kapellakou (KEMEA) Dimitris Kyriazanos (NCSRD), Andeas Ikonomopoulos (NCSRD)		

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

Executive Summary

The development of Artificial Intelligence (AI) has made a big leap in the recent years. Its deployment has become ubiquitous in many public sectors such as education, health and security bringing great promises as well as new risks. Law Enforcement Agencies (LEAs) and Judicial Authorities around the world are among the actors that are increasingly using AI. AI applications (see D2.1) are playing an increasingly significant role in crime prevention and investigation, in migration asylum and border control management, in the administration of justice, cyber operations and LEAs' training (see D3.1). AI applications are used in the security domain for a variety of purposes, with the promise of increasing safety, efficiency, and human capabilities. Nonetheless, AI engenders new challenges that fuel social disharmonies questioning how these technologies are being employed and whether they respect human rights. Public trust has been undermined by a lack of transparency and accountability and by the power asymmetry that characterize those who employ AI technologies and those who are subjected to it. Democratic oversight of AI is dawning, under mounting evidence of how AI in the security domain can be misused, infringe rights, while reinforcing discrimination and historical biases.

To foster public trust in AI, it is important to identify how and to what extent regulatory attempts are addressing public concerns. To achieve this goal, this report documents the current legal frameworks that apply to AI and organizes them in an overarching taxonomy which aims to facilitate analysis of regulations and forecast future trends. After an introduction outlining the topic discussed (section 1) this report presents the legal taxonomy (section 2) which classifies EU legal frameworks in three higher classes (human rights, data and AI) according to the controversy they seek to solve. To this end, each higher class specifies a number of key principles representing important areas that regulatory approaches seek to fulfill to set social disharmonies and develop trust. In particular, the AI class presents an in-depth discussion of US AI regulatory frameworks, with the aim of comparing EU and US approaches.

Next, this report presents a review of EU court rulings and Data Protection Authority (DPA) decisions to provide a picture of how legal aspects are being handled in practice in the security and other relevant domains (section 3). This section discusses case law of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU) and data protection authorities' decisions. Finally, this report provides a conclusion with a summary of the content (Section 4).

Table of Contents

List of Figures

List of Tables

List of Terms & Abbreviations

Abbreviation	Definition
ADM	Automated Decision Making
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AI HLEG	High Level Expert Group on Artificial Intelligence
AIDA	Special Committee on Artificial Intelligence in a Digital Age
APD	Autoritè de Protection des données
ALTAI	Assessment List for Trustworthy AI
CAHAI	Ad Hoc Committee on Artificial Intelligence
CFR	Charter of Fundamental Rights of the EU
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale Informatique & Libertés
CPDP	Commission for Personal Data Protection
CSAM	Child Sexual Abuse Material
DPA	Data Protection Authority
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human RIghts
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ESC	European Social Charter
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
LEAs	Law Enforcement Agencies
LED	Law Enforcement Directive
MEP	Member of the European Parliament
NAIAC	National AI Advisory Committee
NAIAC-LE	National AI Advisory Committee - Law Enforcement
NAIIO	National AI Initiative Office
NIST	National Institute of Standards and Technology
PCAST	President's Council of Advisors on Science and Technology
PNR	Passenger Name Record
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

1 Introduction

Pop AI is a 24 month Coordination and Support Action (CSA) project funded by Horizon 2020 and undertaken by a consortium of 13 partners from 8 European countries. Pop AI aims at bringing together security practitioners, AI scientists, ethics and privacy researchers, civil society organisations as well as social sciences and humanities experts with the purpose of consolidating knowledge, exchanging experience and raising awareness in the EU area. The core vision of Pop AI is to foster trust in AI for the security domain via increased awareness, ongoing social engagement, consolidating distinct spheres of knowledge (including theoretical & empirical knowledge by academics & non-academics) and offering a unified European view across LEAs, and specialised knowledge outputs (recommendations, roadmaps), while creating an ecosystem that will form the structural basis for a sustainable and inclusive European AI hub for Law Enforcement.

AI systems need to be considered "socio-technical" systems, meaning that their development, employment and impact depends on technical factors - such as the design, data used, accuracy, intended purpose- as well as social factors -such as the social, organizational and legal context in which the system is developed or employed. To create a sustainable and inclusive European AI hub for LEAs, it is important to take into account the evolving legal panorama that impacts AI, its development and use in the security domain. To this end, this report presents a legal taxonomy summarizing and comparing the key legal frameworks regulating AI in the security domain.

1.1 Scope and objectives of the deliverable

Work Package 2 “Security AI in the next 20 years: trends, practices and risks” builds on the existing state of the art in relation to the use of AI by LEAs in Europe and elsewhere to identify:

1) the actual AI use and technical characteristics of AI tools in the security domain (T2.1);

2) the legal frameworks and recent court rulings (T2.2);

3) how controversies have shaped technology adoption in the security domain (T2.3);

4) the ethical principles and challenges that can inform a practical ethics toolbox (T2.4);

5) the organisational issues around AI implementation in LEA contexts (T2.5).

Task 2.1 “Functionality taxonomy, dataset mapping and emerging practices and trends” (D2.1) created a taxonomy of AI functionalities in the security domain. It identified over 30 AI functionalities and categorised them according to the data used, the area of application, the algorithm, and the high-level category of the functionality. Deliverable 2.2 “Legal casework taxonomy: emerging trends and scenarios” (D2.2) builds on D2.1 to create a taxonomy of the legal frameworks regulating AI in the security domain. This taxonomy provides insights into the EU legally binding and non-binding instruments that govern the different aspects of AI in the security domain. Furthermore, this deliverable compares the EU against the US AI specific legal tools available. This exercise is meant to drive to the identification of future developments of EU laws regulating AI in the security domain. At the EU level, this deliverable provides a review of court rulings and DPA decisions to portray how the legal tools available this far are applied in practice.

1.2 Structure of the deliverable

This deliverable is organised into four main sections.

Section 1 introduces the main topic discussed in the deliverable, outlines its scope and explains how this work related to other Pop AI tasks and deliverables.

Section 2 presents the legal taxonomy which classifies EU legal frameworks into three high level classes: human rights, data and AI. For each class, the taxonomy indicates several principles which correspond to areas that regulatory approaches seek to address to set controversies and social disharmonies related to the use of AI in the security domain. Each block is discussed in-depth and emphasizes how regulations try to address that area in order to increase public trust. When discussing the AI class, this report presents an in-depth comparison between US and EU emerging regulatory frameworks.

Section 3 reviews of EU court rulings and DPAs' decisions to provide a picture of how legal aspects are being handled in practice in the security and other relevant domains. This section discusses case law of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU) and data protection authorities’ decisions.

Finally, section 4 provides a conclusion with a summary of the main findings.

1.3 Relation to other tasks and deliverables

This report is the outcome of Task 2.2 *Legal Framework and Casework taxonomy: emerging trends and scenarios.* Overall, this report feed into the rest of the project by providing a legal context and guidance for the activities aimed at scoping public trust towards AI use for security. It builds on D2.1 *Functionality taxonomy and emerging practices and trends* by highlighting the legal frameworks that apply to AI in the security domain. Furthermore, this report sets the legal basis for the rest of the tasks in WP2 *Security AI in the next 20 years: trends, practices and risks*. In particular, the legal frameworks and caseworks identified in this report support the following tasks:

- Task 2.3: The controversies and risks that have shaped innovation and will shape AI in the next 20 years
- Task 2.4: From ethical frameworks to ethics into practice
- Task 2.5: AI meets organisational cultures: Human machine interaction at the police station

Additionally, the legal taxonomy will serve the work undertaken in WP3 by Task 3.4: *Engaging LEAs and relevant experts through policy labs* where each policy lab will cover policy needs in relation to human rights, liability, proportionality and gender diversity. Finally, the legal taxonomy will feed into *WP4 The pandect of recommendations for the ethical use of AI for LEAs.* WP4 will provide recommendations to civil societies and technology developers using the taxonomy developed and presented in this report.

2 Regulating AI in the security domain

Artificial Intelligence (AI) is often regarded as the most important and controversial technology of the 21st century (Natale & Ballatore, 2020). Growth in computational power and the increasing abundance of data made up the fourth industrial revolution, a technological revolution that is moving at an exponential pace and changing the way we live, work and build relationship with others at an unprecedented speed (WE forum, 2016). This digital revolution, of which AI is a key technology, has triggered global competition for AI leadership that fueled investments in the tech sector. Against this background, AI is expected to contribute more than $15.7 trillion by 2030 to the global economy. In 2020 the EU commission planned to invest in AI 1 billion per year while mobilising extra investments from the private sector and member states to reach an annual investment volume of €20 billion over the course of the digital decade (2020-2030) (European Commission, 2020). As a comparison, the US and China are investing respectively €5.1 and 6.8 billion annually (Korner, 2020) which has raised MEP's concerns about falling behind in the global race for tech leadership (European Parliament, 2022). When looking at the security sector, in 2021 the European Commission (2021) invested €274 million in research projects. In this heated race for AI leadership, regulatory effort is struggling to keep up with the speed of progress. The pace that characterises traditional legal approaches is very slow when compared to the rapid development of technologies, which can make new rules obsolete before they are enacted. This suggests that AI governance needs a combination of flexible binding and non-binding instruments able to reassure public confidence but also the principle of legal certainty and the rule of law. In this context, the direction of soft and hard instruments created up to date (see OECD policy observatory[1] for some examples) have a strong commonality. While they avoid restrictive regulations for fears that they would hamper innovation, they also avoid a governance vacuum which would create uncertainty, discourage investment, and leave citizens unprotected.

Among all the sectors, the use of AI in the security domain is very sensitive and controversial, as it touches upon the relationship between the state and citizens (see D3.1 for an overview). Recent surveys show that citizens are aware of the benefits as well as the risks. While people tend to agree that AI use by police can benefit the society, they also express important civil right concerns (Akhgar, 2022). On the one hand, AI in law enforcement promises to enhance citizens' safety with a more efficient and effective prevention and control of criminal activities. The potential benefits that AI has for law enforcement include a facilitated identification of suspected individuals or vehicles, a support in the prediction and mapping of criminal activity and decision making, an ease in flagging fake news, tracking illicit flows of money, identifying CSAM material or terrorist activities (INTERPOL & UNICRI, 2019). On the other hand, the use of AI in the security domain presents some serious risks for civil liberties and rights. First, data used by AI can be embedded with bias, reinforcing inequality, and preventing equitable outcomes. Predictive models might use data representing structural inequalities (see D3.1). For example, data produced within the judiciary systems, like crime records, might not represent levels of criminality but policing priorities and the social groups that are most targeted by it. Furthermore, they do not take into consideration the concept of rehabilitation, targeting continuously those who have already paid their debt (Reese, 2022). Next, the purpose of the system might not be clear and might reflect biases and perspectives of its creators (Robinson, 2016). There are also mounting concerns on the rise of an Orwellian state, where governmental agencies exercise extensive control over citizens life, increasing the power asymmetry between the government and the people. Additionally, risk is increased by a lack of

[1] https://oecd.ai/en/countries-and-tools

human oversight, transparency, and accountability through the AI process. Accountability and oversight are crucial to prevent risks when using AI and people have explicitly asked for 1) more transparency regarding how AI is used and its effects; 2) more information about the police operations that involve AI and 3) more evidence showing how AI for police translates into positive change (Akhgar, 2022). This means that to democratise AI in the security domain without seconding already existing power asymmetries, it is crucial to put at the center the people who are subjected to its use, as well as AI developers and users.

Given the risks that AI in security entails, regulatory frameworks are necessary to govern the use of AI in the security domain and citizens have expressed the importance of establishing binding laws to protect their rights (Akhgar, 2022). The central question for regulatory approaches is how they protect citizens and manage their concerns. The following sections of this report will try to answer this question by proposing a taxonomy that seeks to unify the human right, data and artificial intelligence legal perspectives to facilitate the comparison between legal frameworks that affect AI.

2.1 The Legal taxonomy

Legal taxonomies sort legal rules. There are three different methods to classify laws: formal, function-based or reason-based (Sherwin, 2009). A formal taxonomy focuses on the logical relations between laws. The primary criteria to create a formal taxonomy is the internal logic of law instead of external factors such as their social function or moral considerations. A reason-based taxonomy classifies rules according to the reasons that justify them. A function-based taxonomy provides a classification of legal instruments according to the roles they perform within the legal system or society at large. In this type of taxonomy, each category of law contains solutions to a particular type of problem or dispute. This report proposes a three-class high level function based taxonomy, depicted in Figure 1, to classify regulations that apply to the use of AI in the security domain. The three high level classes -Human Rights, Data and Artificial Intelligence- correspond to three broad functions of the laws reviewed: the protection of human rights, the protection of data (title: Data), and the protection of individuals from AI related risks.

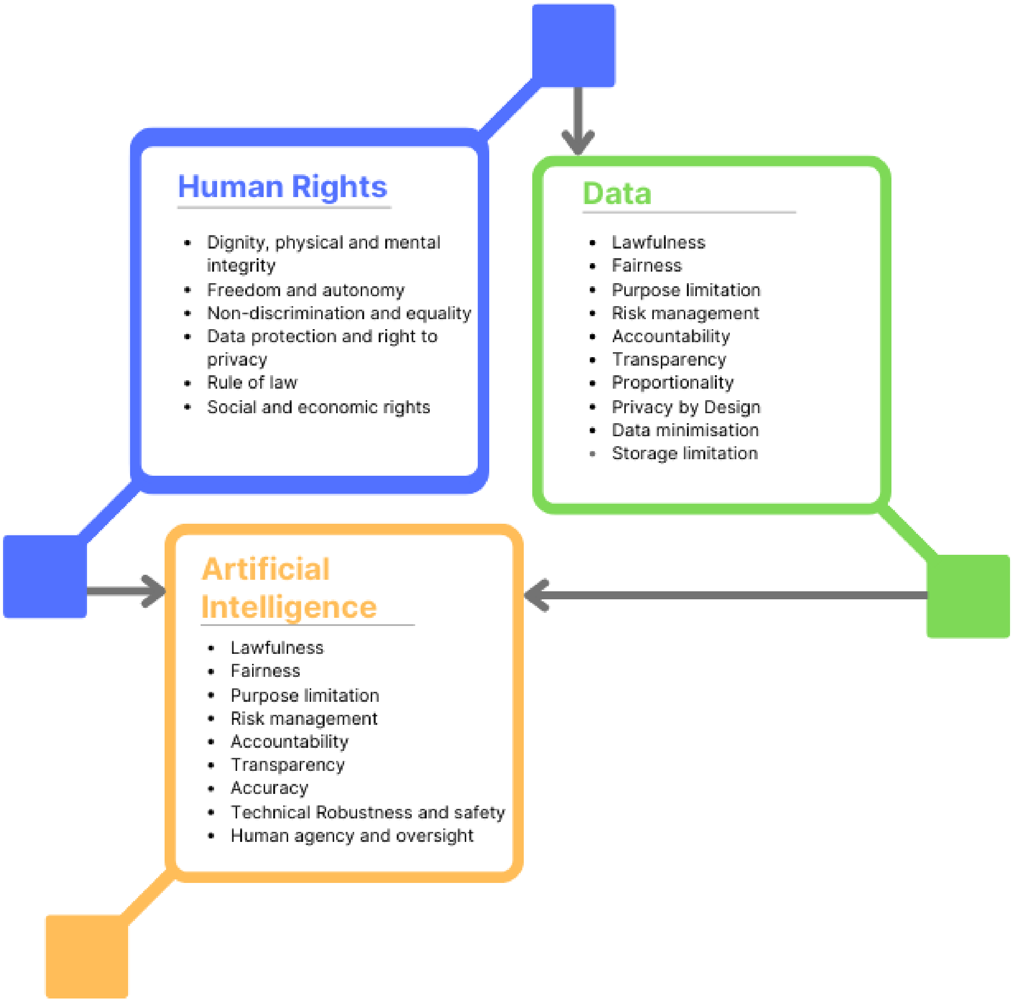

Figure 1: A visual representation of the taxonomy and the key principles within each class.

Each class is articulated into several key principles which represent important areas that regulatory approaches need and seek to address to develop trust, and settle social controversies and disharmonies related to the use of AI applications in the security domain. Some of the principles of the Data and AI class overlap (see Figure 2) and the taxonomy highlights differences in the way they are addressed. For each of these principles, this report will illustrate practical examples of how regulatory frameworks attempt to address them.

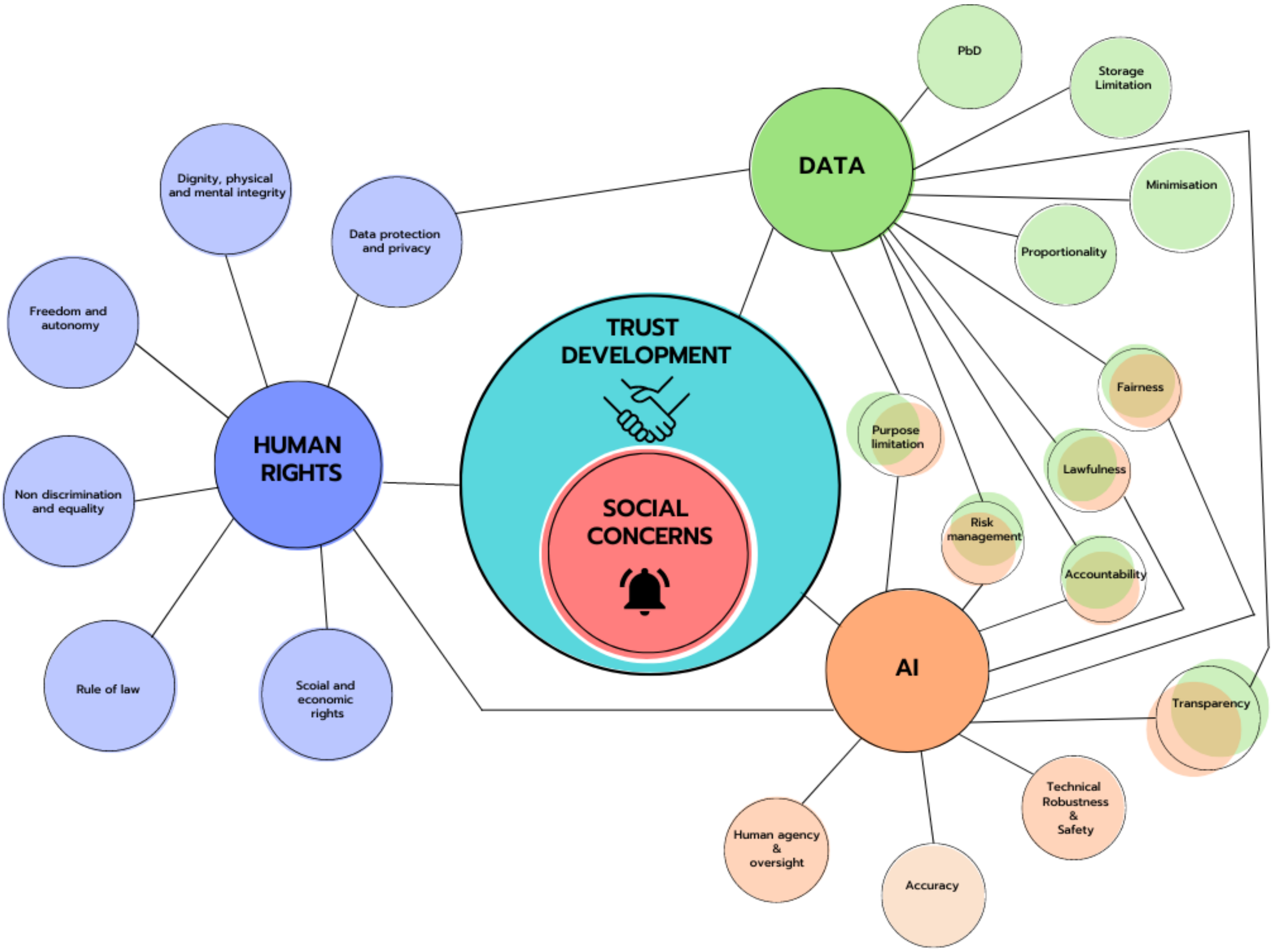

Figure 2: Links between principles and classes. Social concerns are at the center of the taxonomy.

This classification aims to simplify the categorization of regulations that apply to AI in order to enable to 1) better compare how regulations address social concerns, 2) identify areas and intersection of areas that are currently not covered by binding and non- binding instruments and 3) promote a unified approach that merges human rights, data and AI related concerns. At a high level, the proposed taxonomy recognizes three broad categories of laws that apply to AI.

1. **Human rights:** this class refers to regulations that define fundamental rights that must not be violated by AI applications. Human rights are the basic rights and freedoms that are possessed by all human beings from birth to death and they protect the dignity of each person regardless of their race, ethnicity, gender, age, sexual orientation, class, religion, disability status or any other characteristic. The basic human rights as we know them emerged in the 20th century, in the aftermath of World War II. Fundamental rights and freedoms bind governments to protect and fulfill them. When human rights are violated, people are entitled to legal remedies (see sections 3.1 and 3.2 for some examples by CJEU and ECtHR). Artificial Intelligence applications in the security domain can negatively impact a

wide range of human rights such as the right to privacy, freedom of assembly, non-discrimination, right to an effective remedy among others. Making an ethical and trustworthy AI in the security domain involves primarily assessing risks and setting standards ensuring civil, political, economic, social and cultural rights.

2. **Data:** this class refers to data protection regulations that apply to AI and includes an in-depth analysis of European instruments. The processing of data is governed by data protection laws, which started to emerge in the last decades of the 20th century. Many principles of those laws (e.g. purpose limitation, data minimisation, the special treatment of sensitive data) aimed at setting controversies in the data domain are also relevant to AI applications and have been used so far, by data protection authorities to sanction and ban AI applications (see Section 3.3). The tension between the advantages of using AI technologies in the security domain and the risks are evident in the field of data. Artificial Intelligence applications can use, collect, detect personal data that can be employed, for example, to profile individuals or produce predictions of their behaviours. Personal Data can be used to analyse or forecast human behaviour and the outcome of an AI system using such data can be used to make complex decisions. Therefore, to develop ethical and trustworthy AI, it is also vital to ensure that data protection laws and their principles are fulfilled.
3. **Artificial Intelligence** is a domain that poses its own challenges when it comes to regulations. These challenges include, for example, ensuring accountability in the AI-human interaction, appropriate levels of understandability and transparency regarding AI systems' purpose, how they work and how they use data to produce an output. Therefore, this class refers to regulations that are specific to Artificial Intelligence and want to address concerns specific to AI systems. The regulatory effort on AI is very recent. It started in the second decade of the 21st century with the publication of AI principles and ethical guidelines and is ongoing, with most of AI regulations still at the proposal stage. This class includes 1) EU binding instruments 2) EU non-binding instruments showing how to apply existing non-specific AI regulations (eg. Data protection laws) to AI 3) US laws destined to govern AI and AI applications.

Furthermore, Appendix A indicates for each document the functionality/ies mentioned. Where possible, it refers to D2.1 functionalities.

The following sections will discuss in-depth the three classes and the principles within each class that regulations are seeking to pursue.

2.2 Human rights

The development and deployment of AI systems for law enforcement and criminal justice must comply with regulations that ensure democratic rights and civil liberties. This is fundamental to build public trust in AI use by LEAs. Systems powered by AI used for law enforcement are subject to human rights covenants. These are the most basic level of regulation that set out principles for normative reference and cannot be in conflict with law. Fundamental rights and civil liberties protect a person's dignity based on the mere fact of being human. They promote equality in the treatment of citizens and discourage oppression and abuse from private and public actors. In Europe, the most important legislations are the **European Convention on Human Rights**

(ECHR)[2], the **Charter of Fundamental Rights of the EU** (CFR) [3] and the **European Social Charter**[4] (ESC) which are largely based on the **Universal Declaration of Human Rights** (UDHR) the **International Covenant on Civil and Political Rights** (ICCPR) and the **International Covenant on Economic, Social and Cultural Rights** (ICESCR). Respect to human rights is also emphasized in the EU treaties: the **Treaty on the European Union** (TEU)[5] and the **Treaty on the Functioning of the European Union** (TFEU)[6]. EU treaties are binding agreements between EU member countries. They set out EU objectives, rules for EU institutions and how decisions are made. For example, Article 2 of the TEU establishes that "the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities".

The Council of Europe and the Ad Hoc Committee on Artificial Intelligence (CAHAI) has carried out significant work[7] to define a methodology to carry out impact assessments of AI applications from the perspective of human rights, democracy and the rule of law. As this report is being written, there is no binding document requiring a human rights impact assessment of AI systems used in the security domain.

There is no binding instrument requiring human rights impact assessment of AI systems. In this regard, legal requirements must be established as well as binding and non-binding guidelines defining how to carry out human right impact assessments of AI systems.

The human rights that must be safeguarded when employing AI applications in the security domain are related to six broader areas: human dignity, physical and mental integrity; human freedom and autonomy; non-discrimination and equality; data protection and right to privacy, rule of law and social and economic rights.

2.2.1 Dignity, physical and mental integrity

Surveillance, communication, prediction and recognition functions (C.1, C.2, C.4 in D2.1 taxonomy) powered by AI tools might affect people behaviorally and psychologically and can push individuals to conform to certain norms. This increases the asymmetry of power between LEAs using AI, and those who are subjected to AI. AI tools used in the security domain must respect:

- Human dignity (Art. 1, ECHR; Art. 1 CFR)
- Right to the Integrity of the person (Art. 3 CFR)
- Right to liberty and security (Art. 5 ECHR; Art 6 CFR)

[2] https://www.echr.coe.int/documents/convention_eng.pdf

[3] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[4] https://www.coe.int/en/web/european-social-charter/home

[5] https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

[7] https://rm.coe.int/cahai-pdg-2021-02-subworkinggroup1-ai-impact-assessment-v1-2769-4229-7/1680a1bd2d

Article 5 of the AI Act prohibits the placing on the market, putting into service or use of AI system that deploys subliminal techniques beyond a person's consciousness or that exploits people's vulnerabilities in order to materially distort a person's behaviour in a manner that causes or is likely to cause physical or psychological harm. It also bans the use of social scoring to evaluate the trustworthiness of a person by public authorities but not private companies.

On the other hand, AI systems intended to be used by LEAs for risk assessments, for emotional detection (e.g. polygraph) are not prohibited and are classified as high risk

2.2.2 Freedom and autonomy

AI powered systems that automatically track individuals and their communication (C.1, C.2, C.4 in D2.1 taxonomy) might jeopardise their freedom of expression and assembly. Because of surveillance and recognition, people might be discouraged to participate to social protests and demonstrations and might diminish their willingness to express their opinion. AI tools used in the security domain must respect:

- Freedom of expression (Art. 10 ECHR; Art. 11 CFR)
- Freedom of assembly and association (Art. 11, ECHR; Art 12. CFR)
- Freedom of movement and of residence (Art. 45 CFR)

2.2.3 Non-discrimination and equality

AI systems are often seen as neutral and objective but they replicate human biases. The risk of discrimination can arise from biased data, from biased design of the algorithm or optimisation, or from AI contextual use. The need for protection of the articles below is particularly evident for AI recognition functions (C.1), as, for example, facial recognition has been shown to have higher error rates for women and women of colour (e.g. Gender shades project; Buolamwini & Gebru 2018), as well as for data analytics (C.3). For the latter case, a good example is the data used for predictive policing which have been demonstrated to reflect patrolling priorities in disadvantaged areas rather than criminal activities, risking to lead to patrolling decisions that contribute to self-fulfilling prophecies: if police are dispatched to a specific area, it will follow that more crime will appear there (Browning & Arrigo, 2021). AI tools used in the security domain must be in line with rights on:

- Prohibition of discrimination (Art. 14 ECHR; Art. 21 CFR; Art. 10 TFEU)
- Equality between men and women (Art. 23 CFR)

In the context of non-discrimination, The Employment Equality Directive[8], the Racial Equality Directive[9], the Gender Goods and Services Directive[10] and the Gender Equality Directive[11] are also relevant and their articles need to be respected.

2.2.4 Data protection and right to privacy

AI systems use, track, and recognize data (C1, C2, C3 and C4 in D2.1 taxonomy). When data is processed it is crucial to respect people's right to privacy:

- Right to respect for private and family life (Art. 8, ECHR; Art. 7 CFR)
- Protection of personal data (Art. 8 CFR, Art. 16 TFEU)

2.2.5 Rule of law

AI systems making individual predictions (Delia, Italy), profiling (Top 600, The Netherlands) and assessing risk (e.g. ProKid, The Netherlands) are used to inform law enforcement actions and judiciary decisions. The opaqueness that characterise the AI systems (C1, C2, C3 and C4 in D2.1 taxonomy) makes it hard to understand the reasoning behind an output, to challenge the decision and have an effective remedy. This has a direct effect on people's right to have a fair trial, their presumption of innocence and their right to have an effective remedy. AI tools used in the security domain must not violate the following rights:

- Right to have a fair trial (Art. 6 ECHR; Art. 47 CFR)
- No punishment without law (Art. 7, ECHR)
- Right to an effective remedy (Art. 13, ECHR; Art. 47 CFR)
- Presumption of innocence and right of defence (Art. 48 CFR)

2.2.5.1 Social and Economic Rights

The use of AI by LEAs creates also new risks and challenges for Social and Economic rights of the persons working in law enforcement and judicial environment. For example, the use of AI implies new training for LEAs and judiciary authorities to fill expertise gaps (e.g. INTERPOL & UNICRI, 2019), and new assessment for risks of their use at the workplace. The rights to be taken into consideration are:

- The right to work and to be appropriately trained (Art. 1 ESC)
- The right to just conditions of work (Art.2 ESC)
- The right to safe and healthy working conditions (Art. 2 ESC)

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0078

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0043

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0113

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0054

- The right to protection of health (Art. 11 ESC)

The next section will discuss in-depth the Data class of the taxonomy.

2.3 Data

Data protection can be defined as the normative framework that defines the rules for the processing of personal data. Up to date, the European legal frameworks that regulate AI systems largely coincide with the legal instruments that govern privacy and the processing of data. This is consistently shown by the Data Protection Authorities' decisions illustrated in section 3.3. This section reviews the data protection legal tools that have been used to regulate AI in the EU and highlight the main points referring explicitly to automated processing of data. This exercise shows that regulations before the AI act, only refer to "profiling" and "automated decision making", or more generally to "automated processing of data". Next, this section presents the data protection principles relevant for AI and shows how they have been addressed by EU data law. Requirements set by Convention 108+, the General Data Protection Regulation, the Law Enforcement Directive, the Passenger Name Record Directive, Regulation EU 2018/1725 and the e-privacy directive have been used to define the data protection regulation principles that apply to AI.

Convention 108+[12], modernizes the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and sets the standards on rights to privacy and data protection of individuals. The convention includes strong requirements regarding the proportionality and data minimisation principles, the lawfulness of data processing, extends the types of sensitive data to genetic and biometric data as well as ethnic origins, and requires greater accountability of data controllers among others. Convention 108+ has some explicit references to "automated decision making". Article 9 (1a) provides that individuals should not be subjected to a decision that affects them based solely on an automated processing of data without having their views taken into consideration. Further, Article 9 (75 Littera a) grants the rights to individuals who may be subject to automated decision to challenge such a decision. In particular, it provides that data subjects should have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to their particular situation, or other factors that will have an impact on the result of the automated decision. Finally, Article 9 (77 Littera c) entitles data subjects to know the reasoning underlying the processing of data, including the consequences of such a reasoning, which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated decision making including profiling. For instance, in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a “yes” or “no” decision, and not simply information on the decision itself. Having an understanding of these elements contributes to the effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority.

To enable a development and deployment of AI that respects data protection and fundamental rights, in 2019 the Council of Europe published the **Guidelines on Artificial Intelligence and Data Protection**[13]. These guidelines are a non-binding tool providing high-level measures that governments, AI developers,

[12] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[13] https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

manufacturers, and service providers should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms, in particular with regard to the right to data protection. The Guidelines instruct that AI development should be based on 108+ principles which are:

- lawfulness
- fairness
- purpose specification
- proportionality of data processing
- privacy-by-design and by default
- responsibility and accountability
- transparency, data security
- risk management

Another important legally binding tool that applies to AI is Regulation **(EU) 2016/679** or the **General Data Protection Regulation[14] (GDPR),** which aims to address privacy and security concerns within the European Union and was adopted by the EU to give Convention 108+ legal force**.** The GDPR does not contain any explicit reference to AI but mentions automated decision making and some data processing that imply the use of AI powered systems. In this regard, Article 22 refers to profiling and automated decision making, which imply the use of AI technologies. Article 22 provides that data subjects have the rights not to be subject to a decision solely based on automated processing, including profiling which produce legal effects concerning them of where they similarly significantly affect them. Recital 71 states that decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, and should be subject to suitable safeguards. It states that the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions. Finally, Article 35 provides that a data protection impact assessment (DPIA) should be conducted when the processing of data through new technologies is likely to result in a high risk to the rights and freedoms of natural persons.

Another important instrument specific to LEAs is the **Directive (EU) 2016/680[15]** known as the **Law Enforcement Directive (LED).** This directive has set rules to govern the processing of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against threats to public security. LED indicates that the processing of personal data through automatic means should protect natural persons. Similarly to Article 22 of the Convention 108+, Article 11 prohibits member states to make decisions based solely on automated processing, including profiling when they produce an adverse legal effect on the individual or effects that are similarly

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504

significant. It also prohibits profiling that results in discrimination on the basis of special categories. Article 10 regards the processing of biometric data and allows its processing only where strictly necessary, with appropriate safeguards and only when authorised by a Union or Member State, to protect vital interests or when data are made public by the data subject. Article 25 requires member states to keep logs for operations in automated processing systems, which should be able to provide the justification, as well as time and date of the operations. Article 27, similarly to Article 35 of the GDPR, requests to conduct a Data Protection Impact Assessment (DPIA) when the data processing is likely to result in a high risk to the rights and freedoms of natural persons. Furthermore, Article 28 orders a consultation to a supervisory authority when the type of processing when using new technologies involves a high risk to the rights and freedoms to the data subjects. Article 29 defines obligations regarding safety measures to implement in respect to automated processing.

Directive 2016/681[16] aims to regulate the transfer of the passenger name record (PNR) data of passengers on international flights from airlines to the European Union (EU) Member States as well as the processing of these data by Member States' competent authorities. The PNR directive presents a relevant article for automated decision making as Article 22 of the GDPR and Article 11 of LED. Article 7 (6) provides that competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation. Furthermore, Article 6 (5) provides that any positive match resulting from the automated processing of PNR data needs to be individually reviewed by non-automated means to verify whether the competent authority needs to take action under national law.

Regulation **EU 2018/1725**[17] **or EU-DPR** lays down the data protection obligations for the EU institutions and bodies when they process personal data and develop new policies. Also this regulation refers to automated decision making and profiling. Article 17 provides that if automated decision-making is used, including profiling, the data subject has the right to obtain from the controller meaningful information about the logic involved. Article 24 states that data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Finally, Directive **2002/58/EC**[18] known as the **e-Privacy directive** regulates publicly available electronic communication services and telecommunication services irrespective of the technologies used. The e-Privacy directive does not refer explicitly to AI, but mentions automated calling systems, which might be based on AI technologies. Article 13 limits the use of automated calling systems without human intervention to subscribers who have given their consent.

Interestingly, EU data protection regulations refer to "data subjects" multiple times: 162, 405, 342 times for LED, GDPR EU-DPR respectively. The AI Act proposal has only 2 references to the "data subject" and there is no reference to the rights of those who are subjected to AI. For example, in the GDPR it is clear what the rights

[16] https://eur-lex.europa.eu/eli/dir/2016/681/oj

[17] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32018R1725

[18] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

of the data subjects are (chapter 3). In the AI act, it is not clear what the rights of the persons who are subjected to AI systems are.

> To protect citizens, European institutions shall define with clarity the rights of the persons who are subjected to AI systems.

The map in Figure 3 suggests that the Council of Europe, the European Commission and the European Data Protection Board are translating data protection laws into guidelines explaining how to apply them to AI and AI applications. In the future, EU institutions shall produce or facilitate the production of guidelines that are both sector (e.g. Law Enforcement) and also application (Facial Recognition, Decision Making, Prediction) specific and that unify the data, human right and AI perspectives.

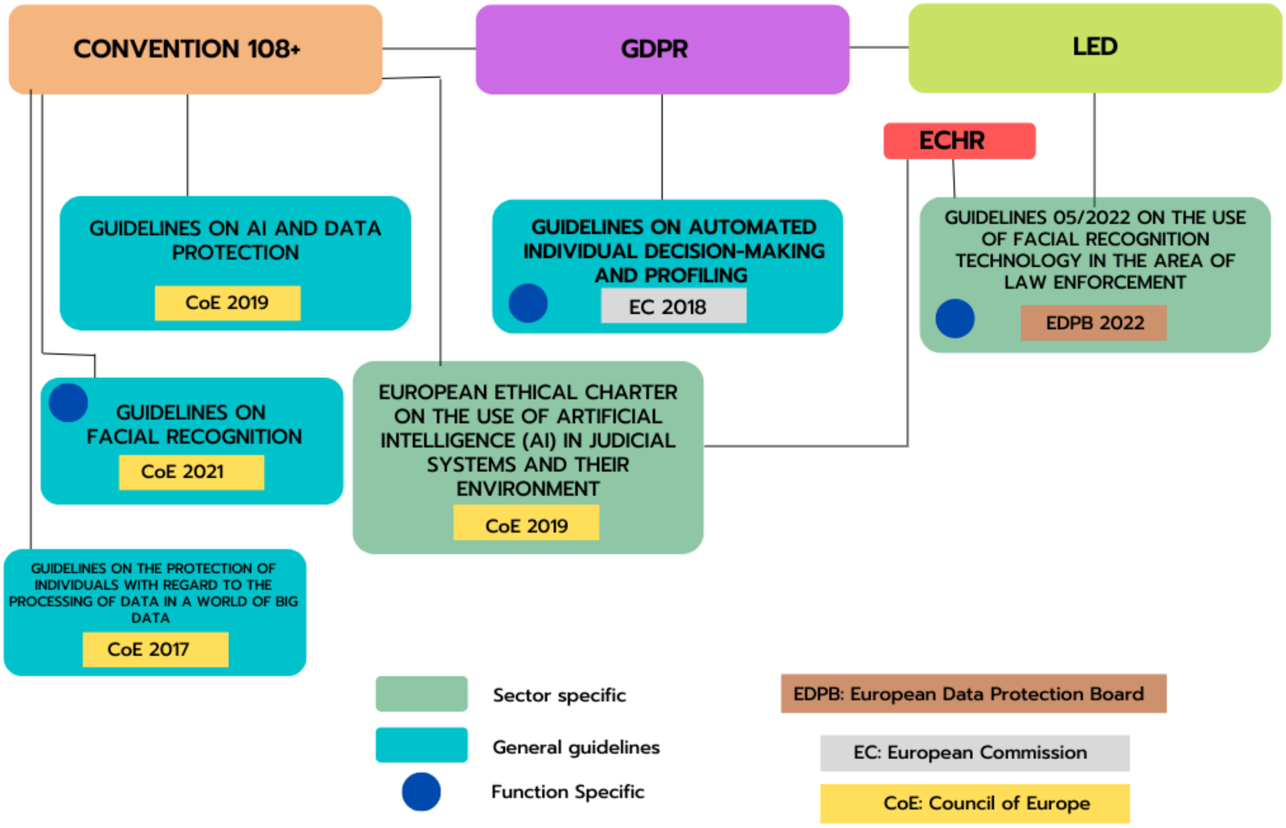
CONVENTION 108+
GDPR
LED
ECHR
GUIDELINES ON AI AND DATA PROTECTION
CoE 2019
GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING
EC 2018
GUIDELINES 05/2022 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT
EDPB 2022
GUIDELINES ON FACIAL RECOGNITION
CoE 2021
EUROPEAN ETHICAL CHARTER ON THE USE OF ARTIFICIAL INTELLIGENCE (AI) IN JUDICIAL SYSTEMS AND THEIR ENVIRONMENT
CoE 2019
GUIDELINES ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF DATA IN A WORLD OF BIG DATA
CoE 2017
Sector specific
General guidelines
Function Specific
EDPB: European Data Protection Board
EC: European Commission
CoE: Council of Europe

Figure 3 A map of guideline documents deriving from data protection laws.

The following sections will discuss the principles of the data class of the taxonomy.

2.3.1 Lawfulness

Lawfulness in data protection means that data cannot be used unlawfully. Data are processed lawfully when:

- the data subject has given the consent (Art.5(3) Convention 108+, Art. 6 GDPR; Art.5 Regulation EU 2018/1725)
- the processing is necessary for the performance of a contract, for compliance with legal obligation, to protect the vital interest of the data subject, for the performance of a task carried out in the public interest or in the exercise of official authority (Art. 6, GDPR; Art.5 Regulation EU 2018/1725).
- Article 8 of the LED provides that Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security and that it is based on Union or Member State law. Furthermore, the article indicates that member states must protect the fundamental rights and freedoms of natural persons.

Furthermore, Art. 25 of LED established that logs should be kept and used for the verification of the lawfulness of processing. Art. 15 of the PNR tasks the National supervisory authority to verify the lawfulness of the data processing.

2.3.2 Fairness

Any processing of personal data should be fair. The principle of fairness requires data subjects to be informed of the existence of the processing operation and its purposes.

- The controller to provide the data subject with the information necessary to ensure fair processing (Art. 13 GDPR, Art.4 EU 2018/1725) and instructs Member States, the supervisory authorities, the Board and the Commission to encourage the creation of code of conducts to contribute to the application of the GDPR (Article 13 GDPR).
- Article 14 of LED provides that Member states should assure that data are processed fairly

2.3.3 Purpose limitation

Personal data should only be collected for specified, explicit and legitimate purposes and not processed further in manners that are not compatible with those purposes (Art. 5 GDPR; Art. 4 LED; Art. 4 EU 2018/1725).

- Processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (Art. 89(1) GDPR) is not considered to be incompatible with the initial purposes.
- Art 4. (3) LED requires authorization for processing personal data for the stated purpose and requires that processing is necessary and proportionate.

2.3.4 Proportionality

The processing of information should be adequate, relevant, suitable, necessary and not excessive in relation to a specified purpose.

- For high-risk processing activities a Data Protection impact assessment is required which needs to assess the proportionality of the processing operations (Art. 35 GDPR).

- Art 4 LED states that processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

2.3.5 Privacy by Design

Privacy by Design means embedding data privacy features into the design of projects at an early stage and through its lifecycle. Privacy by Design is addressed by Art. 25 GDPR; Art.20 of LED; and Art. 27 EU 2018/1725. When planning the processing and during the processing of the data, the controller should implement appropriate technical and organisational measures which are designed to implement data-protection principles [...] in an effective manner and to integrate the necessary safeguards into the processing (Art. 25 (1) GDPR, Art. 27 EU 2018/1725, Art. 20 LED)

2.3.6 Data minimisation

Data minimisation means collecting and processing the minimum amount of personal data needed for the objective. In this regards, data need to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Art. 5(c)GDPR; Art. 71 EU 2018/1725 address minimisation and require the implementation of appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

2.3.7 Responsibility and accountability

The principles of responsibility and accountability require organizations to put in place appropriate technical and organizational measures to demonstrate what has been done under request.

- The controller is responsible for a lawful, fair and transparent data processing (GDPR Art.1 GDPR, Art. 4 LED, Art. 15 EU 2018/1725)
- logging needs to be kept for processing operations in automated processing systems that involve the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data (Art. 25 LED, Art. 88 EU 2018/1725)

2.3.8 Transparency

Transparency requires that information related to the processing of personal data is easily accessible and understandable. The data controller needs to demonstrate that personal data are processed in a transparent manner (Art. 5(2) GDPR) and need to provide any information relating to the processing in a transparent and accessible form (Art. 12 GDPR).

2.3.9 Storage Limitation

Storage limitation of personal data reduces the risk that data become irrelevant, excessive and inaccurate. Art. 5 LED specifies that Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed. The controller is requested to indicate the period of storage (Art. 25, GDPR; Art. 25 EU 2018/1725)

2.3.10 Risk Management

While the AI Act proposal (section 2.4.1) follows a risk-based approach, EU data protection regulation is right based, meaning that it is focused on protecting citizens' data protection rights. Regulations governing data protection have multiple references to risk management. For example, controllers are called to consider risks (Art. 19 & 20 LED, Art. 24 & 25 GDPR, Art. 33 EU 2018/1725). When the use of new technologies is likely to result in a risk to the rights and freedoms of natural persons, a Data protection impact assessment is required (Art. 27 LED, Art. 35 GDPR, Art. 39 EU 2018/1725). This needs to include an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data.

The following paragraph will analyse EU and US regulatory panorama and will discuss the principles of the Artificial Intelligence class of the taxonomy.

2.4 Artificial Intelligence

This section will outline both binding and non-binding instruments such as communications, recommendations and guidelines that have been produced in the EU and US in the attempt to regulate the development and use of AI in the security domain. It will also compare the EU and US legislation in relation to the principles outlined in the taxonomy.

2.4.1 European Union

The European Union started to develop regulatory frameworks for AI only very recently. In 2018, the European Commission established a European strategy on AI[19] followed by a coordinated plan[20]. In the coordinated plan, the European Commission planned to allocate substantiate funding to AI for security purposes to deploy AI tools in support of LEAs to better prevent, detect and investigate terrorism. On the other hand, it emphasized an approach based on ethics and security by design that facilitates LEAs activities. To support the implementation of the EU AI strategy, the Commission constituted a European AI alliance and AI High Level Expert group (AI HLEG) which produced the Ethics guidelines on Trustworthy AI (Table 1) [21],a practical Assessment List for Trustworthy AI (ALTAI)[22] and policy and investment recommendations[23] that called for more debate, research, and scrutiny on the use of AI by LEAs.

Human agency and oversight	AI systems need proper human oversight (e.g. human-on-the-loop) and empower humans to make informed decisions.
Technical Robustness and safety	AI systems need to be safe, reliable, accurate and reproducible.
Privacy and Data Governance	AI systems should ensure full respect of privacy and data protection.
Transparency	Data, systems and AI business models should be transparent.
Diversity, non-discrimination and fairness	AI systems should avoid unfair bias and foster diversity.
Societal and environmental wellbeing	AI systems should be sustainable and environmentally friendly.
Accountability	There should be mechanisms that ensure responsibility and accountability for AI systems and their outcomes.

Table 1 The 7 EU key requirements that AI systems must meet to be trustworthy.

[19]https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe

[20] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#ecl-inpage-l6ov8brl

[21] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[22] https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[23] https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-sectoral-considerations-policy-and-investment-recommendations-trustworthy-ai

In 2020, the Commission created the Expert Group on Artificial Intelligence in the domain of Home Affairs[24], composed only by member states authorities and public entities, tasked with assisting the Directorate-General for Migration and Home Affairs in preparing legislation.

The expert group has raised concerns among MEPs for a lack of transparency, the failure to include in the agenda controversial topics and the lack any member of civil societies to guarantee the respect of human rights (In't Veld, 2021). Following MEP question, the Commission answered "Depending on the topic of discussion, other organisations, including academia, are also invited. For instance, in the fourth meeting representatives from the Norwegian Business School and the Université Côte d'Azur presented their work on surveillance in urban security. Given the plurality of the profiles of the participants, the Commission considers that the discussions of this expert group are balanced, also as regards the topic of potential risks posed by artificial intelligence to fundamental rights. The matters for discussion within the group are selected on the basis of their relevance, significance and timeliness. The goal is to provide participants with information and generate discussion on key topical issues in the context of the various work strands within the policies of artificial intelligence and the European Data Strategy." (Johasson, 2021).

In the same year, the European Parliament established a Special Committee on Artificial Intelligence in a Digital Age (AIDA) with the goal of setting out a long-term EU roadmap on Artificial Intelligence (AI). In a recent resolution[25], AIDA stressed the importance of AI boosting LEAs' ability to identify and counter criminal activities. It also emphasised the risks that AI misuses pose for fundamental rights and the importance to have civil societies, academia and LEAs cooperating to protect them.

In 2021, the European Commission published a review of the 2018 Coordinated Plan on Artificial Intelligence[26] and established the development of harmonized standards in all member states for the creation of rules to regulate AI. In the reviewed plan, the European Commission proposed to build a strategic leadership in "Applying AI to law enforcement, migration and asylum" by, among others, 1) funding the UN Interregional Crime and Justice Research Institute project, to develop a global toolkit for law enforcement agencies with a view to fostering the trustworthy, lawful and responsible use of AI for law enforcement, 2) launching proofs of concepts for concrete use-cases of AI in the field of migration border control and police checks and 3) funding research on AI and innovation. In this regard, there are several documents highlighting the role of AI to respond to terrorist threats and crime management and to the facilitation of the EU commission in the development of these technologies[27]. In October 2021, the European Parliament adopted a resolution[28] that called for the EU Fundamental Rights Agency, in collaboration with the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), to draft guidelines, recommendations and best practices

[24] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3727

[25] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html

[26] https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0795&qid=1631885972581 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1632306192409

[28] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

in order to further specify the criteria and conditions for the development and deployment of AI applications and solutions used by law enforcement and judicial authorities. The resolution also planned to carry out a study on the implementation of the Law Enforcement Directive to identify how privacy is ensured by Law Enforcement and Judicial authorities particularly when it comes to new technologies. Finally in April 2022 the European Parliament and the Council, published a proposal for a regulatory framework on artificial intelligence: the **AI Act (AIA)**[29].

The AI Act proposes to implement a risk-based framework to govern AI. AI systems of unacceptable risk will be prohibited, high risk systems that could have an adverse impact on safety or fundamental rights are subject to a number of specific governance requirements, limited risks systems will be subjected to transparency requirements whilst minimal risk systems will be encouraged to follow codes of conduct respectively.

Risk based regulations target activities that pose the highest risk to the public and lowers requirements for lower risks sectors. The AI act seeks to introduce safeguards on developers and users of AI systems that might violate the safety and fundamental rights of people. There are a number of challenges regarding the definition of risks and AI: risk is not well-defined and it is hard to measure quantitatively and qualitatively. Furthermore, level of risk of an AI application can vary and become unacceptable depending on the context and on the population (eg. vulnerable groups) on which it is used.

AI systems used for the purpose of law enforcement, migration, asylum and border control management and the administration of justice fall under the category of high-risk systems.

As the US section will show, US national laws proposed and enacted this far are sector (e.g. Law enforcement) and function specific (e.g. facial recognition in body camera, ADM systems).

As high-risk systems, AI tools used for the purpose of law enforcement (e.g. for profiling, crime analytics, to detect emotional states, deep fakes, to evaluate the reliability of evidence, to predict the occurrence of crime), migration, asylum and border control management (e.g. verification of documents) and the administration of justice (e.g. to assist the interpretation of law and facts) are subjected to the following measures:

- adequate and iterative risk assessment and mitigation systems (Art. 9);
- high quality of the datasets feeding the system to minimise risks and discriminatory outcomes (Art. 10);
- up to date technical documentation providing all information necessary on the system and its purpose for authorities to assess its compliance (Art. 11)
- automatic record of activities to ensure traceability of results (Art. 12);
- clear and adequate information that enables the user to interpret the system output and use it appropriately (Art. 13) ;
- guarantee appropriate human oversight measures during the use of the AI system (Art. 14);

[29] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

- high level of robustness, security and accuracy which should be declared in the accompanying instructions of use (Art. 15).

The AI Act sets out several obligations for users providers - and importers (Art. 26)- of high risk systems such as a conformity assessment that demonstrate the compliance with the requirement outlined in AIA Chapter 2 (Art.19). The conformity assessment can be performed internally or by a third party. These third parties are notified bodies that satisfy the requirements provided by Art. 33. and that have been designated by a notifying authority.

According to recital 64, the Conformity assessment will be performed internally by the provider with the only exceptions of AI system to be used for real time and post emote biometric identification of a person.

While LED requires a DPIA carried out by the controller when the processing is likely to be high risk to the rights and freedom, the conformity assessment of a high risk system is primarily carried out by the provider (or by a product manufacturer, distributor or importer or a third party under specific conditions).

The AI Act also instructs member states to designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation, and notification of conformity assessment bodies and for their monitoring (Art. 30). Furthermore, users are called to inform the provider or distributor when they have identified any serious incident or any malfunctioning.

Further, the AI Act proposal prohibits the use of those systems whose risk is "unacceptable" because, for example, they violate fundamental rights. It prohibits the use of real-time remote biometric identification systems in public access spaces for law enforcement purposes unless it is needed for targeted search of potentials victims of crime, the prevention of an imminent threat to life and the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence (Art. 5). Each use of a ‘real-time’ remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. With this, the AI Act distinguish between real time and remote biometric identification, leaving the latter under the jurisprudence of from Article 9(1) of Regulation (EU) 2016/679, Article 10(1) of Regulation (EU) 2018/1725 and Article 10 of Directive (EU) 2016/680.

The AI Act establishes that AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences (Section 38).

To support innovation, the AI Act proposal establishes regulatory sandboxes (Art. 53) which enables the further processing of personal data lawfully collected for other purposes for AI systems destined to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public safety, under the control and responsibility of the competent authorities (among others.

Finally, it is important to consider that any breach of the rules set out in the AI Act may entail fines of up to EUR 30 000 000 or, if the offender is a company, up to 6% of the total annual worldwide turnover of the previous financial year.

2.4.2 United States of America

The United States, being a federal state, is regulated at both the national and local levels. This means that each of the 50 states has the power to issue its own regulations as long as they do not contradict the federal constitution. During Trump administration, a memorandum discouraged[30] any regulatory and non-regulatory federal action with the fear that they would hamper innovation. However, over the years, a series of proposals have been launched to establish certain parameters and principles aimed at strengthening an adequate regulation. In this regard, in February 2019, Executive Order 13859[31] "**Maintaining American Leadership in Artificial Intelligence**" emphasized the role of AI in enhancing security, established a series of principles and strategies to strengthen the USA capabilities in AI and appointed the **US National Institute of Standards and Technology** (NIST) to create a federal engagement in the development of technical standards for AI technologies[32]. NIST development of technical standards is following a voluntary consensus standard logic where the public sector relies on and assists private agencies to provide technical standards. These standards include clear guidelines for the design and development of AI systems, sharing best practices and setting clear measurements of AI performance.

The EU AI act generally refers to harmonised standards and requirements for conformity assessment (e.g. human oversight, record keeping) but no rule has been set on measuring AI systems performance and assess bias quantitatively. To assure an ethical use of AI in the security domain, the EU must develop a perspective on clear measurements of performance and quantified standards that AI applications need to meet (e.g. Face Recognition Vendor Test).

NIST is also developing a risk management framework for voluntary use to help AI developers and users to identify risk, manage it and address it purposefully. The work is on progress and utilizes a "crowdsource" approach where public comments are requested via email and through the participation to public workshops[33]. In the last draft, the AI Risk Management Framework Core propose a culture of risk management providing a list of actions that enable mapping measuring and managing risks[34].

The EU AI act requires the establishment of a risk management system (Art. 9) for high risks AI systems. The actual indications for AI risk management lack details in respect to the where, when and what type of risk might arise and how to manage it. NIST risk management framework breaks this down into different actionable points and help users and developers on how manage risks. Defining clear factors to look at and practical guidelines on how to manage risk would aid AI developers and users to comply with the regulation and develop AI systems that are lawful and trustworthy. This is particularly important for fields such those of Law Enforcement and Criminal Justice that are particularly sensitive. Therefore, it is important for European institution to develop a clear European perspective on AI risk management.

[30] https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

[31] https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

[32] https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

[33] https://www.nist.gov/news-events/news/2022/08/nist-seeks-comments-ai-risk-management-framework-guidance-workshop-date-set

[34] https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf

In 2020, the White house set out 10 key principles to regulatory and non-regulatory approaches on AI[35] (Table 2).

Differently from the EU ethical principles for trustworthy AI, the 10 principles set to guide AI regulations stress the importance of public participation during the rule making process. To this end, in 2018 the EU Commission established the European AI alliance to have a open policy dialogue on AI with citizens, civil societies, business and consumers, trade unions, academia among others. However, the Expert Group on Artificial Intelligence in the domain of Home Affairs that assist the Directorate-General for Migration and Home Affairs in preparing AI related legislation is composed only by member states authorities and public entities with no civil societies. As section 3.3 shows, civil societies are playing a vital role in flagging to DPAs AI systems that function against civil rights. Having them not involved let citizens wonder how controversial systems will be treated and how risks for fundamental rights will be protected, which undermines trust.

Furthermore, the US principles emphasize interagency cooperation. To aid an efficient and effective rule making, EU shall facilitate an active dialogue on AI and Law Enforcement and Criminal Justice between AI stakeholders (public institutions, civil societies, citizens).

In 2021, the national AI Initiative Act of 2020[36] became law with the goal of ensuring US AI leadership in research and development of trustworthy AI as well as on preparing society for the integration of AI systems. With the national AI Act the National AI Initiative Office (NAIIO) was created to oversee and implement the AI strategy and the National AI Advisory Committee (NAIAC) was established to advise on topics related to the National AI Initiative. In May 2022, NAIAC announced the creation of its subcommittee on Law enforcement (NAIAC-LE) to provide advice to the President on topics that include bias, security of data, the adoptability of AI for security or law enforcement, and legal standards that include those that ensure that AI use is consistent with privacy rights, civil rights and civil liberties, and disability rights. As this report is being written, members of NAIAC-LE are being defined.

Similarly, the High Level Expert Group on Artificial Intelligence shall follow up with the creation of a subgroup with expertise on Law Enforcement. AI systems are socio-technical, meaning that their impact depends largely on the way the AI system is used in a specific environment and context. AI applications used in the security domain for law enforcement and judiciary purposes have very specific and contextual risks and consequences that need targeted attention and study.

[35] https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf
[36] https://www.congrss.gov/bill/116th-congress/house/bill/6216

Establish public trust in AI	Government regulatory and non-regulatory approaches should contribute to public trust by promoting reliable AI applications
Public participation	The Government should encourage public participation in all stage of the rulemaking process and public awareness of AI standards and technology
Scientific integrity and information quality	regulations of AI systems should be based on scientific and technical information
Risk assessment and management	regulations of AI systems should use a risk based approach
Benefits and costs	regulations on the development and deployment of AI systems should consider societal costs, benefits and distributional effects
Flexibility	regulations of AI systems should be flexible
Fairness and non-discrimination	agencies need to consider discrimination risks
Disclosure and transparency	Guarantee context specific levels of transparency to allow the understanding of experts and non-experts
Safety and security	Agencies should promote AI systems that are safe and operate as intended
Interagency coordination	Government should promote interagency coordination for a coherent approach on AI.

Table 2: The 10 principles (US) that guide regulatory and non-regulatory approaches.

In addition, to oversee the development of AI in the United States at the federal level, **Executive Order 14007**[37] established the **President's Council of Advisors on Science and Technology (PCAST).** PCAST is an independent federal advisory committee composed by members from industry, academia, and non-profit organizations and charged of making science, technology, and innovation policy recommendations to the President and the White House.

At a federal level, there are also a couple of pending regulation. The first is the **Algorithmic Accountability Act of 2022**[38], which has not passed yet and would require companies that use and sell automatic decision systems new transparency requirements and to conduct impact assessment for bias and effectiveness among others.

[37] https://www.federalregister.gov/documents/2021/02/01/2021-02176/presidents-council-of-advisors-on-science-and-technology

[38] https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202022%20Bill%20Text.pdf

Another pending bill is the **Ethical Use of Facial Recognition Act**[39] which would prohibit any officer, employee, or contractor of a federal agency from engaging in specified activities with respect to facial recognition technology without a warrant until a congressional commission -established by this bill-recommends rules governing the use and limitations on both government and commercial use of such technology. Specifically, it would prohibit setting up a camera to be used in connection with facial recognition technology, accessing or using information obtained from such technology, or importing such technology to identify an individual in the United States until Congress enacts legislation implementing the guidelines established by the commission. Furthermore, **the Facial Recognition Technology Warrant Act**[40] would require federal law enforcement to obtain a court order before using facial recognition technology to conduct targeted ongoing public surveillance of an individual. The **Federal Police Camera and Accountability Act**[41] is also at a proposal stage and would require federal law enforcement officers to wear body cameras and install cameras in patrol cars not equipped with facial recognition technologies or other biometric surveillance. Another bill[42] under consideration would prohibit a federal agency from applying facial recognition technology to any photo identification issued by a state or the federal government or any other photograph in the possession of a state or the federal government unless the agency has obtained a federal court order determining that there is probable cause for the application of such technology.

When considering the laws proposed at a Federal Level there is a key difference to the European approach: US federal proposed regulations tend to be functionality specific and context specific (e.g LEAs)

The above represents the main instruments that have been issued to date regarding the regulation of AI. There is no regulation at the federal level that can be compared to the proposed AI Act of the European Union. This indicates that the federal approach to AI governance is radically different to the EU approach.

2.4.3 State laws

On the other hand, it is important to consider that several states have promoted and enacted a series of regulatory instruments aimed at regulating AI in security. Some of them are limited and others cover much broader issues in this area. The following are the most relevant regulatory instruments grouped by state:

1. **Alabama:** Alabama has implemented, by rule, the establishment of the Alabama Council on Advanced Technology and Artificial Intelligence to develop and advise the governor, local congress and other interested parties on the use and development of artificial intelligence-focused technologies in the state[43]. Furthermore, in 2022 Alabama passed a new law[44] that prohibits the results of AI or a facial recognition technology from being the sole basis for making an arrest or for establishing probable cause in a criminal investigation. When LEAs seek to establish probable cause, the bill only permits

[39] https://www.congress.gov/bill/116th-congress/senate-bill/3284#:~:text=This%20bill%20prohibits%20any%20officer,limitations%20on%20both%20government%20and

[40] https://www.coons.senate.gov/imo/media/doc/FRTWA%20One-Pager%20FinalFinal.pdf

[41] https://www.congress.gov/bill/117th-congress/house-bill/1163/text

[42] https://www.congress.gov/bill/116th-congress/house-bill/4021#:~:text=This%20bill%20prohibits%20a%20federal,determining%20that%20there%20is%20probable

[43] https://www.bamapolitics.com/alabama/bills/2021-alabama-legislative-regular-session/2021-alabama-senate-bills/sb78-alabama-2021-session/

[44] http://alisondb.legislature.state.al.us/ALISON_LCC/SESSBillStatusResult.ASPX?BILL=SB56&WIN_TYPE=BillResult

LEAs to use Facial Recognition (FR) technology match results in conjunction with other lawfully obtained information and evidence. The bill also prohibits state or local LEAs from using AI or facial recognition to engage in ongoing surveillance except for in certain circumstances and to use AI to identify someone based on other images.

Art. 11 (LED) prohibits to make decisions based solely on automated processing, including profiling when they produce a legal effect on individuals, unless authorised by a Union Member state law. The AI Act does not provide any further direction in regards to using AI produced output as a sole basis for arrest or for establishing a cause in criminal investigation. This needs to be addressed by EU policymakers, as evidences coming from the US show how individuals have been wrongfully arrested on the basis of faulty FR technologies (e.g. Johnson, 2022).

2. **California:** in 2019 California passed a three year[45] ban on state and local law enforcement from using body cameras with facial recognition or other biometric surveillance software over fears that facial recognition would disproportionately affect civil rights and civil liberties of people living in highly policed communities. More specifically, the legislation prohibits officers from running facial recognition in real time or after an event on footage collected by body cameras. On the other hand, the law allows LEAs to use biometric software to blur faces in videos disclosed to the public, in order to protect individual's privacy. The prohibition will expire in January 2023. Some interesting local cases in California are the city of Santa Cruz, Davis and Los Angeles. Santa Cruz in 2020 was the first city to unanimously ban municipal use of predicting policing for fears that this technology would perpetuate racial inequality. Santa Cruz was one of the first cities in the country to experiment predictive policing technologies and adopted a predictive policing program[46] in 2011. Davis in 2018 passed an ordinance[47] that required police departments, before buying surveillance technologies, to demonstrate that its benefits outweigh any harm to civil liberties. The city of Davis stated that decisions about the use of surveillance technologies must be balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties. Furthermore, it highlighted the importance to have an informed public debate about surveillance technologies to enhance transparency, accountability, and oversight. Los Angeles in 2017 approved public oversight of the police drone program[48] and the same year, the oversight commission rejected the proposed use of drones.

In order to develop public trust, it is crucial to demonstrate to the public that the benefits of using specific AI applications outweighs harms to civil liberties and translate into positive change for policing activities .

[45] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

[46] https://www.cityofsantacruz.com/government/city-departments/city-manager/community-relations/city-annual-report/march-2012-newsletter/predictive-policing

[47] https://library.qcode.us/lib/davis_ca/pub/municipal_code/item/chapter_26-article_26_07-26_07_010

[48] https://www.courthousenews.com/la-county-commits-to-oversight-of-sheriffs-drones/

3. Colorado: this state has passed a law[49] prohibiting insurance companies from using any external consumer data and information sources, as well as any algorithms or predictive models that use external consumer data and information sources in a manner that unfairly discriminates based on race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity or gender expression. There is also a bill[50] recently enacted that:

1. creates a task force to study issues related to facial recognition,
2. requires state and local agencies that use or intend to use a facial recognition to file a notice of intent and produce an accountability report. Agencies using FR technologies for decisions that produce legal effects must also ensure that those decisions are subject to meaningful human review. Furthermore, agencies using facial recognition would need periodic training of individuals and must maintain records sufficient to facilitate public reporting and auditing of compliance with FR systems policies.
3. restricts LEA's use of FR. It prohibits LEAs from using facial recognition to conduct ongoing surveillance, real-time identification, or persistent tracking unless the LEA obtains a warrant, and LEAs may not apply facial recognition to an individual based on protected characteristics.
4. requires agencies to disclose their use of facial recognition on a criminal defendant to that defendant in a timely manner prior to trial.
5. prohibits the use of facial recognition services by any public school, charter school, or institute charter school.

4. Illinois: This state has introduced an amendment[51] to the Artificial Intelligence Video Interviewing Act, to provide that employers who rely solely on artificial intelligence to determine whether an applicant will qualify for an in-person interview must collect and report certain demographic information to the Department of Commerce and Economic Opportunity, requires the Department to analyze the data and report to the Governor and General Assembly whether the data discloses a racial bias in the use of artificial intelligence. Illinois has created[52] the Future of Work Task Force to identify and assess the new and emerging technologies, including artificial intelligence, that impact employment, wages, and skill requirements.

This law is not specific to Law Enforcement but it is relevant to avoid discriminatory practices also in law enforcement as it suggests to report demographic information and analyze it to spot bias. For High risk AI applications, the AI Act requires to report in the technical documentation accuracy levels for specific groups or persons on which the system is intended to be used (Annex IV) Information about the performance in regards to the groups or persons on which the system is going to be used should be also contained in the instructions (Art.13).

[49] https://www.leg.colorado.gov/sites/default/files/2021a_169_signed.pdf

[50] https://leg.colorado.gov/bills/sb22-113

[51] https://custom.statenet.com/public/resources.cgi?id=ID:bill:IL2021000H53&ciq=ncsl&client_md=cf812e17e7ae023eba694938c9628eea&mode=current_text

[52] https://www.ilga.gov/legislation/BillStatus.asp?DocNum=2481&GAID=16&DocTypeID=SB&SessionID=110&GA=102

5. **Maine** in 2021 has prohibited[53] governmental use of facial recognition, especially in specifically outlined situations with exceptions if police have probable cause that an unidentified person in an image committed a serious crime, or for proactive fraud prevention. Maine police does not have access to Facial Recognition and is able to ask to FBI and Maine Bureau of Motor Vehicles (BMV) to run these searches. The law blocked loopholes that police previously used to access FR technologies through third agencies. The law also requires to create and keep the public record of logs of all FR searches by Maine Bureau of Motor Vehicles.

6. **Maryland** has a pending bill that would authorise LEAs to use real time digital spotters (a system that use AI to assess and transmit an image of a potential violation to a law enforcement office) to detect and enforce vehicle laws governing speeding, the use of wireless communications devices, and the use of seat belts. It would require a law enforcement agency to ensure that certain images captured by a real–time digital spotter are deleted or destroyed; and to develop and implement policies for the shielding of certain information captured by a real–time digital spotter. There has been an attempt to prohibit certain units of State and local government from using a facial recognition service or any information derived from a facial recognition service in the State but the bill[54] failed. Maryland has also a pending bill that aims to create a Facial recognition and Privacy Protection task[55] force.

7. **Massachusetts:** this State has several rules related to security and user privacy and some of them focused on the field of artificial intelligence. These regulations have not been approved yet and they focus on the establishment of a commission on automated decision making by the administration[56]; and the privacy of data in the field of artificial intelligence[57]. The latter requires impact assessments and audits of high-risk automated decision systems to advance fair and just data practices and data aggregators not to use facial recognition technology; or not to collect, use or share any personal data obtained from facial recognition technology.

Massachussets requires an ex ante impact assessments and ex posts outcome audits of high risk practices. The AI Act, requires the Conformity Assessment to be performed prior to placing the high risk system into the market, or prior to its first use in the EU territory and require an additional conformity assessment if the system has undergone through substantial modifications.

7. **Michigan** required an audit[58] of computer system algorithms and logic formulas used by the unemployment security agency.

[53] http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=2&snum=130

[54] https://www.billtrack50.com/BillDetail/1192175

[55] https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0587?ys=2021RS

[56] https://malegislature.gov/Bills/192/SD457

[57] https://custom.statenet.com/public/resources.cgi?id=ID:bill:MA2021000H136&ciq=ncsl&client_md=9d921a7cf50f89a29dd65c32e1507654&mode=current_text

[58] https://custom.statenet.com/public/resources.cgi?id=ID:bill:MI2021000H4439&ciq=ncsl&client_md=d49decc1dc67701c838976e3218c95f3&mode=current_text

8. North Carolina has a bill[59] pending on requiring body worn camera recording to be searched by AI powered technologies. It requires to keep analytics for at least 90 days after which the analytics can be used for training. Directing all law enforcement agencies in the state which use body-worn cameras to, by January 1, 2024, implement a natural language processing technology review protocol that can identify flags and do the following: a. Transcribe and make searchable recording audio, b. Use machine learning or similar technology to create daily, weekly, monthly, and annual reports of analytics for each officer and law enforcement agency that must be reviewed by agency managers, and c. Send automatic alerts to law enforcement agency management.

9. New York in 2020 adopted a law [60] that introduced a moratorium on the use of facial recognition in schools.

10. New Jersey: this State has a bill pending that establishes a prohibition on certain discriminatory acts based on automated decision systems.[61] Specifically, the Act provides that it is unlawful discrimination and a violation of the law against discrimination for an automated decision system to discriminate against any person or group of persons who are members of a protected class in: 1) the granting, retention, extension, modification, renewal or purchase, or in fixing the rates, terms, conditions or provisions of any loan, extension of credit or financial assistance; 2) refusing to insure or continue to insure, limiting the amount, scope or type of insurance coverage, or charging a different rate for the same insurance coverage provided to persons who are not members of the protected class; or 3) the provision of health care services.

11. Virginia in 2021 passed a law that banned the use of facial recognition, barring local and campus police from purchasing or using the technology unless authorized by the legislature. However, early in 2022 the ban was lifted[62] and passed a legislation that allows LEAs to use the FR in certain circumstances, including for the identification of individuals when they have a reasonable suspicion that the person committed a crime. It also allows to use FR to identify crime victims, sex trafficking victims and unidentified bodies. The bill requires FR technologies to be evaluated by NIST as part of the NIST Face Recognition Vendor Test and to have an accuracy score of at least 98 percent true positives across all demographic groups. It requires all approved vendors to annually provide independent assessments and benchmarks offered by NIST to confirm continued compliance. It directs the Department of State Police to develop a model policy regarding the investigative uses of FR technology, including training requirements and protocols for handling requests for assistance in the use of facial recognition technology made to the Department of State Police by local law-enforcement agencies and campus police departments. It requires local law-enforcement agencies or campus police departments that use facial recognition technology to either adopt the Department of State Police model policy or develop an individual policy that meets or exceeds the standards set by the Department of State Police model policy. The bill directs local law-enforcement agencies, campus police departments, and the Department of State Police to collect and maintain certain data related to the use of facial

[59] https://www.billtrack50.com/BillDetail/1372463

[60] https://www.nysenate.gov/legislation/bills/2019/a6787

[61] https://legiscan.com/NJ/bill/S1943/2020

[62] https://lis.virginia.gov/cgi-bin/legp604.exe?221+sum+SB741

recognition technology and to publish an annual report to provide information to the public regarding the agency's use of facial recognition technology. The bill clarifies that any match made through facial recognition technology shall not be used in an affidavit to establish probable cause for the purposes of a search or arrest warrant.

12. **Vermont** has three major regulatory projects on artificial intelligence. The first is focused on the development, use and acquisition by the State of automated decision systems[63] and it tasks the Secretary of Digital Services to create an inventory of all automated decision systems that are used, developed or procured by the state, listing all the features that the inventory should include. On the other hand, a rule has also been developed that establishes the creation of the advisory committee[64]. The duties of the committee would include the creation of anti-bias standards for any software used by the State of Vermont. The last proposes to establish the Artificial Intelligence advisory council [65] to provide advice and counsel to the Director of the Division of Artificial Intelligence with regard to the Division's responsibilities to review all aspects of artificial intelligence systems developed, employed, or procured in State government. The regulations are currently under discussion pending final approval by the local congress.

12. **Washington:** This state has a proposed rule[66] establishing guidelines for public procurement and the use of automated decision systems to protect consumers, improve transparency and create more predictability in the marketplace. The law prohibits public agencies to 1) develop procure or use automatic decision systems that discriminate; 2) install or commission the operation of AI powered systems used for profiling in public spaces. On the other hand, it would allow to use automated decision systems by public agencies only under prior completion of an algorithmic accountability report. This law is still in the process of final approval by the local Congress. In 2020 this state passed a law[67] establishing safeguards for the use of facial recognition by state and local governmental agencies. The law requires any state or local government agency intending to use a facial recognition service to file a notice of intent for the service and specify a purpose for which the technology will be used. It also requires the production of an accountability report.

The following sections discuss the data laws for each principle of the taxonomy.

[63] https://custom.statenet.com/public/resources.cgi?id=ID:bill:VT2021000H263&ciq=ncsl&client_md=7fcb043c609beb468b49a53ca7e6dee1&mode=current_text

[64] https://custom.statenet.com/public/resources.cgi?id=ID:bill:VT2021000H429&ciq=ncsl&client_md=f50a9f7903cf3652c5d6123b01b3f90a&mode=current_text

[65] https://custom.statenet.com/public/resources.cgi?id=ID:bill:VT2021000H410&ciq=ncsl&client_md=d9744d8eb4dbb213bebb222c496a20a6&mode=current_text

[66] https://custom.statenet.com/public/resources.cgi?id=ID:bill:WA2021000S5116&ciq=ncsl&client_md=7812d7f0c1cbfb1e190a742851078fdc&mode=current_text

[67] https://app.leg.wa.gov/billsummary?BillNumber=6280&Year=2019&Initiative=false

2.4.4 Lawfulness

The AI Act poses requirements for high risk AI systems to facilitate the development and deployment of lawful AI applications. However, contrary to EU data law (e.g. Art. 8 LED "lawfulness of processing"), the AI Act does not contain any article specifying the principle of lawfulness for AI systems.

Further practical specifications of the principle of lawfulness in relationship to AI might be needed to protect citizens from risks and misuses of AI.

2.4.5 Accuracy

A model can be considered accurate when it correctly captures a relationship that exists in the training data (NIST, 2021) and is not defined in the AI Act. In Machine Learning, accuracy can be assessed through various metrics: considering true positive, true negatives, false positives and false negatives, F1 score, Mean absolute Error, Logarithmic Loss among others. The accuracy of the model can also be assessed through overfitting (good performance on the training data and poor performance to other data) and underfitting (poor performance on the training data and poor generalisation to other data).

- In the AI Act, accuracy is a requirement for high risk AI systems and the technical documentation that shall be provided before the high risk system is put on the market (Art. 11) needs to contain the metrics used to measure accuracy and the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose (Annex IX). Furthermore, levels of accuracy need to be indicated also in the instructions of use (Article 15).
- The AI Act does not indicate any specific test or threshold of accuracy to be met for AI applications, undermining a meaningful protection of people rights to security and non-discrimination. This is important as several studies found that for example, recognition applications are less accurate for darker skinned women than for white men (see Groether et al. 2019). When used by LEAs, these inaccuracies could lead to false accusations and wrongful arrests (see Hill, 2020). To address this, Virgina law requires facial recognition technologies used by LEAs to be evaluated by NIST as part of the NIST Face Recognition Vendor Test and have an accuracy score of at least 98 percent true positives across all demographic groups. Furthermore, it requires all approved vendors to annually provide independent assessments and benchmarks offered by NIST to confirm continued compliance.

To address accuracy, adopting a functionality-oriented approach with specific EU benchmarks shall prevent risks and violation of rights related to AI systems inaccuracies.

2.4.6 Technical Robustness and safety

According to NIST (2021) a model is robust if it applies to multiple settings beyond which it was trained. The EU ethical principles for trustworthy AI list technical robustness and safety as key requirements for trustworthy AI. Robustness is also a key requirement for high-risk systems in the AI Act. AI systems should be resilient against risks connected to the limitations of the system (e.g. errors, inconsistencies, unexpected situations) as well as against malicious actions that can compromise the security of the AI system and result in harmful or undesirable behaviour (Recital 50). Failure to protect against these risks can lead to negatively impact fundamental rights due to, for example, erroneous decisions or biased output. According to Art 15, Robustness can be achieved through technical redundancy solutions, including backup or fail-safe plans.

Regulatory documents are vague when defining AI technical robustness and potential solutions to it both in the EU and US. Considerations about technical robustness of AI systems shall be included in guidelines helping to define risk managment strategies in this regard.

2.4.7 Risk management

For high risk systems, the AI Act requires to establish, implement, document and maintain a risk management system (Art. 9). The risk management system consists of an iterative process through the lifecycle of the AI system that needs to comprise:

- identification and analysis of the foreseeable risk of the AI system
- estimation and evaluation of the risk that might emerge when the high-risk AI system is used in accordance to its purpose
- evaluation of other possible arising risks
- adoption of suitable risk management measures.

However, risk is a complex concept. In this regard, NIST[68] indicates that AI systems involve different sources of risks in the AI lifecycle regarding the technical design, socio-technical characteristics and also guiding principles about AI. These risks can affect people and their liberties at different levels: individual, group and societal; organizational or at the level of enterprises or systems[69]. Furthermore, AI risks and impact are not well defined and yet difficult to measure. Thus, the risk management obligation might fail to address the risks without effective risk management guidelines.

To foster an effective risk management, EU institutions need to develop guidelines with indications on types of AI risks related to security and risk management strategies.

2.4.8 Purpose limitation

The AI Act does not refer explicitly to purpose limitation but to "intended purpose". In the AI Act, intended purpose means the use for which the AI system is intended by the provider, including the context and conditions of use as specified in the information supplied by the provider in the instructions, promotional materials and technical documentation (Art 3(12)). The intended purpose is key to classify a system as high risk (Art. 7), for managing risks (Art. 9), and it is a piece of information to include in the instructions for users as set by the transparency requirements (Art. 13). If the intended purpose is modified, systems need to undergo through the obligations detailed in Art.16 another time.

[68] https://www.nist.gov/system/files/documents/2021/10/15/taxonomy_AI_risks.pdf
[69] https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pfd

2.4.9 Accountability

According to the OECD AI principles, AI actors should be accountable for the proper functioning of AI systems[70]. The AI Act (Art.17) provides that an accountability framework should be set to specify the responsibilities of the management and other stuff with regard to the aspects listed in Art.17. Colorado SB22-113[71] asks for an accountability report from agencies using, intending to develop, procure or use a facial recognition service. This law provides that the accountability report should include information about the vendor and software, capabilities and limitations, type of data inputs that the FR technology uses, the type of data the facial recognition service generates, how data is processed, the purpose of the FR service, benefits provided by using the service with evidences supporting them, a clear use of the data management policy including when, how and by whom the FR technology will be used factors that determine its use, the measurement taken to minimize the collection of data, data integrity and retention policies, the processes required before the FR use, how data will be stored, agency training procedure, policies governing the service, false rate matches and impact on subpopulations and how error rates are addressed, a description of the impacts of the FR service on civil liberties and human rights, the agency procedure for receiving feedback from the people affected by the use of the FR technology as well as the procedure to respond to feedback. The law provides a periodic training of agencies using FR software or their products and outlines some points that the training must include (e.g. capabilities and limitation, procedures for interpretation). Furthermore, the law requires to allow the accountability report for public review, leave a comment period and hold at least three public meetings. Similar requirements were also proposed by a Vermont law that failed. This law tasked the Secretary of Digital Services[72] to review and build an inventory of all ADMs developed by state agencies containing specific information about system accountability. Much of the requirements corresponded to what the AI Act asks to provide in the technical documentation. Similarly to Vermont, Article 60 of the AI Act requires the creation of a public EU database where providers of AI systems should register the High-risk system for transparency and public oversight.

> To increase transparency and accountability, EU institutions shall set up appropriate platforms that ease the public and civil societies to provide feedback on the use of specific AI applications in the security domain.

Additionally, Colorado SB22-113 requires specifying the training procedures and how the agencies ensure the personnel who operate the FR service [...] are knowledgeable about it and able to ensure compliance. The lack of training has already emerged as an issue in recent DPA decisions (see section 3.3) and while the AI act touches on training (Art. 9(c)) it does not define any transparency requirement or test that prove that users are aware of how the system works.

> To foster LEAs accountability and facilitate the risk management, more specific standards and guidelines on the accountability framework as well as LEA's training shall be provided.

[70] https://oecd.ai/en/dashboards/ai-principles/P9

[71] https://leg.colorado.gov/bills/sb22-113

[72] https://custom.statenet.com/public/resources.cgi?id=ID:bill:VT2021000H263&ciq=ncsl&client_md=7fcb043c609beb468b49a53ca7e6dee1&mode=current_text

2.4.10 Human agency and oversight

Interpretability of the AI system is vital to guarantee explainability, human agency and oversight. Art.13(2) of the AI act states that High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct, and clear information that is relevant, accessible and comprehensible to users. Article 14 states that High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use. Human oversight must be identified or provided into the high-risk system before placing it in the market (Art.14). Oversight mechanisms for high-risk system need to include: capacity and limitations of AI systems, users' awareness of the automation bias, be able to interrupt the AI system processing, be able to interpret the AI system. Beyond requirements for providers to set up clear instructions and interfaces that facilitate human-machine interaction, to ensure efficacy in human oversight periodical training of users is also important (Art. 9(c)) and has been shown to be an issue this far (Akhgar,2022).

2.4.11 Transparency

Transparency obligations attempt to combat AI opacity and are often perceived in conflict with the right to protection to intellectual property and trade secrets. In this regard, the Breyer v. Research Executive Agency (REA) case discussed in section 3.2 where the General Court of the EU held that that public interest exists only once innovation and research are completed, failed to acknowledge the importance of ensuring transparency during technological development of publicly funded projects in domains that are highly sensitive. The transparency requirements set by the AI Act are focused on users to the end of easing interpretation. Article 1(c) provides that the regulation lays down harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content. Article 13 provides that High risk AI systems need to be designed and developed to ensure that their operation is sufficiently transparent to enable users to interpret the system’s output and use it appropriately. Therefore, transparency standards for High-risk applications regard users and not those who are subjected to the AI systems, which disproportionately increase the power asymmetry and undermines trust. Article 52 specifies that developers should ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system [...]. However, this obligation does not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence. The public EU database enhance transparency toward the public but the information provided is still limited for the purpose of enhancing trust.

To increase public trust, EU institutions shall define some transparency standard toward the public that, as discussed in the previous section, requires evidence that benefits of using AI systems in law enforcement outweigh harms. Transparency on potential human rights impact or technical information about bias of the systems intended are crucial to reassure citizens and enhance trust.

2.4.12 Fairness

AI applications can lead to unfair, biased and discriminatory outcomes. In order to be fair, algorithms need to make predictions that do not favour or discriminate against certain individual or groups. Unlike EU data protection regulation, the concept of fairness is not defined, nor mentioned in the EU AI act. However, there are multiple references to how AI can have discriminatory effects. In this regard, the AI act requires the technical documentation of high-risk systems to indicate potentially discriminatory impacts (Annex IV-g) and detailed information about the monitoring, functioning and control of the AI system in regards to risks of discrimination.

Fairness is a cornerstone of public trust. Future binding and non-binding documents need to build on the concept of fairness and show how to apply EU regulations in practice to different AI applications in the security domain.

The next section will discuss relevant ECtHR, CJEU case law and recent data protection authority decisions.

3 Case Law

3.1 European Court of Human Rights (ECtHR)

Up to date there is no ECtHR case law regarding specifically AI for law enforcement purposes or judiciary purposes. However, the ECtHR has, in several decisions, addressed the question of whether surveillance, automated data processing, and creation of databases for policing purposes is compatible with fundamental rights. In the cases outlined below, the violation of Article 8 and Article 10 of the ECHR has been discussed in regard to the lack of "end-to-end" safeguards to prevent abuse and arbitrariness of data collection, retention and processing.

In the case of Big Brother Watch and Others v. The United Kingdom[73] the European Court of Human rights found that some features of the UK's mass surveillance regime were violating the right of privacy (Article 8, ECHR) and the right to freedom of expression (Article 10 ECHR). The case was raised by organisations and individuals that campaign on issue of civil liberties and journalists' rights and sought to challenge three different systems of mass surveillance adopted by the UK intelligence service: (1) the UK Government’s bulk interception of communications; (2) obtaining communications data from communication service providers; and (3) intelligence sharing between foreign governments. The applicants argued that the nature of their activities meant that their electronic communications and data were likely to have been intercepted by the UK intelligence services or obtained from communications service providers or foreign intelligence. The Court held that a bulk interception regime did not, in itself, violate the ECHR. According to the ECtHR such a regime must be subject to certain end-to-end safeguards, meaning that, at the domestic level, an assessment of proportionality should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent review. The Court found that the UK’s bulk interception regime did not contain sufficient “end-to-end” safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse and as such, it was in violation of the right to privacy and of the right to freedom of expression. In particular, the UK's bulk interception regime was found to be deficient in the following respects: it lacked an independent authorization, there was an absence of independent oversight over the entire process for selecting bearers for interceptions, identifying the selectors and search terms to be used to filter intercepted communications, and the selection of material to be examined by analysts. The Court also found the regime for obtaining data from communications service providers to be incompatible with the ECHR because its use was not limited to combating “serious crime”, it was not subject to prior review by a national authority, and it did not sufficiently protect journalists’ confidential communications. On the other hand, the Court upheld the compatibility of the UK’s intelligence sharing regime with the Convention. Having decided that the practice of bulk interception is compatible with the ECHR principles, the ECtHR limitedly protected article 10 of the ECHR. The court recognised that the interference could have been more serious if the journalistic communications were targeted. Furthermore, it did not find the UK's intelligence sharing practice -which allowed the UK authorities to request to foreign intelligence agencies to collect intercepted communication- to be in violation with the ECHR.

[73] Big Brother Watch and Others v. The United Kingdom App no. 58170/13, 62322/14 and 24960/15 (ECtHR May 2021)

The Catt v The United Kingdom[74] case regards the collection and retention of personal data for policing purposes when the data subject has never been convicted of any crime. In this case, the ECtHR found a violation of a peace activist's right to privacy in relation to personal data that have been collected and retained in an "extremist database" despite the applicant had never been convicted of any offence and his risk of violent crime was remote. The data held included information such his name, address, date of birth, presence at demonstrations and in some cases the description of his appearance. Most of the records related to demonstrations organised by the violent protest group but others related to the applicant’s attendance at political and trade union events. The Court affirmed previous case law which found the broad collection of information to prevent crime and disorder to be lawful and pursue a legitimate purpose. However it held that, in this case, the retention of personal data without scheduled review and beyond established limits was disproportionate and unnecessary. The Court took issue with the domestic courts failure to recognize the sensitive nature of some of the data retained on Catt, namely data revealing his political opinions and affiliations with labor unions, which are subject to greater protections. It also called attention to the “ambiguous” nature of legal framework for the "extremist database" and lack of appropriate safeguards to prevent abuse or arbitrariness. The ruling called for increased safeguards for personal data collected overtly by the police, and upheld laws that protect sensitive data such as that which reveals political opinions, racial or ethnic origin of the data subject, or membership in trade unions from unjustified retention.

In Szabò and Vissy v Hungary[75] the applicants complained that the legislation defining the competence of the Anti-Terorism Task Force ("the TEK") in section 7/E of the Police Act, as amended in 2011, and the National Security Act , and in particular “section 7/E (3) surveillance” of the Police Act, violated Article 8 of the Convention because it was not sufficiently detailed and precise and did not provide sufficient guarantees against abuse and arbitrariness. The TEK was entitled to search and keep under surveillance homes secretly, to check post and parcels, to monitor electronic communications and computer data transmissions and to make recordings of any data acquired through these methods. The Court found that these measures constituted interference by a public authority with the exercise of the applicants’ right to respect for their private life, home and correspondence. The Court concluded that it was a violation of article 8 on the grounds that the surveillance practices were overbroad, no assessments of strict necessity were carried out by the authorising entities and, crucially, there was no judicial supervision of surveillance activities. Whilst the protection of national security was a legitimate aim for the enactment and implementation of surveillance measures, minimum safeguards were required in order to ensure adequate and effective guarantees against abuse. In the absence of such safeguards, surveillance measures were counterproductive, resulting in the perceived threat of unfettered executive power intruding into citizens’ private spheres substituting the terrorist threat.

The M.K v. France[76] case concerned a French national who complained of the fact that his fingerprints had been retained on a database by the French authorities. He had been the subject of two investigations concerning book theft, which ended in one case with his acquittal and in the other with a decision not to prosecute. The court recognised that the interference of Article 8 had been in accordance with the Code of Criminal Procedure and a 1987 decree and pursued the legitimate aim of preventing crime. It reiterated the importance of the protection of personal data especially when data go through automatic processing and are

[74] Catt v. The United Kingdom App no. 43514/15 (ECtHR January 2019)
[75] Szabò and Vissy v Hungary App no. 37138/14 (ECtHR January 2016)
[76] M.K. v. France App no. 19522/09 (ECtHR April 2013)

used for policing purposes. The Court considered that the French court failed to strike a balance between the public and private interest and that retention of the data in question amounted to disproportionate interference with the applicant's right to respect for his private life.

In Gardel v. France[77] the Court upheld that the right to privacy of a person, sentenced to life imprisonment for raping a child, was not violated when his name was put on a sex offenders' list while he was imprisoned. The Court ruled that the law provided for sufficient safeguards to protect the applicant's rights. It provided time limits for which the information was to be kept; the data would be deleted automatically on the expiry of 20 or 30 years, depending of the severity of the rape; the person concerned might ask the prosecutor to delete the data if its retention no longer appeared necessary, and the prosecutor's decision could be appealed against before the court.

3.2 Court of Justice of the European Union (CJEU)

Currently, there are only two EU case laws of the CJEU that deal with the use of AI for law enforcement purposes. The first case concerns the development of new AI based technology for border control and the access to public information (Breyer v. Research Executive Agency). The second case addresses the question of whether the automatic collection and processing of personal data is compatible with the GDPR and fundamental rights (Ligue Des Droits Humains v Conseil Des Ministres).

The Breyer v. Research Executive Agency (REA)[78] case concerns issues of access to public information during the development of a surveillance, AI based, technology. In 2016 REA, in collaboration with a consortium of partners, started a research project funded by the Horizon 2020 framework called "iBorderCrtl: Intelligent Portable System". The project aimed at testing and developing new emotion recognition technologies for border control, including a video lie detector to detect whether people lied to border agents. In 2018, Mr Breyer asked the European Commission to access documents related to the projects pursuing Regulation 1049/2001 regarding public access to European Parliament, Council and Commission documents. REA granted full access to one document, partial access to another one and refused to share other under the Article 4 of the Regulation, regarding the protection of personal data and the commercial interests of the consortium members. The General Court of the EU held that REA did not sufficiently justify its denial of access. It recognised that there was a public interest in the democratic oversight of the development of surveillance and control technologies but suggested that such democratic oversight should begin only after the research was concluded. The court ruled that public interest exists only once innovation and research are completed. According to the Court, harm to commercial interest outweighed the public interest in having the information.

In Ligue Des Droits Humains (LDH) v Conseil Des Ministres, the CJEU emphasized the importance of interpreting EU acts in conformity with primary law as a whole and, with the provisions of the ECHR. It also recognised how the opacity of algorithmic systems used for law enforcement purposes can affect fundamental rights. LDH brought an action before the Cour Constitutionnelle (Constitutional Court, Belgium) for the annulment in full or in part for the Law of 25 December 2016 that transposed into domestic law the PNR Directive, the API directive and Directive 2010/65. According to LDH that law infringed the right to respect for

[77] Gardel v. France App no. 16428/05 (ECtHR January 2009)

[78] Breyer v. Research Executive Agency (REA) case no T-158/19

private life and the right to the protection of personal data guaranteed by the Belgian and EU law. LDH alleged breach of Article 22 of the Constitution, in conjunction with article 23 of the GDPR Articles 7, 8 as well as Article 52(1) of the Charter as well as Article 8 ECHR, and the second, alleging, in the alternative, breach of Article 22 of the Charter, read in conjunction with Article 3(2) TEU and Article 45 of the Charter. LDH submitted that the scope as well as that the concept of "passenger" as defined by the law was too broad, leading to systematic, non-targeted automated processing of the data of all passengers. Further, the PNR Directive provides that the Passenger Information Unit (PIU) may also process PNR data against pre-determined criteria. LDH submitted that the nature and rules of the "pre-screening" methods and the databases against which those data are compared, once transmitted, are not defined in a sufficiently clear manner. In October 2019 the Belgian Constitutional Court referred ten questions to the Court of Justice for a preliminary ruling on, among other things, the validity of the PNR Directive and the compatibility of the Law of 25 December 2016 with EU law. In the answer to Questions 2 to 4 and Question 6, and in regard of Processing PNR data against pre-determined criteria intended to identify persons who may be involved in a terrorist offence or serious crime, the CJEU stated that the definition of pre-determined criteria precludes the use of artificial intelligence in self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria.[79] It specified that the use of such technology would be liable to render redundant the individual review of positive matches and monitoring of lawfulness required by the provisions of the PNR Directive. The Court recognized that due to the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. It stated that in those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter[80]. In its judgment, the CJEU court held to the conclusion that since the interpretation given by the Court to the provisions of the PNR Directive in the light of the fundamental rights guaranteed by Articles 7, 8 and 21 and Article 52(1) of the Charter of Fundamental Rights of the European Union ensured that the directive is consistent with those articles, the examination of the questions referred has revealed nothing capable of affecting the validity of the directive. It pointed out that EU acts must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Member States must therefore ensure that they do not rely on an interpretation of that act that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law. Finally it concluded that the transfer, processing and retention of PNR data provided for by that directive may be regarded as being limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, provided that the powers provided for by that directive are interpreted restrictively[81].

[79] Case C-817/19 Ligue Des Droits Humains v Conseil Des Ministres (CJEU 21 June 2022), para 194.
[80] Case C-817/19 Ligue Des Droits Humains v Conseil Des Ministres (CJEU 21 June 2022), para 195.
[81] Case C-817/19 Ligue Des Droits Humains v Conseil Des Ministres (CJEU 21 June 2022), para 299.

3.3 Data Protection Authorities

This section presents European DPA decisions over the use of AI for policing and other relevant purposes. As the cases outlined below show, European DPAs highlighted several times police's lack of knowledge of the AI system used, training and familiarity with the regulations on data collection and data processing.

a. Belgium

The Belgian Data Protection Authority (APD, Autoritè de Protection des données) imposed[82] a fine of €100,000 to Brussels South Charleroi Airport SA and imposed a reprimand for violations of Articles 30(1)(a) and 30(1)(d) of the GDPR, following an investigation on the use of thermal cameras. The cameras were used to check whether the passengers at Brussels South Charleroi Airport had a temperature of 38 ° Celsius or above. The purpose was to prevent sick travelers from entering the departure hall. The DPA held that the Airport was violating the principles of lawfulness and necessity, purpose limitation, and transparency. It was also failing in its obligations related to information provision, conducting a Data Protection Impact Assessment (DPIA) prior to commencing data processing activities, implementing technical and organisational measures to ensure the security of personal data, Privacy by Design, maintaining records of processing activities, and the independence of the data protection officer (DPO). In addition, the airport lacked a legal basis for processing data related to the temperature of the passengers, which as health data are a special category under the GDPR.

b. Bulgaria

Bulgaria Commission for Personal Data Protection (CPDP) issued a statement that is not strictly related to AI but still interesting for the purpose of the report. The statement issued by CPDP was on the legality of the processing of personal data by the Ministry of Interior during the COVID-19 pandemic[83]. The CPDP emphasized that the Ministry's collection of declarations from citizens passing through checkpoints around Bulgaria was a temporary measure and concerned the data processing of a limited number of people. The Statement highlighted that the legislation on the protection of personal data allows for the possibility of limiting the scope of rights and freedoms of citizens under the conditions of Article 23 of the GDPR and that the Ministry's personal data processing is necessary and proportionate in order to guarantee public health and the prevention of crime.

c. Finland

The Deputy Data Protection Ombudsman issued a statutory reprimand to the National Police Board for illegal processing of special categories of personal data during a facial recognition technology (Clearview AI) trial[84]. Clearview AI is an American based company that offers a facial recognition service and has an enormous database through scraping images from social media like Facebook. Additionally, it ordered the National Police Board to inform the people subjects of the personal data breach as their identity could be determined. It also ordered the National Police Board to request Clearview AI to erase the data transmitted by the police. The illegal processing was performed by the National Bureau of Investigation, a unit specialised in the prevention of child sexual abuse, which in early 2020 decided independently and without the approval of the controller (e.g. the National Police Board) to use Clearview AI to identify potential victims.

[82] Autorité de protection des données 4 April 2022 DOS-2020-04022

[83] Commission for Personal Data Protection 25 March 2020

[84] Deputy Data Protection Ombudsman 20 September 2021 Decision no 3394/ 171/21

The Deputy Data Protection Ombudsman found that the controller's responsibility was not fulfilled in these operations, and the measures taken by the controller had not prevented the unlawful processing of personal data. It would have been the duty of the National Police Board to ensure that police personnel were familiar with regulations and the required procedures. Further, the police did not take into consideration the requirements for processing special categories of personal data. The data processing had also started without being aware of how Clearview AI was processing personal data. The police did not know how long the data would be stored or whether it could be disclosed to third parties.

d. France

The French Data Protection Authority (Commission Nationale Informatique & Libertés; CNIL) ordered Clearview AI to stop collecting and using data of people in the French territory in the absence of a legal basis and to erase the data within two months[85]. After having carried out an investigation, CNIL revealed that Clearview AI was violating two articles of the GDPR. It was unlawfully processing personal data as the collection and processing of biometric data were carried out without a legal basis. It was also failing to take into account the rights of individuals in an effective way, specifically the request to access to their data.

e. Greece

The Hellenic DPA fined Clearview AI for €20 million. The Authority examined a complaint against Clearview AI[86], lodged by the civil non-profit organization "Homo Digitalis". The Hellenic DPA found that the company failed to comply with the principles of lawfulness and transparency (art. 5 paragraphs 1(a) and (2), 6, 9 GDPR) and its obligations under Articles 12, 14, 15 and 27 of the GDPR.The Authority ordered the company to comply, and imposed on Clearview AI a prohibition on the collection and processing of personal data of subjects located in the Greek territory. It also ordered Clearview AI Inc. to delete the personal data of those subjects located in Greece.

In March 2022**,** the Hellenic DPA started an investigation on the supply and use of two systems (YPERION and KENTAYROS) for the reception and accommodation of asylum seekers by the Ministry of Immigration and Asylum[87]. While the Yperion system deals with the reception and identification of people, KENTAYROS uses AI and Behavioural Analytics algorithms to manage security around and inside the facilities. The investigation followed a request submitted by a number of civil rights organisations (e.g. Hellenic League for Human Rights, HIAS Greece, and Homo Digitalis). The Hellenic DPA ordered the Ministry of Immigration and Asylum to inform it immediately about the legal basis for the processing of personal data in the of the YPERION and KENTAYROS systems. Further, it requested to carry out an impact assessment on the effect of the data processing on the protection of personal data as for surveillance and monitoring systems, the impact assessment must be carried out before its operation, but also before its procurement, in order to comply with the principles of data protection by design and by default.

[85] Commission Nationale Informatique & Libertés 1 November 2021 Decision no MED 2021-134

[86] Hellenic DPA 13 July 2022 Decision No. 35/2022

[87] Hellenic DPA 2 March 2022 Protocol No. 563

f. Italy

The Italian data protection agency, the Garante per la Protezione dei Dati Personali, imposed on Foodinho S.R.L., a food delivery application belonging partly to the Spanish group Glovo, a fine of €2.6 million for a series of serious infringements[88], with respect to algorithms used for the management of workers involving the use of artificial intelligence mechanisms and automated decisions. The DPA held that the App violated GDPR principles around transparency and lawfulness of processing and cited illegal algorithmic discrimination against certain employees. Beyond the fine, the Garante ordered Foodinho to bring their processing operations into compliance with the GDPR by specifying the information on processing operation, by conducting a DPIA, by introducing measures to safeguards the data subject's rights, fundamental freedoms and legitimate interests, and by introducing suitable measures to regularly check fairness and accuracy of the results of algorithmic systems, partly in order to ensure that the risk of errors is minimised.

Following several complaints filed by the Italian non-profit organisation Privacy Network, the Garante per la Protezione dei Dati Personali, imposed on Clearview AI[89] a fine of €20 million for having implemented a biometric monitoring on people in the Italian territory. According to the Italian DPA Clearview AI held unlawfully and without an adequate legal basis personal data, including biometric and geolocation data. These data cannot be the legitimate interest of the American company. Furthermore, Clearview AI has breached the basic principles of the GDPR such as those relating to:

- the transparency obligations, by not having adequately informed users.
- the limitation of the purposes of the processing, having used user data for purposes other than those for which had been published online.
- the limitation of conservation, having not established data retention times.

The activity of Clearview AI, therefore, has been deemed to violate the freedoms of the data subjects, including the protection of confidentiality and the right not to be discriminated against (related to art. 5, 6, 9, 14, 15, 16, 17, 21, 22, 35). Furthermore, the Garante per la protezione dei dati ordered the company to delete all data of people residing in Italy and forbid the collection and processing of data through the Cleaview system. Finally, the Garante imposed on Clearview AI to designate a representative in the territory of the European Union who acts as an interlocutor, in addition to or in place of the data controller based in the United States, in order to facilitate the exercise of the rights of people.

Procedure 9703988[25](Italy): in this procedure, the data protection agency sanctions a university for a breach of the GDPR rules for the inappropriate use of facial recognition mechanisms through artificial intelligence systems. Specifically, a penalty of 200,000 is imposed on a university for considering that the university did not implement adequate security measures for the processing of data by this artificial intelligence system and improperly carried out an international transfer of data to the USA.

d. Spain

In this proceeding before the Spanish Data Protection Agency (AEPD), the supermarket chain Mercadona was sanctioned for the use of artificial intelligence mechanisms using biometric technology[90]. Specifically, a penalty

[88] Garante per la Protezione dei Dati 10 June 2021, sanctioning proceeding 9675440

[89] Garante per la Protezione dei Dati 10 February 2022, sanctioning proceeding 9751362

[90] Agencia Española Protecciòn de Datos 5 May 2021 No: PS/00120/2021

of €2.5 million was imposed. The AEPD understands that the processing of data based on facial recognition for identification purposes implemented by Mercadona is prohibited by the provisions of article 9.1, as there is no cause to lift the prohibition among those set out in art. 9.2 of the GDPR, so it is not appropriate to rely on the grounds of lawfulness of art. 6.1 of the same. Thus, the AEPD stated that "automatic identification raises serious concerns both from a legal and ethical point of view, given that it can have unexpected effects on many psychological and sociocultural levels"; therefore, they differentiate "between the identification of a person versus their tracking and tracing, and between selective or mass surveillance."

e. Sweden

The Swedish Authority for Privacy Protection (Integritetsskydds Myndigheten, IMY) found that the Swedish Police Authority processed personal data violating the Swedish Criminal Data Act when using Clearview AI to identify individuals[91]. The Swedish Authority for Privacy Protection launched an investigation against the Police after media reported that the Swedish Police Authority was using the application Clearview AI for facial recognition. The investigation concluded that Cleaview AI has been used by the Police on a number of occasions and without any prior authorisation. IMY concluded that the Police has not fulfilled its obligations as a data controller on a number of factors with regards to the use of Clearview AI. Specifically, the Police has failed to implement sufficient organisational measures to ensure and be able to demonstrate that the processing of personal data in this case has been carried out in compliance with the Swedish Criminal Data Act. When using Clearview AI the Police unlawfully processed biometric data for facial recognition as well as failed to conduct a data protection impact assessment which this case of processing would require. It was the responsibility of the Police to ensure that employees were aware of rules and regulations on how the Police may process personal data. IMY imposesd a fine of SEK 2,500,000 (approximately € 250,000) on the Police Authority for infringements of the Criminal Data Act and ordered the Police to conduct further training and education of its employees in order to avoid any future processing of personal data in breach of data protection rules and regulations. Additionally, it ordered the Police to inform the data subjects, whose data has been disclosed to Clearview AI, when confidentiality rules so allows. Finally, the Police was ordered to ensure, to the extent possible, that any personal data transferred to Clearview AI had been erased.

f. United Kingdom

In May 2022 the UK data watchdog (ICO) fined Clearview AI £7.5m[92] for using mages of people in the UK, and elsewhere, that were collected from the web and social media to create a global online database that could be used for facial recognition. The penality was issued for the infringement of Art. 5 (1)(a), 5 (1)(e) of the GDPR and UK GDPR, the requirements set in Art. 6 of the GDPR and UK GDPR, Art. 9 of the GDPR and UK GDPR, Art. 14 of the GDPR and UK GDPR, Art. 15, 16, 17, 21 22 of the GDPR and UK GDPR and the duty to carry out a DPIA under Art. 5 of GDPR and UK GDPR. It also ordered UK data to be deleted.

f. EU level

In 2019 the European Data Protection Supervisor (EDPS)[93] imposed a temporary ban on the European Asylum Support Office (EASO) project which monitored refugee social media to detect new routes. The EDPS held that the EASO had no legal basis for monitoring refugee routes on social media. It recognised that social media monitoring programs and personal data processing put at stake individual freedoms and rights and involve the

[91] Integritetsskydds Myndigheten 12 February 2021 No: DI-2020-2719

[92] Information Commissioner's Office (ICO) 23 May 2022

[93] European Data Protection Supervisor 12 November 2019 Case 2018-1038

use of personal data against and beyond individuals' reasonable expectations. Furthermore, the EDPS stated that the profiling activities may imply interference of interests or other characteristics which the individual had not actively disclosed, thereby undermining the individual's ability to exercise control over their personal data. The EDPS showed concerns for using data from profiles for different purposes through algorithms as data loses its original context. It stated that the repurposing of data is likely to affect a person's information self-determination, further reducing the control of data subjects over their data and affecting the trust in digital environments and services. The EDP recognised that the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health and democracy.

On January 2022 the EDPS ordered the law enforcement agency Europol to delete data of individuals with no established link to criminal activity[94]. With this order EDPS concluded an inquiry started in 2019 under mounting concerns that Europol data processing activities were going beyond their mandate and breaching the data protection rules -e.g. the principles of purpose limitation, data minimisation, data accuracy, storage limitation, the impact of potential data breaches, location of storage, general management and information security. In September 2020 EDPS admonished Europol for the continued storage of big dataset with no data subject categorisation, putting at risk individuals' fundamental rights. Europol in response put in place some measures but did not comply with the EDPS' requirement to define data retention period for their data processing activities, resulting in a data retention that was longer than necessary. The EDPS deemed that these data processing practices were against the principles of data data minimisation and storage limitation as set by the Europol Regulation. As a consequence, on the 3rd of January 2022 the EDPS imposed a 6-month retention period to filter and to extract the personal data and ordered that datasets older than 6 months that have not undergone this data subject categorisation must be erased. This means that Europol was no longer permitted to retain data about people who have not been linked to a crime or a criminal activity for long periods with no set deadline. The EDPS granted a 12-month period for Europol to comply with the Decision for the datasets already received before this decision was notified to Europol. However, following the EDPS decision, Europol regulation (EU) 2022/991 was amended and rendered ineffective the EDPS decision issued in January 2022. The amendments expanded Europol capacity to exchange personal data with third parties, the use of AI, and the processing of large datasets. The amendments allow to treat the data of individuals with no established link to a criminal in the same way as the personal data of individuals with a link to criminal activity. In June 2022 the EDPS expressed its concerns[95] for the amendments made on Regulation (EU) 2022/991 which entered into force on June 28, 2022. The EDPS expressed its preoccupation for the lack of safeguards for data protection that would supervise Europol new powers and on the legality of the amended regulation as it retrospectively authorise Europol to process large data sets already shared with Europol prior to the entry into force of the amended regulation. The EDPS requested Europol's Management Board to further specify the data protection safeguards in place to effectively limit the impact of Europol intrusive data processing activities on individuals and announced that it expects to be formally consulted in the process. On September 2022, the EDPS requested the CJEU to annul two provisions (Art 74a and 74b[96]) of the amended Europol regulation. These two provisions are the ones that legalise retroactively Europol's practice of

[94] European Data Protection Supervisor 3 January 2022 Cases 2019-0370 & 2021-0699

[95] European Data Protection Supervisor 27 June 2022

[96] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.169.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A169%3ATOC#d1e3940-1-1

processing large amounts of individuals' personal data with no established link to criminal activity. According to the EDPS, " the choice to introduce such amendments undermines the independent exercise of powers by supervisory authorities. The contested provisions establish a worrying precedent with the risk of authorities anticipating possible counter-reactions of the legislator aimed at overriding their supervision activities, depending on political will. Data protection supervisory authorities, in this case the EDPS, could be compelled to consider political preferences or may be subject to undue political pressure in a manner that undermines their independence as enshrined in the EU Charter of Fundamental Rights"[97].

3.4 Key findings

So far, legal decisions on AI tools and systems used for law enforcement have been ruled with references to data related legislations (e.g. GDPR) and human rights principles (e.g. ECHR). The main legal issues raised regarding the use of AI by LEAs are related to the collection, use and processing of personal data as well as the transparency of the technological development phase. In terms of data processing, Courts have only made high level considerations on how the opaqueness of algorithms might further endanger fundamental rights and threat the control that people have over their data. The court rulings reviewed indicate that violations to fundamental rights are recognised when the technology has been used without appropriate safeguards (e.g. independent reviewer, DPIA, authorisation) and without a legitimate purpose. Overall, this court ruling and DPA decisions review suggests that, to protect citizens' rights, strict safeguards, clear guidelines and LEAs training are needed on the specific functionalities of AI tools and how to apply regulations to them. The review of court rulings also indicated that, among all the AI functionalities and applications listed by D2.1, only those related to facial recognition and border control are actively discussed by Data Protection Authorities around Europe. In terms of technology development, the decision taken in Breyer v. Research Executive Agency showed little legal attention to the importance of ensuring transparency during technological development of publicly funded projects, as the Court ruled that democratic oversight should start after the research is concluded. This could actively undermine public trust. Finally, the DPA section demonstrated the primary role that civil societies have in reporting systems that present risks for human rights. In this context, DPA around Europe pointed out in different cases the need of adequate training, awareness of rules and regulations and awareness of how the AI powered technology used works.

[97] https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-takes-legal-action-new-europol-regulation-puts-rule-law-and-edps-independence-under-threat_en

4 Conclusions

The use of AI in the law enforcement and judiciary context is sensitive as it introduces a new technology with scarce transparency and accountability in the relationship between the citizen and the state. Regulations and guidelines that govern with clarity the use of AI in the security domain are needed to enhance safety, public trust and reassure citizens. The regulatory scenario on AI is dawning, with the first US binding efforts being enforced at a local level as early as 2018 and the AIA being actively discussed by European Institutions since 2020. This report taxonomised the European regulatory scenario into three classes: human rights, data and AI. For each class, it specified key areas that regulatory binding and non-binding efforts should address to enhance a safe use of AI tools and public trust. This classification wants to highlight the need of having a unified approach that merges human rights, data and AI principles to address public concerns.

In terms of AI specific legislation, this report showed that the US regulatory scenario is well articulated and nuanced, with a number of national and local regulation aimed specifically at governing or banning specific AI applications (e.g. facial recognition) in the security domain. This contrasts with the dominant view describing the US as largely unregulated. More importantly, the review of DPAs' decisions highlighted the pivotal role of civil societies in monitoring and signaling AI systems that can harm fundamental rights.

The following are the key findings:

- Legal requirements and binding and non-binding tools must be produced on human rights impact assessment of AI applications.
- Transparency on human rights impact of the systems intended to be used by LEAs might help to reassure citizens and enhance trust.
- As LED has been developed in the data field, a specific legal tool that address the use of AI in law enforcement and judiciary context shall be developed, given the high sensitivity of the area and the risks for human rights it poses.
- Institutions shall produce practical and clear guidelines on how to comply with regulations that are both sector (e.g. Law Enforcement) and also application (Facial Recognition, Decision Making, Prediction) specific and that unify the data, human right and AI perspectives.
- To protect citizens, there need to be clarity on the rights of the persons who are subjected to AI.
- EU must develop a perspective on risk management and on clear measurements of performance and quantified standards that AI applications in Law Enforcement need to meet (e.g. Face Recognition Vendor Test) and against which they can be audited. To this end, the EU-US Trade and Technology Council[98] might produce highly beneficial work, given the advanced stage of NIST in developing standards and risk management frameworks.
- In order to develop public trust, it is crucial to demonstrate to citizens that the benefits of using specific AI applications outweighs harms to civil liberties and translate into positive change for policing activities. This shall be incorporated in future binding tools, code of conducts and guidelines.
- To increase transparency and accountability, EU institutions shall facilitate public and civil societies to provide feedback on the use of specific AI applications in the security domain. This requires more transparency on the AI development process and use.

[98] https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council

- To foster LEAs accountability and enhance trust, more specific standards and guidelines on LEA's training on AI and computational thinking shall be provided.
- Civil societies are key to monitor and report systems that present risks for human rights. As such, their work and effort need to be consistently and actively integrated into institutional groups and work.
- The Expert Group on Artificial Intelligence in the domain of Home Affairs that assists the Directorate-General for Migration and Home Affairs in preparing AI related legislation shall include civil societies in its list of members.
- Similarly to NAIAC-LE, the High Level Expert Group on Artificial Intelligence shall follow up with the creation of a specific subgroup on Law Enforcement.

5 References

Akhgar B., Bayerl P.S., Bailey K., Dennis R., Gibson H., Heyes S., Lyle A., Raven A., Sampson F., CENTRIC. Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain. AP4AI Framework Blueprint. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf

Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91). PMLR. Available at: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Browning, M., & Arrigo, B. (2021). Stop and risk: Policing, data, and the digital age of discrimination. *American Journal of Criminal Justice*, *46*(2), 298-316. Available at: https://link.springer.com/article/10.1007/s12103-020-09557-x

Europea Commission (2020). A European approach to artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#:~:text=Through%20the%20Digital%20Europe%20and,course%20of%20the%20digital%20decade.

European Commission (2021). EU to invest over €270 million in security research. Available at: https://rea.ec.europa.eu/news/eu-invest-over-eu270-million-security-research-2021-05-17_en

European Parliament (2022). Artificial Intelligence in a digital age. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html#def_1_36

Hill, Kashmir (2020) Another Arrest, and Jail Time, due to a bad Facial Recognition Match. The New York Times. Available at: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

INTERPOL & UNICRI (2019). Artificial Intelligence and Robotics for Law Enforcement. Available at: https://unicri.it/in_focus/on/interpol_unicri_report_ai

In't Veld S. (2021). Question for written answer E-004974/2021 to the Commission. https://www.europarl.europa.eu/doceo/document/E-9-2021-004974_EN.html

Johasson (2021). Answer given by Ms Johansson on behalf of the European Commission.

https://www.europarl.europa.eu/doceo/document/E-9-2021-004974-ASW_EN.html#ref1

Korner, Kevin (2020) How will the EU become an AI superstar?. Deutsche Bank Research. Available at: https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000505746/%28How%29_will_the_EU_become_an_AI_superstar%3F.PDF?undefined&realload=6/WD3blzhvj~BzIY08A3vEe3Hh2VJYnuzHjRGV~MqT6OxSTJhSbsa1cMa2ptqDC0

Natale, S., & Ballatore, A. (2020). Imagining the thinking machine: Technological myths and the rise of artificial intelligence. *Convergence*, *26*(1), 3-18. https://journals.sagepub.com/doi/full/10.1177/1354856517715164

NIST (2021) Taxonomy of AI risk. Available at: https://www.nist.gov/system/files/documents/2021/10/15/taxonomy_AI_risks.pdf

Patrick Grother, et al., 2019 "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects," National Institute of Standard and Technology, US Department of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Reese, H. (2022). What Happens when police use AI to predict and prevent crime? JSTOR Daily. Available at: https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/

Robinson D. & Koepke L. (2016). Stuck in a Pattern. "Early evidence on predictive policing and civil rights". Upturn. Available at: https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf

World Economic Forum (2016). The Fourth Industrial Revolution: what it means, how to respond. Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

6 Appendix A

FR= Facial Recognition; ADM= Automated Decision Making

Where	Regulation	Class	Functionality
EU	the Charter of Fundamental Rights of the EU	Human RIghts	na
EU	European convention on Human Rights	Human RIghts	na
EU	European social charter	Human RIghts	na
EU	the Employment Equality Directive (2000/78/EC)	Human RIghts	na
EU	the Racial Equality Directive (2000/43/EC)	Human RIghts	na
EU	the Gender Goods and Services Directive (2004/113/ EC)	Human RIghts	na
EU	Gender Equality Directive (2006/54/EC)	Human RIghts	na
EU	Convention 108+	Data	na
EU	Guidelines on the protection of individuals with regards to the processing of personal data in a world of Big Data	Data	na
EU	Directive 2016/679 - GDPR	Data	profiling, ADM
EU	Directive 2016/681 - PNR	Data	na
EU	Directive 2016/680 - LED	Data	profiling, ADM
EU	Directive 2018/1725 EU-DPR	Data	profiling, ADM
EU	2002/58/EC e-Privacy directive	Data	na
EU	Guidelines on artificial intelligence and data protection	AI	General AI
EU	Artificial Intelligence for Europe	AI	General AI
EU	Ethics Guidelines for trustwhorthy AI	AI	General AI
EU	Assessment List for trustworthy AI	AI	General AI
EU	Coordinated Plan on Artificial Intelligence	AI	General AI
EU	Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems	AI	General AI
EU	Artificial Intelligence for Europe	AI	General AI
EU	Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matte	AI	General AI used by LEAs and in Judicial context
EU	European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment	AI	General AI in judicial context
EU	Committee of Ministers - Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes	AI	General AI
EU	Policy and investment recommendations for trustworthy Artificial Intelligence	AI	General AI
EU	Guidelines on the use of facial recognition	AI	FR
EU	Parliamentary Assembly - Recommendation 2102 (2017) Technological convergence, artificial intelligence and human rights	AI	General AI
EU	Accountability principles for artificial intelligence in the Internal security domain	AI	General AI

This project has received funding from the *European Union's Horizon 2020 research and innovation programme* under grant agreement No 101022001.

	AI Act	AI	Risk assessment tools Poliygraph Deep fake detection evaluation reliability of evidence profiling prediction of occurrence & re-occurrence of crime crime analytics verification of authrnticity of documents examination application for asylum or residence AI systems assisting judicial authorities
EU	Building Trust in Human-Centric Artificial Intelligence	AI	General AI
EU	Guidelines on the use of facial recognition technology in the area of law enforcement	AI	FR
EU	National strategies	AI	General AI
Alabama	SB 78: Technology, Alabama Council on Advanced Technology, estab., to advise Governor and Legislature, members, duties	AI	na
Alabama	SB56: Facial recognition technology, use of match as the sole basis of probable cause or arrest, prohibited	AI	FR
California	AB 1215: Law enforcement: facial recognition and other biometric surveillance.	AI	FR
California- Davis	Surveillance Technology Ordinance	AI	Surveillance technologies
California - Santa Cruz	Ordinance no. 2020-17 An Ordinance of the City Council of Santa Cruz	AI	Predictive Policing
Colorado	SB 21-69: Concerning Protecting consumers from unfair discrimination in insurance practices	AI	Predictive Models
Colorado	SB22-113 Concerning the use of personal identifying data	AI	Facial Recogniton
Illinois	IL HB 53 amendment to The Artificial Intelligence Video Interview Act	AI	Data, AI at the workplace
Illinois	SB 2481 Future of Work Task Force	AI	na
Maryland	HB 1082 / SB 863: Vehicle Laws Enforcement and Use of Real Time Digital Spotters	AI	RT Digital Spotters
Maryland	MD SB 857 Facial Racognition Services Moratorium	AI	Facial Recogniton
Maryland	Task Force Facial Recognition and Privacy Protection	AI	Facial Recogniton
Massachussets	MA H.B. 136 An act relative to Data Privacy	AI	ADM
Maine	An Act To Increase Privacy and Security by Regulating the Use of Facial Surveillance	AI	FR
Massachussets	MA S. 60 An act establishing a commission on automated decision making by government in the commonweath	AI	ADM
Michigan	MI H.B 443 Michigan employment security act	AI	na
New Jersey	NJ SB1943 Prohibits certain discrimination by automated decision systems.	AI	ADS
New York	AB 6787D Relates to the use of biometric identifying technology	AI	AI
North Carolina	H 937: Automatic Police Body Cam Analysis	AI	FR Body camera
Virginia	SB 741 Facial recognition technology; authorized uses.	AI	FR
Vermont	VT HB263 Information technology; Agency of Digital Services; Stateprocurement; automated decision system	AI	Automated decision making
Vermont	VT HB 429 proposes to establish an advisory committee to address bias in software programs used by the State.	AI	na
Vermont	VT HB 410 An act relating to the use and oversight of artificial intelligence in State government.	AI	General AI
Federal	Facial Recognition Ban on Body Cameras Act, 117 H.R. 8154	AI	FR
Federal US	Advancing Facial Recognition Technology Act, 117 H.R. 4039	AI	FR
Federal US	Ethical Use of Facial Recognition Act, 116 S. 3284	AI	FR
Federal US	Facial Recognition Technology Warrant Act of 2019	AI	FR
Federal US	Facial, Analysis, Comparison, and Evaluation Protection Act of 2019, 116 H.R. 4021	AI	FR

Federal US	Facial Authorization Cannot be Enforced Act, 117 H.R. 6609	AI	FR
Federal US	Artificial Intelligence Initiative Act	AI	General AI
Federal US	Facial Recognition Technology Warrant Act of 2019, 116 S. 2878	AI	Generai AI
Federal US	Algorithmic Accountability Act	AI	General AI

7 Appendix B

Key documents on AI produced by the CoE, EP and EU Commission.

Who	When	What
CoE- CEPEJ	2019	European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment
CoE-CAHAI	2020	Feasibility study on a legal framework on AI design, development and application based on CoE standards
CoE-CAHAI	2021	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
CoE- Committee of Ministers	2021	Declaration by the Committee of Ministers on the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net
CoE- Committee of Ministers	2021	Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes
CoE-CAHAI	2021	Human Rights, Democracy and Rule of Law Impact Assessment of AI systems
CoE-Committee of Ministers	2020	Recommendation CM/Rec(2020)1 of the Committee of Ministers to member Stateson the human rights impacts of algorithmic systems
CoE	2019	Unboxing Artificial Intelligence: 10 steps to protect Human Rights
CoE-Parliamentary Assembly	2017	Technological convergence, artificial intelligence and human rights
CoE-Committee of Ministers	2021	Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling
CoE	2021	Guidelines on Facial Recognition
CoE	2019	Guidelines on Artificial Intelligence and Data Protection
CoE	2017	Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data
CoE-CEPEJ	2021	Guidelines on electronic court filing (e-filing) and digitalisation of courts
CoE-Committee of Ministers	2021	Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings
CoE-CDCJ	Ongoing	Review of The Administration and You handbook in the light of the use of artificial intelligence (AI) and non-AI algorithmic systems (based on comparative study in member States)
CoE-Committee of Ministers	2021	Declaration by te Committee of Ministers on the risks of Computer Assisted or artificial intelligence enabled decision making in the field of the social safety net
CoE-CAHAI	2020	Towards regulation of AI systems: Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law
CoE	2019	A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework
CoE	2019	Artificial Intelligence and Data Protection: Challenges and Possible Remedies
CoE	2020	Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study
CoE	2020	Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems
CoE	2017	Study on the Human Rights Dimensions of automated data processing techniques and possible regulatory implications
CoE	2019	Artificial Intelligence and Data Protection: Challenges and Possible Remedies
EU Commission	2018	Artificial Intelligence for Europe
EU Commission- AI HLEG	2019	Ethics Guidelines for trustworthy AI
EU Commission- AI HLEG	2020	Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment
EU Commission- AI HLEG	2020	Sectoral Considerations on Policy and Investment Recommendations for Trustworthy AI
EU Commission	2019	Communication: Building Trust on Human Centric Artificial Intelligence
EU Commission	2021	Coordinated plan on Artificial Intelligence 2021 Review
EU Commission	2020	White Paper on Artificial Intelligence: a European approach to excellence and trust
EU Commission	2021	Proposal for a Regulation laying down harmonised rules on artificial intelligence
EU Commission	2020	Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics
EU Commission- AI HLEG	2019	A definition of AII: main capabilities and Disciplines
European Parliament	2021	Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters
European Parliament	2021	Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters
European Parliament	2021	Artificial intelligence: questions of interpretation and application of international law
European Parliament	2022	Artificial intelligence in a digital age
European Parliament	2020	Intellectual property rights for the development of Artificial Intelligence Technologies
European Parliament	2020	Artificial intelligence in education, culture and the audiovisual sector
European Parliament	2020	Civil Liability Regime for Artificial Intelligence
European Parliament	2020	Frameworks of ethical aspects of Artificial Intelligence, robotics and related technologies
European Parliament	2020	Setting up a special committee on Artificial Intelligence in the Digital Age and Defining its responsibilities, numerical strenght and term of office

European Parliament	2020	Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights
European Parliament	2020	The ethics of artificial intelligence: Issues and initiatives
European Parliament	2022	Governing data and artificial intelligence for all: Models for sustainable and just data governance
European Parliament	2022	Europe's PegasusGate: Countering spyware abuse
European Parliament	2021	Biometric Recognition and Behavioural Detection Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces
European Parliament	2021	Artificial intelligence at EU borders: Overview of applications and key issues
European Parliament	2021	Regulating facial recognition in the EU
European Parliament	2022	Auditing the quality of datasets used in algorithmic decision-making systems
European Parliament	2022	Ethical and societal challenges of the approaching technological storm