STUDY

Requested by the LIBE committee

Artificial Intelligence and Law Enforcement

Impact on Fundamental Rights

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 656.295 – July 2020

EN

Artificial Intelligence and Law Enforcement

Impact on Fundamental Rights

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines the impact on fundamental rights of Artificial Intelligence in the field of law enforcement and criminal justice, from a European Union perspective. It presents the applicable legal framework (notably in relation to data protection), and analyses major trends and key policy discussions. The study also considers developments following the Covid-19 outbreak. It argues that the seriousness and scale of challenges may require intervention at EU level, based on the acknowledgement of the area's specificities.

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

AUTHOR
Prof. Dr. Gloria GONZÁLEZ FUSTER, Vrije Universiteit Brussel (VUB)

ADMINISTRATOR RESPONSIBLE
Alessandro DAVOLI

EDITORIAL ASSISTANT
Ginka TSONEVA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in July 2020
© European Union, 2020

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER AND COPYRIGHT

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy

CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
ADM	Automated Decision Making
AI	Artificial Intelligence
CJEU	Court of Justice of the European Union
DAPIX	Working Party on Information Exchange and Data Protection
DPA	Data Protection Authority
EASO	European Asylum Support Office
EC	European Commission
ECHR	European Convention on Human Rights
ECRIS-TCN	European Criminal Records Information System for Third-Country Nationals
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights Initiative
EES	Entry/Exit System
EIO	European Investigation Order
EPIC	Electronic Privacy Information Center
EPPO	European Public Prosecutor’s Office
EU	European Union
FAT	Fairness, Accountability and Transparency
FIU	Financial Intelligence Unit

GDPR	General Data Protection Regulation
GSMA	Global System for Mobile Communications association
GVM	Gangs Violence Matrix
ICO	Information Commissioner's Office
IT	Information Technology
JRC	Joint Research Centre
LED	Law Enforcement Directive
LFR	Live Facial Recognition
OECD	Organisation for Economic Co-operation and Development
PNR	Passenger Name Record
RBI	Remote Biometric Identification
SIS	Schengen Information System
UNICRI	United Nations Interregional Crime and Justice Research Institute
VIS	Visa Information System

LIST OF BOXES

LIST OF FIGURES

EXECUTIVE SUMMARY

Background

Artificial Intelligence (AI) is high on the agenda of the European Union (EU). Discussions on its possible regulation have been particularly prominent since Ursula von der Leyen announced, already before her nomination as President of the European Commission (EC), a strong will to situate AI among the Commission's top priorities. The endorsement of AI as an EU-level policy priority has been accompanied by a reflection on how to promote trust in AI technologies, and how to guarantee that AI systems do not compromise, during their development or deployment, EU fundamental rights. This specific reflection is actually not completely novel, but entrenched in prior legal and policy debates on fundamental rights issues connected notably to 'big data', as well as, more generally, related to the regulation of the processing of both personal and non-personal data.

Aim

This study aims at analysing the **impact on EU fundamental rights of AI in the field of law enforcement and criminal justice**. It approaches the subject from an EU law and policy perspective. It first succinctly presents the main features of the applicable legal framework. Second, it introduces recent and ongoing developments in the field, focusing on 'predictive policing', facial recognition, the use of AI in criminal justice, and AI and borders. It discusses the impact on fundamental rights of these trends, and reviews relevant policy discussions around AI regulation. After such exploration, the study puts forward some concrete recommendations.

Findings

The field of law enforcement and criminal justice is **particularly sensitive**, as it touches upon core issues of the relation between the individual and the State. There is a broad consensus on the fact that reliance on AI systems in this area can substantially impact EU fundamental rights, and more generally democracy itself. The issue thus deserves special consideration in the context of any discussion on the future of trustworthy AI.

This study:

- Shows that the advent of AI in the field of law enforcement and criminal justice is already a reality, as **AI systems are increasingly being adopted or considered**; such systems might take many different shapes, and occur at the cross-roads of different sustained trends to increase the use of data, algorithms, and computational power; these developments are connected to pre-existing trends, some of which had been previously broadly framed under other notions or policy priorities ('big data');
- Documents that such developments have already generated **significant controversies**, notably in relation to 'predictive policing', facial recognition, AI and criminal justice, and AI and borders (including a reflection on the European Travel Information and Authorization System, ETIAS), for instance in litigation and calls from civil society to better prevent or mitigate associated risks, both in the EU and beyond;
- Points out that discussions around AI regulation in the EU have been deeply embedded in the **EU Digital Single Market agenda**, and that generally speaking, although they might refer to the need to consider law enforcement and criminal justice specificities, such policy discussions are most often not based on a detailed review and taking into account of concrete applicable rules (and, especially, of applicable restrictions and derogations);

- Warns that such policy discussions suffer from **persistent ambivalences on the role of 'ethics'** in relation to the safeguarding of fundamental rights, generating not only lack of conceptual precision but most importantly uncertainty as to whether effective protection of fundamental rights will be delivered;
- Emphasises that **the current EU data protection legal framework shall not be assumed to offer enough solid safeguards for individuals** in light of the increased uses of automated decision-making and profiling for law enforcement and criminal justice purposes, as:
  - the general safeguards provided by the General Data Protection Regulation (GDPR) do not necessarily apply when the processing is for such purposes, as restrictions and derogations might be applicable;
  - the Law Enforcement Data Protection Directive (LED Directive), which might be the applicable relevant instruments, provides for safeguards that are similar to those of the GDPR, but nevertheless not exactly equivalent, and equally provides for possible restrictions and derogations.
- Reviews a variety of fundamental rights considerations connected to AI in the field of law enforcement and criminal justice, illustrating the fact that they include privacy and data protection issues but also other challenges, notably related to **non-discrimination**;
- Describes a **problematic lack of minimum transparency standards in relation to the support of AI research with EU funds**, affecting notably the possibility to assess how funded research complies with the respect of EU fundamental rights and EU law in general, but also further scientific work towards trustworthy AI solutions;
- Cautions that **responses to the Covid-19 outbreak have led to the rapid proliferation of technological measures and data-driven initiatives to be carefully assessed**, including initiatives which have the ambition of sustaining an unprecedented widespread generalised collection of data about individuals ('contact tracing apps'), and initiatives that build on the fragile distinction between 'personal' and 'anonymised' data to facilitate extensive data processing;
- Recommends that due consideration be given to **the need for a legislative intervention to guarantee EU fundamental rights in the field of law enforcement and criminal justice**; that any possible role granted to 'ethics' in such intervention shall be clarified and justified in detail; that the possible gaps and inefficiencies of the EU data protection law, as well as national laws implementing EU data protection law, shall be duly examined specifically in the light of the law enforcement and criminal justice context; that EU-funded AI research must be better framed, and finally, that developments related to the Covid-19 outbreak shall be monitored with extreme attention.

1. GENERAL INFORMATION

KEY FINDINGS

Law enforcement and criminal justice can benefit from AI developments, and there are many AI-related systems and technologies being adopted and developed for law enforcement and criminal justice purposes in the European Union (EU). Some of these solutions, however, raise important questions in terms of their compatibility with EU fundamental rights.

EU-level policy discussions around the regulation of AI have been marked until recently by their strong embedding in the development of the Digital Single Market. In this policy context, the European Commission (EC) is notably advocating embracing the advent of AI while at the same time pursuing the establishment of an 'ecosystem of trust' – trust in AI - as a policy objective in itself. Ethical considerations have been given much attention from this perspective.

The magnitude and seriousness of challenges triggered by AI in the field of law enforcement and criminal justice, however, do not appear to be conveniently addressed by ongoing reflections. In this sense, future steps should notably consider the legal specificities of the area, and most notably the complexities and limitations of the EU data protection legal framework, especially insofar as personal data processing for law enforcement and criminal justice purposes is concerned, and more generally in relation to data processing in the Area of Freedom, Security and Justice (AFSJ).

EU-funded AI research related to law enforcement and criminal justice also deserves further attention. Important investments have already taken place, and more substantial funding is planned, but the framework accompanying the selection of projects and their implementation presents problematic transparency gaps.

The Covid-19 outbreak has led to data-driven and AI solutions being more present than ever, potentially exponentially multiplying the personal data to be eventually available for law enforcement purposes. Whereas fundamental rights safeguards, including data protection safeguards, appear more important now than ever, there have also been cases in which these safeguards appear to be threatened by exceptional measures taken invoking needs related to the crisis. This generates a particularly delicate situation for EU fundamental rights, calling for great vigilance.

Artificial Intelligence (AI) can be of substantial use **in the field of law enforcement and criminal justice**. This idea is broadly accepted and endorsed at European Union (EU) level,[1] and the trend towards using automated processing techniques and algorithms in crime prevention and the criminal justice systems has been described as generally growing for already a number of years (MSI-NET, 2018, 10). AI, however, is also generally perceived as being, at least potentially, in tension with certain **fundamental rights** recognised as such in the EU, and constituting a particularly high risk to such rights when used in the field of law enforcement and criminal justice.

Paradoxically, despite the wide acknowledgement of these tensions, there are relatively limited studies or even policy discussions on the specific needs and challenges of regulation at European Union (EU) level of AI in law enforcement and criminal justice. These possible specific needs and challenges often

[1] *'AI can… help to detect fraud and cybersecurity threats, and enables law enforcement authorities to fight crime more efficiently'* (COM(2019) 168 final, 1).

appear as a concluding thought, if not an afterthought, amidst broader reflections related to the regulation of AI in general. Almost as an exception to this rule, there European Parliament is currently discussing a ***Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters*** (LIBE, 2020/2016(INI)).

At EU level, deliberations on a possible need for an AI regulatory framework have primarily surfaced and been developed until now in a **Digital Single Market** context. This is not without consequences on the nature and substance of the debate, and has notably tended to leave out of the picture the singularity of law enforcement and criminal justice, both regarding the specific risks in the field and the peculiarities of the EU legal framework in the **Area of Freedom, Security and Justice (AFSJ)**.

If EU-level policy debates have only touched upon the challenges of AI in law enforcement and criminal justice in a limited manner, many of these challenges are nevertheless already been visibly surfacing, in an often-contentious mode, in EU territory and globally. This is most probably connected to the fact that law enforcement and criminal justice have a bearing on foundational aspects of the relations between individuals and the State, relations that are thus particularly sensitive to the deep transformations potentially conveyed by AI systems. It might also be, however, that the manner in which certain related technologies have been deployed was not the best suited manner, and that different approaches – and possibly, indeed, a revised regulatory framework – would contribute to mitigate fundamental rights risks, ease critical concerns, and increase trust in these technologies.

The European Commission noted already in 2014 that although digitisation of public services opened up new opportunities to optimise data analysis, the '*reported use of similar technologies for **surveillance purposes**, by public or private actors, is liable to feed concern and **reduce trust** in the digital economy among individuals and organisations*', deserving thus special attention (COM(2014) 442 final, 3). The amplification of widespread surveillance is, precisely, one of the impacts of the advent of AI in certain countries such as the United States and China, according to some observers (AI Now Institute, 2018).

Much has been said about 'the race for AI dominance', or the 'race of AI', typically referring to the capacity of specific actors to take economic advantage of AI developments.[2] In the context of law enforcement and criminal justice, the most important ongoing race might be the one between legislative efforts to appropriately frame and counter the risks triggered by AI, on the one hand, and judicial challenges and other 'bottom up' developments that bring to the fore a variety of fundamental issues that appear to be requiring, if not further protection by the law, at least, urgently, more clarity.[3]

1.1. Objectives and structure

This study aims at critically assessing ongoing developments in relation to **AI in the field of law enforcement and criminal justice**, in order to review their **impact on EU fundamental rights** and, on the basis of such an assessment, put forward policy recommendations. For this, it first briefly introduces the relevant legal framework, and then reviews the main trends and controversies in the area, focusing in particular in 'predictive policing', facial recognition, AI and criminal justice, and AI and border control. It then analyses their impact on EU fundamental rights, before moving to pertinent policy discussions around the regulation of AI, in a section also examining the support of AI in law enforcement and criminal justice through EU funding. The study also introduces some of the main relevant developments that have taken place following the outbreak of the Covid-19 virus. It concludes by putting forward a series of policy recommendations.

[2] See, for instance: Castro, McLaughlin & Chivot, 2019.

[3] In relation to this 'competition' and the regulation of facial recognition, see, for instance: Lynch, 2020.

The notion of AI is here **broadly understood**, in order to offer a wide view of the relevant debates and challenges. Legal and policy discussions often tend to soften the boundaries between certain concomitant notions, and issues which are of interest for the purposes of a discussion of AI in the field of law enforcement and criminal justice have sometimes manifested themselves relying on different terminology (for instance in debates around 'algorithmic discrimination', 'accountable algorithms', 'algorithmic transparency', etc.).

The study does not have the ambition of exhaustively covering all recent and ongoing developments in this area, which are numerous. The EU Agency for Fundamental Rights has, in this sense, compiled a collection of almost 300 policy initiatives in EU Member States and beyond for the period 2016-2020 (EU FRA, April 2020). Researchers working on AI regulation have also stressed the difficulty of having a full overview of the many initiatives concerning the ethical, social and legal aspects of AI (Boddington, 2017, 3).

The study also notably does not cover issues such as the misuse of AI for criminal purposes. When AI is used maliciously (Brundage, 2018), additional challenges for fundamental rights can be triggered.

1.2. Methodology

The study is based on desk-research and the review of existing available data, studies and analyses from sources and documents from EU, national and international institutions, as well as Data Protection Authorities (DPAs), experts, academia, industry, and civil society. It principally encompasses legal instruments and policy documents of EU institutions, bodies and agencies, but also from the Council of Europe. The analysis of EU primary and secondary legislation constitutes an essential part of the research. Various reports have also been used to the extent they are useful to illustrate recent trends and controversies.

2. EU LEGAL FRAMEWORK

Before considering the impact on fundamental rights of AI in the field of law enforcement and criminal justice it is useful to briefly recall which are the applicable standards in the EU. This section succinctly examines the main elements of the relevant **EU legal framework**, touching upon both primary and secondary law.

There are actually **many legal instruments** that might be regarded as directly or indirectly applicable to AI-related developments.[4] For the purposes of this study, special attention shall be given here to EU fundamental rights obligations, but also to rules on data and its free movement, in light of the importance of data as both an enabler and a product of AI solutions.

It is important to remember however that EU law obligations coexist with other fundamental rights and data protection obligations, such as those derived from national legal orders. In addition, Council of Europe instruments also deserve a special mention, most notably the **European Convention on Human Rights** (**ECHR**) and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**'Convention 108'**),[5] which was recently reviewed leading to a modernised version, known as '**Convention 108+**'.[6]

These **Council of Europe** instruments are accompanied by soft-law instruments such as the *Guidelines on Artificial Intelligence and Data protection* published by the Consultative Committee of Convention 108 in 2019.[7] Previously, in 2018, the Consultative Committee of Convention 108 had also adopted *The Practical Guide on the Use of Personal Data in the Police Sector*, offering guidance on how to legally prevent and combat crime, including through the use of personal data (Consultative Committee of Convention 108, 2018). The Guide warns that there are *'considerable risks'* linked to using big data technologies and analysis techniques to assist crime detection, and identifies a series of requirements to which data controllers are advised to *'pay additional attention'* when processing personal data for such purposes, such as special awareness requirements (ibid., 10-11).

2.1. Primary law

As established in Article 2 of the Treaty of the EU, the EU *'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'*. Article 6 of the Treaty of the EU specifies which are the fundamental rights recognised as such by EU law, referring to the future accession to the European Convention on Human Rights (ECHR), the fundamental rights which are part of the general principles of EU law, and the fundamental rights recognised in the **Charter of Fundamental Rights of the EU** – such as human dignity (Article 1), the right to life (Article 2), the right to the integrity of the person (Article 3), the right to liberty and security (Article 6), the right to respect for private and family life (Article 7), the right to the protection of personal data (Article 8), freedom of expression and information (Article 11), freedom of assembly and of association (Article 12), equality before the law (Article 20), non-discrimination

[4] Such as, for instance, EU cybersecurity law (Hamon, Junklewitz & Sánchez, 2020, 4).

[5] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108.

[6] See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223.

[7] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Artificial Intelligence and Data Protection*, T-PD(2019)01.

(Article 21), the rights of the child (Article 24), the right to an effective remedy and to a fair trial (Article 47), and the presumption of innocence and right of defence (Article 48).

All these fundamental rights are applicable also in relation to law enforcement and criminal justice; fundamental rights requirements derived from primary law apply to all areas of EU law. In relation to the right to the protection of personal data of Article 8, it is worth noting that a Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation attached to the Lisbon Treaty observed that '*specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields*'.[8]

2.2. Secondary law

In this section are presented the most salient elements of EU secondary law applying to **the processing of both personal data** and **non-personal data**. The distinction between personal and non-personal data is not deprived of frictions, especially as technological developments – including AI-related developments – might oblige to regard as personal data certain data sets that were not previously regarded as such.

2.2.1. Rules on the processing of personal data

Personal data are defined in EU law as '***any information relating to an identified or identifiable natural person*** *('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'.[9]

The right to personal data protection is currently recognised as an **EU fundamental right** both in the EU Charter of Fundamental Rights (Article 8) and in the Treaties (Article 16 of the Treaty on the Functioning of the EU). This right is currently recognised as an **autonomous fundamental right**, different from the right to the respect for private life, to which it has been historically closely connected in some legal frameworks. This does not mean, however, that such as right does not serve at the same time **other fundamental rights**, including the right to respect for private life. In this sense, EU secondary law giving substance to Article 8 of the EU Charter simultaneously aims at guaranteeing the respect of **all fundamental rights**.[10]

The EU legal framework on data protection is composed of a number of different legal instruments, of which must be mentioned:

- Regulation (EU) 2016/679,[11] or **General Data Protection Regulation** (**GDPR**), named 'general' because it applies 'generally' to the processing of personal data, within the limits of its material

[8] Declaration 21 of the Declarations Annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007.

[9] Article 4(1) of the General Data Protection Regulation (GDPR).

[10] This has practical implications for the interpretation of the GDPR. Its Article 35, for instance, refers to the need to take into account a likely high risk 'to the rights and freedoms of individuals'. This has been interpreted as primarily concerning the rights to data protection and privacy, but as also potentially involving other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion (Art. 29 WP, WP 248 rev.01, 6)

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.

and territorial scope (but does not apply to personal data processing by EU institutions, bodies, offices and agencies);

- Directive (EU) 2016/680,[12] known as the **Law Enforcement Directive** (**LED**), which applies generally to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, but only when these authorities process personal data for such purposes (but does not apply to personal data processing by EU institutions, bodies, offices and agencies);
- Regulation (EU) 2018/1725,[13] or **EU-DPR**, which is generally applicable to the processing of personal data by EU institutions, bodies, offices and agencies, but includes special rules for the processing of 'operational personal data',[14] for instance by Eurojust, and leaves out of its scope Europol and the European Public Prosecutor's Office, pending a possible change in 2022;
- Directive 2002/58/EC,[15] or **e-Privacy Directive,** applying to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.

In addition to such instruments, other legal instruments include particularly important data protection rules applying to specific data processing activities in this field, such as, for instance:

- Regulation (EU) 2016/794,[16] or the **Europol Regulation**, on the EU Agency for Law Enforcement Cooperation (Europol) – regarded as *'a hub for information exchange in the Union'*,[17] which has its own data protection provisions;
- Council Regulation (EU) 2017/1939,[18] of **EPPO Regulation**, on the European Public Prosecutor's Office, which equally has its own data protection provisions;
- Regulation (EU) 2018/1727,[19] or the **Eurojust Regulation**, on the European Union Agency for Criminal Justice Cooperation (Eurojust), which has data protection rules to be regarded as *lex specialis* to the relevant provisions of the EU-DP Regulation;

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89, p. 89–131.

[13] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

[14] 'Operational personal data' are defined all personal data processed by EU bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 (Judicial cooperation in criminal matters) or Chapter 5 (Police cooperation) of Title V of Part Three TFEU to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies (Art. 3(2) of Regulation (EU) 2018/1725).

[15] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications services (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47, as subsequently amended.

[16] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

[17] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, p. 53–114.

[18] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1-71.

[19] Recital (12) of (EU) 2016/794.

The panorama of EU data protection law is actually **more complex** than what this short presentation might suggest. Even if the establishment of '*a harmonised framework for all data processing activities by law enforcement authorities for law enforcement purposes*' has been a major, recurrent concern of the European Parliament for many years (EP, 2014, 15), EU law does not currently offer a fully homogenous outlook. The approach notably enshrined by the LED in conjunction with the EU-DPR, whereby certain EU agencies processing data for law enforcement purposes are excluded from the reach of general provisions in the field, has been described as leading *'to a multi-level data protection regime where different legal instruments, and therefore different standards affecting individuals in exercising their data protection rights, apply'* (Belfiore, 2013, 367). There exist also a number of specific provisions on the protection of personal data in certain EU instruments that remained unaffected by the entry into force of the LED and have not been revised since – specific provisions for the protection of personal data that had entered into force before May 2016 in the field of judicial cooperation in criminal matters and police cooperation. In June 2020, the European Commission announced its action plan to progressively align with the LED the provisions still requiring alignment, a total of 10 according to its assessment (COM(2020) 262 final).

Often, discussions on the possible need for future EU-level regulation of AI take as a starting point an **explicit or implicit assumption according to which the general standards of the GDPR are the central element** of the current legal framework, if not the only element worth being reviewed (Penner, 2019). When focusing on personal data processing for law enforcement and criminal justice, taking such starting point is, however, unsuited, for two main reasons:

- first, the GDPR might in many relevant cases not apply, as other instruments will be applicable;
- second, even when the GDPR does apply, restrictions grounded on the fact that the processing relates to law enforcement and criminal justice might apply, *de facto* modulating the general safeguards it foresees.

It is thus crucial to appropriately situate discussions on AI regulation in this field by grounding them on a more refined understanding of applicable rules. The Annex to this study provides an overview of the some of the most relevant provisions of the GDPR and the LED in relation to algorithmic data processing, illustrating how they are not fully coincidental.

As explained by the European Data Protection Supervisor (EDPS), in the field of law enforcement '*data processing activities used are often opaque to individuals, which makes it difficult for them to know who is processing their data and for what purposes*', and '(i)*ndividuals' rights are often restricted*' in spite of the fact that *'the impact of data processing activities on their rights and freedoms is significant'* (EDPS, 2019, 38).

An additional challenge from a data subject's perspective is the fact that to some data processing activities might apply intricate combinations of different provisions, depending on the exact purpose of each processing operation and the identity of the controller.[20] In the AFSJ, the fact that data processing activities related to some information systems are governed by '*complex data protection regimes due to their multiple possible uses*' can result in a problematic lack of clarity (FGB, 2019, 4).

The question of whether the **GDPR** as such offers appropriate protection for individuals in the face of the proliferation of automated decision making is in itself not settled (Penner, 2019), and it is generally apprehended as an extremely delicate question, to the extent that it could lead to a push for a review of the GDPR eventually worsening its standards (De Brouwer, 2020). In relation to the safeguards useful

[20] See, for instance, the case of the *European Travel Information and Authorization System* (ETIAS) described below.

in an AI context, an often-quoted provision of the GDPR is its **Article 22**, devoted to ***'automated individual decision-making, including profiling'***.[21] Many, including the European Commission, refer specifically to Article 22 of the GDPR when considering the future of AI in Europe (COM(2019) 168 final, 4).

There is however much disagreement about the exact scope of Article 22 of the GDPR, and on its very nature - whether it imposes a general ban on certain types of automated decisions, or whether it provides data subjects with some rights whether certain types of automated decisions are taken (Brkan, 2019, 98; A29WP, 2017/2018, 19). There is equally controversy on the legal implications of Article 22 of the GDPR. Finally, there is also controversy on whether the provision is actually of any use in practice – whether it is effectively applied. The existence of a **'right to explanation'** under the GDPR has also been widely debated, leading for instance to the assertion that a legal basis for such a right is 'rather shaky and inconclusive' (Temme, 2017, 482). These issues have generated what some have described as *'vast debate in the research community'*, intertwined with a similarly vast debate surrounding the very explainability of AI systems (Sartor and Lagioia, 2020, 54).

Whenever some of the mentioned instruments apply, the fact that certain data processing operations relate to **law enforcement and criminal justice** can have important consequences on the scope of applicable rights and obligations.[22] In general terms, **exemptions and derogations based on law enforcement grounds are permitted** in EU data protection law, to the extent that they would be necessary and proportionate and if accompanied by safeguards. In this sense, Article 23 of the GDPR foresees that both EU and national laws may restrict a the scope of certain rights and obligations, including the mentioned **Article 22 of the GDPR**, if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[23]

Article 23 of the GDPR, described as *'highly controversial from the beginning'*, authorises deviations *'from core contents of the GDPR'*, even if *'with equally high requirements'* (Wagner & Benecke, 2016, 357). There is at the moment no official overview of the use at EU and national level of the exemptions and derogations grounded on this provision.[24] The rights granted to data subjects under the **LED** can also be restricted, by means of legislative measures, in order *'to avoid obstructing official or legal inquiries,*

[21] Profiling is defined in Article 4(4) of the GDPR as *'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.*

[22] The e-Privacy Directive, in this sense, foresees in its Article 15(1) that 'Member States may adopt legislative measures to restrict the scope' of certain rights and obligations when such restrictions *'constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences'*.

[23] Article 23(1)(d) of the GDPR.

[24] It is known that in any case the majority of Member States have made use of it (cf., for instance, Section 41 of the Dutch General Data Protection Regulation Implementation Act). Typically law enforcement considerations emerge: for example, in the Czech Republic, when what are at stake are 'protected interests' such as the prevention, investigation or detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures, compliance with obligations related to the exercise of any of the data subject rights from Art. 12 to 22 of the GDPR might be postponed (*Zákon ze dne 12. března 2019 o zpracování osobních údajů* (original); Czech Act No. 110/2019 Coll., act of 12 March 2019 on personal data processing, Section 6(2)(b) and Section 11(1)). To allow for this it is simply required to notify the DPA, a notification which would nonetheless not be necessary if the processing to which this applies is carried out by courts (ibid., Section 11(2)).

investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[25]

There is significant case law by the **Court of Justice of the EU (CJEU)** on EU data protection law. The Court has notably emphasised the need to interpret its provisions in a manner that guarantees the '*effective and complete protection*' of data subjects.[26] Particularly relevant here is the case law about the obligations imposed on the providers of public telecommunications services and networks with respect to **data retention** in order to ensure that data related to communication are available for the purpose of the investigation, detection and prosecution of serious crime, as often AI solutions in the field of law enforcement and criminal justice rely on the use for such purposes of data originally processed for other, sometimes unrelated, purposes, and involve both private companies and public authorities.

Notable in this context was the judgment of the CJEU in *Digital Rights Ireland,*[27] which annulled Directive 2006/24/EC[28] (known as the 'Data Retention Directive'), which, building on Article 15(1) of the e-Privacy Directive, imposed EU-wide restrictions of the rights and obligations set by such instrument in a way that the Court described as exceeding *'the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter'* (paragraph 69). Concretely, the CJEU decried that Directive 2006/24/EC covered, *'in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime'* (paragraph 57), and warned that '*the fact that data are retained and subsequently used **without the subscriber or registered user being informed** is likely to generate in the minds of the persons concerned **the feeling that their private lives are the subject of constant surveillance**'* (paragraph 37).[29]

In spite of its importance for individuals, the protection of personal data processed for law enforcement and criminal justice has received relatively **limited attention** from the European Commission, at least

[25] Recital (44) of the LED. The Czech instrument transposing the LED, to continue with a similar example, foresees that competent authorities might not comply with requests to exercise the right of access if doing so would endanger the performance of a task in the area of prevention, investigation and detection of criminal offences, prosecution of criminal offences, execution of criminal penalties and protective measures (ibid., Section 28(2)). As a safeguard is imposed the obligation to keep a record for the reasons justifying such decision, for a period of three years (Section 28(4)).

[26] Cf. *Google Spain*, Judgment of the Court (Grand Chamber) of 13 May 2014, Case C-131/12, ECLI:EU:C:2014:317, paras. 34, 38, 53, 58.

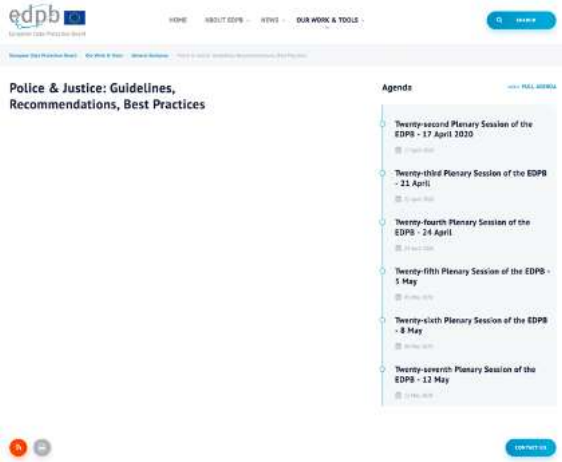
[27] *Digital Rights Ireland,* Judgment of the Court (Grand Chamber) of 8 April 2014, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[28] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

[29] In the subsequent *Tele2 Sverige and Watson* judgment, the CJEU held that the Member States cannot impose on the providers of electronic communication services an obligation of general and indiscriminate retention of data, noting that EU law, read *'in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication'* (Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, para. 112). Since then, the CJEU has been regularly confronted with further cases around data retention, and has notably still to adjudicate on relevant references for a preliminary ruling, sent by the French *Conseil d'État* (Joined Cases C-511/18 and C-512/18), the *Cour constitutionnelle de Belgique* (Case C-520/18) and the Investigatory Powers Tribunal (UK) (Case C-623/17) in which the primary issue is the application of the e-Privacy Directive to activities relating to national security and combatting terrorism – notably in light of Article 4 of the Treaty of the EU, under which national security is the exclusive responsibility of each Member State. In February 2020, the Irish Supreme Court discussed the submission of a request for a preliminary ruling in the case *Dwyer v Commissioner of An Garda Siochán* (Judgment of Mr. Justice Clarke, Chief Justice, delivered the 24th of February, 2020, Supreme Court, *Graham Dwyer vs. the Commissioner of An Garda Síochána*, Record No: 2019/18), also about data retention, safeguards related to the access to data, and the validity of convictions relying on data obtained through data retention schemes (Hennessy, 2020).

compared to the GDPR as such. The work of the European Data Protection Board (EDPB) in this area has also been until now noticeably weak, as illustrated by the absence of published guidelines, recommendations or best practices on its official website (see Figure 1, below).

Figure 1: EDPB work on police and justice



Police & Justice: Guidelines, Recommendations, Best Practices

Twenty-second Plenary Session of the EDPB - 17 April 2020

Twenty-third Plenary Session of the EDPB - 21 April

Twenty-fourth Plenary Session of the EDPB - 24 April

Twenty-fifth Plenary Session of the EDPB - 5 May

Twenty-sixth Plenary Session of the EDPB - 8 May

Twenty-seventh Plenary Session of the EDPB - 12 May

Source: Screenshot of https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en [accessed 7 July 2020].

2.2.2. Rules on the processing of non-personal data

AI is explicitly mentioned in Regulation (EU) 2018/1807 on the **Free Flow of Non-Personal Data in** the EU,[30] which aims at ensuring the free flow of non-personal data within the EU by regulating data localisation requirements, the availability of such data to competent authorities, and the porting of data for professional users. Recital (9) of that Regulation states indeed that **AI**, together with the Internet of Things and machine learning, represents a major source of non-personal data, which might take the form of '*aggregate and anonymised datasets used for big data analytics*'.

The Regulation on Free Flow of Non-Personal Data does not define 'non-personal data', but uses this term as equivalent to '*electronic data other than personal data*' (Article 2(1)). It acknowledges there might exist data sets in which personal and non-personal data are '*inextricably linked*', in which case the its provisions shall not prejudice the application of the GDPR (Article 2(2)). The European Commission published Guidance on the interaction between this Regulation and the GDPR, which clarifies that the notion of 'non-personal data' in the Free Flow of Non-Personal Data must be defined by opposition (*a contrario*) to personal data as laid down by the GDPR, and that there can be both 'non-personal data' which were originally as such, and data which were first personal but became 'non-personal' after anonymisation (COM(2019) 250 final, 4-5). The Guidance concedes that *'(i)n most real-life situations, a dataset is very likely to be composed of both personal and non- personal data'* (ibid., 4).

The key principle of the Regulation on the Free Flow of Non-Personal Data is that such non-personal data must **flow freely in the EU**. Data localisation requirements, referring to Member States imposing the processing of data in their territory or hindering the processing of data in another Member State,

[30] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

are in principle not permitted, unless justified on the grounds of public security (encompassing the need to facilitate the investigation, detection and prosecution of criminal offences) in compliance with the principle of proportionality. Regardless of the localisation of data, persons subject to obligations to provide data to competent authorities shall comply with such obligations by providing and guaranteeing effective and timely electronic access to the data to competent authorities.[31] If said persons would fail to comply, national competent authorities shall provide assistance to each other, if appropriate under instruments in the area of police cooperation and criminal justice such as the Council Framework Decision 2006/960/JHA (known as 'the Swedish initiative'),[32] Directive 2014/41/EU on the European Investigation Order (EIO),[33] and the Cybercrime Convention.[34]

All in all, the Regulation represents an important step in making available non-personal data across internal borders. Although it exceptionally allows for data localisation requirements to be established on the basis of security grounds, it nevertheless also foresees the need to comply with certain obligations to provide data across borders and reaffirms the relevance of mechanisms allowing for **cross-border access to data**, including **for law enforcement purposes**.

[31] Recital (25) of the Regulation on Free Flow of Personal Data.

[32] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89-100.

[33] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1-36.

[34] Convention on Cybercrime of the Council of Europe, CETS No 185.

3. AI IN LAW ENFORCEMENT AND CRIMINAL JUSTICE

This section provides an overview of the main current trends related to AI in the field of law enforcement and criminal justice, as relevant for an EU-level discussion of their impact on fundamental rights. They are clustered around four major themes: 'predictive policing', facial recognition, AI and criminal justice, and AI and borders.

The notion of AI espoused for these purposes is deliberately **wide**. In line with ongoing policy developments at EU level, the notion embraced here recognises as key components of AI developments their reliance on '**data**', '**algorithms**' and '**computing power**'.[35] Decomposing AI into these three basic elements allows to better perceive the continuities and discontinuities between AI and other notions that have previously instigated policy change and discussions in the area, such as **'smart surveillance'**, **'profiling'**, or '**big data'**.

The term 'smart surveillance' places the emphasis on the fact that new solutions are supposed to be 'intelligent', in the sense that they appear to 'learn' from data observed, as well as 'take decisions' potentially 'on their own' on the basis of certain algorithms. In this sense, it has been stated that what is at the core of EU-level discussions around AI are as a matter of fact '*algorithmically controlled ADM* [Automated Decision Making] *systems*' (Penner, 2019).

Generally speaking, the word 'profiling' is connected to the sorting out of individuals based on the '*computer analysis of large data sets'*, and is as such already commonly used by used by law enforcement officers and border guards *'to prevent, investigate and prosecute criminal offences, as well as to prevent and detect irregular immigration'* (FRA, 2018a, 7-8).

The term 'big data' is typically used to evoke the processing of vast data sets, including data sets with data of heterogenous origins. The EDPS noted that in its recent *White Paper on AI* the European Commission relied on a conception of AI that is broad, and that can be interpreted as encompassing what other refer to as 'big data' (EDPS, Opinion 4/2020, 7). In the past, 'big data' had been associated with changes of potentially profound repercussions - portrayed as tearing down what counts as crime-relevant knowledge, what counts as proper reasoning, and even how should crime be prevented, investigated and prosecuted (Završnik, 2017a, 3). In any case, the development of AI systems, in particular those based on machine learning, both presupposes and fosters the creation of vast data sets that can be connected to 'big data' (Sartor & Lagioia, 2020, i), and today's AI development is largely driven by data (Boucher, 2019, 5).

The term AI as emerging in these debates is, all in all, both *'poorly defined and potentially misleading'* (Babuta, Oswald & Rinik, 2018, 2). Furthermore, the field of AI being a very dynamic field, the most rigorous efforts to define AI and provide an operational definition and related taxonomies and keywords stress the necessity to do so always in the context of a dynamic process, subject to regular reviews and iterations (Samoili et al., 2020, 6).

Situating AI in the context of other, pre-existing policy discussions does not aim at negating its innovative dimension, but should help to perceive that debates around AI are not completely unique, and have not arisen in a void space. They surfaced among many other developments encouraging reliance on computers and algorithms, and supporting wide access to data, also insofar as law enforcement and criminal justice are concerned.

[35] Cf. the broad vision entertained by the EC according to which *'AI is a collection of technologies that combine data, algorithms and computing power'* (COM(2020) 65 final, 2).

The processing of data for law enforcement purposes of data not originally collected for such purposes is an issue that pops up regularly, also beyond AI discussions.[36] The constant multiplication of data in our societies has indeed been accompanied over the years with a sustained interest among the law enforcement community to **access any possibly relevant data**. Such interest includes, for instance, an interest in data held by private companies, including data that might require crossing national borders (Carrera & Stefan, 2020, 3).

Finally, AI-related developments in this field also need to be placed against the background of a progressive 'digital transformation' of the state. The United Nations (UN) Special Rapporteur on Extreme Poverty and Human Rights, in this sense, described in 2019 the emergence of the 'digital welfare state' in many countries across the globe, as systems of social protection and assistance are increasingly driven by technologies '*used to automate, predict, identify, surveil, detect, target and punish*' (UN Special Rapporteur on Extreme Poverty and Human Rights, 2019, 1).

3.1. 'Predictive policing'

'Predictive policing' has been described as a catchphrase relying broadly on the claim that through the algorithmic processing of data sets it is possible to **reveal patterns of probable future offending and victimisation**, which can thus be interdicted before they happen (Wilson, 2017, 108). Although the origins of predictive policing might be traced back to experiments of computer-assisted crime control in the 1970s, and although prediction in the area of crime and punishment has been developed and discussed more many decades (Harcourt, 2008), the term became eventually connected to the rise of 'big data' (Wilson, 2017, 109). **Prediction as an extensive trend** has noticeably marked security developments globally and in Europe over the past decade at least, typically associated to **prevention**.

'Predictive policing' can take a variety of shapes, and multitude of typologies have been put forward. Predictive policing methods can for instance be divided into four broad categories: methods aiming at predicting **crimes**, or forecasting places and times with an increased risk of crime; methods aiming at predicting **offenders**, or identifying individuals at risk of offending (or reoffending) in the future; methods aiming at predicting **perpetrators' identities**, or creating **profiles** similar to those of past offenders, and methods aiming at predicting **victims of crimes**, used to identify groups or individuals who are likely to become victims of crime (Perry et al., 2013, xiv). Typologies can also be grounded on the possible purposes of algorithmic data or intelligence analysis within the policing context: it is then possible to distinguish predictive policing **on a macro level** incorporating strategic planning, prioritisation and forecasting; and **operational intelligence** linking and evaluation which may include, for instance, crime reduction activities; and decision-making or risk-assessments relating to **individuals** (Oswald & Grace, 2016, 3).

The NGO Electronic Privacy Information Center (EPIC) in 2020 a report dating from 2014 from the US Department of Justice to former President Obama, about predictive analytics and algorithms in law enforcement.[37] The report states that the use of 'social network analysis' was gaining '*gaining the attention of some State and Local law enforcement agencies*' (US Department of Justice, 2014, 3). Social network analysis was by then starting to be used to **identify individuals** who may then '*receive increased scrutiny, additional support services, or both*' (idem). According to the report, most of the US Federal Bureau of Investigation (FBI) data analysis targeted particular subjects, although in some cases

[36] The EDPS, for instance, expressed concern in July 2020 about the possibilities granted by Microsoft to possible access to data connected to the use by EU institutions of its products and services to third parties including law enforcement or other government agencies (EDPS, *Outcome of...*, 24).

[37] The report was obtained following a Freedom of Information Act (FOIA) request, lawsuit, and negotiated settlement: EPIC v. DOJ, No. 18-5307 (D.C. Cir.).

it was used '***to identify sub-sets of persons** who may bear further investigative scrutiny*' (ibid., 8). Information used for such data analysis was described as originating in a '*a variety of data sources*', including commercial databases, and encompassing '*among other things, biographical information, biometric information, financial information, location information, associates and affiliations, employment and business information, visa and immigration information, travel information, and criminal and investigative history information*' (idem).

'Predictive policing' initiatives have popped up in different Member States mainly since the beginning of the 2010s these have been, for instance, initiatives somehow connected to or involving automatic license plate control systems (Alfter, 2019, 52; Van Brakel, 2019, 44). The expansion of police use of algorithms in the recent years has been connected to three factors: austerity measures that limit resources and push towards apparently more economically efficient new solutions; an increasing perception that police ought to adopt a preventative posture, placing emphasis on anticipating harm, and an increase in the volume and complexity of data available, necessitating increasingly sophisticated processing tools (Babuta & Oswald, 2020, vii).

Prediction and prevention have been particularly productive in relation to **money laundering and terrorist financing**.[38] Current approaches in this field are indeed built upon obligations imposed on banks and other obliged entities to take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account **risk factors** including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels. This risk assessment by the entities acting as 'gatekeepers' can eventually lead to the reporting of transactions regarded as **suspicious** to competent EU Financial Intelligence Units (FIUs), which have their own reporting and data sharing obligations. The eventual labelling of certain individuals as **suspects** during this process can lead to situations requiring special attention, raising issues of data protection but also potentially impacting the right to presumption of innocence (Article 48 of the EU Charter of Fundamental Rights).[39]

Predictive approaches in law enforcement often rely at least partially on the processing of data that is not as such originally related to crime, but initially collected by **private companies** in the context of their normal business activity (e. g. banking, telecommunications, travelling). Predictive policing schemes also typically rely on predictive software produced by private companies, be it vendors specialising in this field (the most often quoted being probably the company PredPol) or large technological corporations (Wilson, 2017, 114).

In the US, the media have reported practices by private companies targeting the **AI market** that would actively involve collecting data in a not particularly transparent manner for, or in view of eventually making it available to, law enforcement authorities (Koebler, Maiberg & Cox, 2020). For instance, in March 2020 surfaced accusations against an AI company, Banjo, of designing apps specifically conceived to covertly collect social media data (Cox & Koebler, 2020).

Many relevant developments have materialised in the United Kingdom (UK). Especially interesting are discussions around the **Gangs Violence Matrix (GVM)**, a tool used since 2012 by the Metropolitan

[38] See, notably: Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117. Also referring to money laundering and terrorist financing: LIBE, 2020/2016(INI), 5.

[39] Data protection issues were at the forefront of the ban imposed by the EDPS on 19 December 2019 on processing operations carried out by Europol in the technical operation of FIU.net, a decentralised information network designed to support national FIUs (EDPS, 2019, 41).

Police in order to identify and risk-assess gang members[40] across London involved in gang violence, and to identify those at risk of victimisation. The GVM measures the harm that individuals pose by scoring them based on evidence of them committing violence and weapons offences, as well as police intelligence relating to them having access to weapons, or them being involved in, or at risk from, gang violence: individuals are thus graded as red, amber or green, denoting the level of risk (for victims) or harm (for offenders) they present.[41] The database encompasses both adults and minors (MOPAC, 2018, 4).

According to the NGO Amnesty International, the Metropolitan Police has refused to divulge information about the precise criteria used to assign automated 'harm scores' to individuals on the matrix, and it would also be unclear how such scores might relate to any enforcement action (Amnesty International, 2018, 13-14). More generally, the NGO has denounced that the data processing practices around the database and the lack of proper safeguards generate a risk that the tool would '*discriminate against already marginalised young people, with disproportionate impact on black boys and young men'* (ibid., 3). An enforcement notice was served on the Metropolitan Police Service by the Information Commissioner's Office (ICO) in 2018, relating to lack of compliance with data protection law. Since then, a significant number of individuals are believed to have been removed from the database (Dodd, 2020).

'Predictive policing' initiatives can sometimes rely on the use of facial recognition technologies, which in their turn rarely develop separately from other developments more broadly connected to the monitoring of public spaces, for instance to detect 'abnormal behaviour (e. g., Kayser-Bril, 2020).

3.2. Facial recognition

Facial recognition technology allows for the automatic identification – or authentication - of an individual by matching facial features from two or more digital images (EU FRA, 2019, 2). Under EU data protection law, even if the processing of photographs as such is not systematically considered as processing deserving **special protection** beyond general data protection rules, when data are processed in order to allow for such identification or authentication they are to be regarded as biometric data deserving special protection.[42]

The use of facial recognition technologies is not limited to the law enforcement and criminal justice field. Facial recognition has, a matter of fact, generated much interest and disputes globally also in other fields, as illustrated by a class-action lawsuit in the US against Facebook's automated photo-labelling and its use of face-matching software to suggest names of people in users' photos.[43]

From a global perspective, the uses of facial recognition by some specific states have been particularly controversial; in this sense, must be mentioned international concerns about the use of facial recognition in China to identify members of the Uighur minority, a largely Muslim group (Mozur, 2019). Facial recognition in public spaces is said to be growing particularly rapidly in Russia (Light, 2019).

In the field of law enforcement, the use of facial recognition that has gathered more attention concerns **live facial recognition**.

In 2016, a **US** report warned of the widespread use of live facial recognition in the country, alerting that already at the time several major police departments were actively exploring real-time face recognition

[40] A gang is defined in this context as a relatively durable, predominantly street-based group of young people who see themselves (and are seen by others) as a discernible group, and engage in a range of criminal activity and violence.

[41] As explained by the Metropolitan Police's website.

[42] See notably Recital (51) and Arts. 4(14 and 9(1) of the GDPR; Art. 3(13) and 10 of the LED.

[43] Lawsuit settled in January 2020: Singer & Isaac, 2020.

on live surveillance camera video (Garvie, Bedoya & Frankle, 2016).[44] Documenting a variety of issues related to these developments, including privacy and bias issues but also threats to free speech, the authors emphatically called for **legislation** to regulate law enforcement use of facial recognition searches, and notably for more transparency, under the admonition that *'Face recognition is too powerful to be secret'* (ibid.).

Some US cities such as San Francisco and Boston have banned certain uses of facial recognition in their territory (Vaas, 2020). In Detroit, there is **ongoing litigation** on the matter between the American Civil Liberties Union (ACLU) and the Detroit Police Department, related to the case of a man who was wrongfully arrested on the basis of a misidentification by facial recognition software (Lee, 2020). Still in the US, campaigners have been countering the spread of facial recognition at university campuses, notably on the grounds of what they described as **systemic racial and gender bias** in the deployed systems (Fight for the Future, 2020).

In June 2020, the US Technology Policy Committee (USTPC) of the Association for Computing Machinery (ACM) urged an immediate suspension of private and governmental use of facial recognition technologies *'in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights'*, pending the adoption of appropriately comprehensive law and regulation to govern its use, oversee its application, and mitigate potential harm (ACM USTPC, 2020, 1). The call was based on the assessment that the technology too often produces results demonstrating clear **bias based on ethnic**, **racial, gender, and other human characteristics**, characteristics that the ACM USTPC nevertheless described as being *'recognizable by computer systems'* (idem).

Policy discussions around facial recognition are prominent in the **UK**, where a series of police forces rely on these systems. In London, for instance, the Metropolitan Police uses Live Facial Recognition to *'to help tackle serious violence, gun and knife crime, child sexual exploitation and help protect the vulnerable'*.[45] The UK is notably funding a research project on fostering unconstrained face biometrics capability, presented as potentially significantly contributing to the UK government's security agenda in the framework of smart cities and national security.[46] The Metropolitan Police Service is one of the project's collaborators, together with inter alia a Chinese academic institution, and the UK Home Office is one of the project's partners.[47]

In 2019, the High Court of England and Wales declared that the use of automated facial recognition technology to match the faces of members of the public against police watchlists was **lawful**, in a case concerning the programme piloted for already a number of years by **South Wales Police**, called AFR Locate.[48] The programme is described by South Wales Police as a 'live-time' deployment of automated facial recognition technology which compares live camera feeds of faces against a predetermined **watchlist**, in order to 'locate' persons of interest, generating possible matches that are reviewed by the operator(s).[49] A 2018 evaluation of the use of facial recognition technology by South Wales Police noted that legal instruments surrounding it *'and the ethical principles they expound pre-date the kinds of*

[44] The original deployment of a 'smart CCTV system' in public streets in the US has been traced back to 2001; the first uses of these technologies are believed to have been in prison settings (Gates, 2011, 54 and 64).

[45] See the MET online information about Live Facial Recognition.

[46] Project *Face Matching for Automatic Identity Retrieval, Recognition, Verification and Management*, FACER2VM, EP/N007743/1, January 2016- September 2021.

[47] Idem. See also: See also: Privacy International, 2020d.

[48] R (on the application of Edward Bridges) v The Chief Constable of South Wales [2019] EWHC 2341.

[49] See *ad hoc* website by South Wales Police: http://afr.south-wales.police.uk/. 'Persons of interests' are defined as people wanted on warrants and suspects for particular crimes, but also potentially missing persons and vulnerable people, and people sought for intelligence purposes.

affordances AFR technologies provide', adding that *'[a]s such, new regulatory frameworks will probably be necessary as this technology becomes more widely adopted'* (Davies, Innes & Dawson, 2018, 41).

Over the years, a number of calls for a **suspension of the deployment of certain uses** of facial recognition technology have been voiced out internationally by civil society organisations. The Public Voice's 2019 Declaration *A Moratorium on Facial Recognition Technology for Mass Surveillance* not only called for such a suspension, but also urged countries *'to establish the legal rules, technical standards, and ethical guidelines necessary to safeguard fundamental rights and comply with legal obligations before further deployment of this technology occurs'*.[50]

A particularly controversial issue concerns the role of **private companies** in the deployment of these technologies. In February 2020, media reported that according to leaked documents the company Clearview AI had contracts with thousands of law enforcement agencies, companies, and individuals around the world, and also in Europe (Mac, Haskin & McDonald, 2020). Clearview AI services, which it formally targets to *'active law enforcement personnel'*,[51] can be described as consisting in matching persons to online images taken from a variety of platforms (Hill, 2020). The service allows for instance an investigating officer to upload a photo of an individual 'of interest' and search a database, compiled by Clearview AI, of what are presented as 'publicly available images', posted online by somebody (Blatt, 2020) – not necessarily the person at stake. Some of the platforms from which Clearview AI appeared to capture images have formally objected to such scraping of pictures by Clearview AI (Porter 2020).

In March 2020, the Swedish Data Protection Authority (Datainspektionen) disclosed it was investigating the possible use of Clearview AI services by Swedish public authorities (*Datainspektionen*, 2020). In July 2020, the ICO and the Australian Information Commissioner announced they had opened a joint investigation into Clearview AI, focusing on its use of 'scraped' data and biometrics of individuals (ICO, 2020).

In a letter in response to concerns raised by a number of MEPs regarding **the possible use of Clearview AI products by EU law enforcement authorities**, dating from 10 June 2020, the EDPB noted that such authorities may under certain circumstances use facial recognition technologies to check images against templates '*in databases that are under the control of the official authorities and that have been established under Union or Member State law'*, but that the *'possible use of a service such as offered by Clearview AI by law enforcement authorities would, however, be fundamentally different, in that it would imply, as part of a police or criminal investigation, the sharing of personal data with a private party outside the Union and the biometric matching of such data against the latter's mass and arbitrarily populated database of photographs and facial pictures accessible online'* (Jelinek, 2020). The EDPB added it had '*doubts as to whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI'*, noted that *'several EDPB members have already started to further inquire about the use of such facial recognition technologies in their respective jurisdictions'*, and expressed its willingness to contribute to further debate on these matters (idem).

Clearview AI is not the only company about which reports of agreements with law enforcement authorities have been published. Amazon's owned company Ring, a 'smart security' device company mostly known for selling interactive video doorbells, has been reported to have a variety of agreements with law enforcement authorities, including in Europe (Privacy International, 2020b), which may or not relate specifically to facial recognition or other AI-related technologies.

[50] Full text and list of signatories available here.

[51] See, in this sense: https://clearviewai.typeform.com/to/SFnULY.

The deployment of **facial recognition technologies in the public space** has provoked controversy in many countries worldwide. It is the case for instance in Brazil, where the installation in the public metro of a system to deliver ads based on automated 'detection' of emotion, gender, and age of passers-by led to litigation by the Brazilian Institute of Consumer Protection (IDEC) (Arroyo & Leufer, 2020).

In the EU, the deployment of facial recognition in public spaces, including in test mode, has generally provoked a variety of reactions. In 2017, the public was said to be divided when a field test of a facial recognition programme was launched at Berlin's railway stations (Fürstenau, 2017).

There have also been reactions from the judiciary and DPAs. In Belgium, the DPA halted a deployment of facial recognition cameras at Zaventem Airport that had no legal basis (Peeters, 2020). In France, **an administrative court declared invalid** in February 2020 a decision taken by a regional council allowing to test **a surveillance system relying on facial recognition** to monitor access to two high schools.[52] The judgment criticised *inter alia* the lack of prior impact assessment and the attempt to ground the processing of personal data on the consent of the individual concerned, or their parents, despite the fact that their relation towards the institutions rendered impossible the provision of genuinely free consent. The judgment followed a complaint introduced together with other associations by the NGO La Quadrature du Net, also active in contesting the use of facial recognition to monitor participants to demonstrations (La Quadrature du Net, 2019).

In August 2019, the Swedish DPA fined a municipality 200 000 for using facial recognition technology to monitor the attendance of students in school (EDPB, 2019). Facial recognition had been deployed in the context of a pilot based on the consent of individuals, but the DPA considered that consent was not a valid legal basis in such context given the clear imbalance between the data subject and the controller (idem). The same DPA has, however, authorised certain uses of facial recognition by law enforcement authorities (Barik, 2019).

Facial recognition technologies have been until now deployed in public, or semi-public spaces, both by public authorities and private companies. In Spain, for instance, facial recognition systems have been recently deployed in some supermarkets presumably in order to automatically detect individuals who might be subject to a restraining order not allowing them to enter the premises or approach the supermarket's workers (Rubio, 2020). EU DPAs have sometimes authorised certain uses of live facial recognition by private actors – for example, the Danish DPA authorised its use by a football club at the entrance of its stadium, to identify persons banned from attending football matches (IT-Pol, 2019).

In 2020, some large companies such as IBM announced they would refrain in the future from certain commercial activities related to facial recognition (Peters, 2020).

3.3. AI and criminal justice

AI-related developments, relying on an increasingly extensive use of data, computation and algorithms, have also permeated the administration of justice,[53] including criminal justice. The origins of some current developments may be traced back to the emergence of 'computerised justice' as a trend aiming at improving the accountability and predictability of judicial decisions, by reducing discretionary powers in the hands of judges regarded by some, in some circumstances, as excessive (Franko Aas, 2005, 65).

[52] Tribunal administratif de Marseille (9ème chambre), N° 1901249, 27 February 2020.

[53] Justice has embraced the digital in a number of ways, such as online dispute resolution, where algorithms play an increasing role (Katsh & Rabinovich-Einy, 2017).

AI is used or being explored in European legal systems for a variety of purposes, such as facilitating access to law (e.g. through chatbots), supporting alternative dispute settlement measures in civil matters, online dispute resolution, or 'judge profiling'.[54] Some of the ways in which AI-related practices have entered the courts relate to the calculation of the risks of misconduct, for instance for algorithmic probation (Wilson, 2017b, 144). The use of predictive tools by judges in criminal trials in Europe, sometimes labelled 'algorithmic justice' or 'automated justice', has nonetheless at least until recently been described as very rare (Ronsin & Lampos, 2018, 37).

Recidivism algorithms have gathered much attention especially in the **US**. Many of the concerns raised over the use of algorithms for criminal justice purposes refer to indirect racial **bias** in models that predict offending and re-offending, for instance by the use of proxy variables that are not neutral. A ProPublica investigation conducted in 2016 into the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system found that black defendants were almost twice as likely to be deemed at risk of offending than white defendants (Babuta, Oswald & Rinik, 2018, 7, noting however the system's developer contested the analysis; Završnik, 2017b, 145).

Issues around **due process** safeguards have also come to the fore, most famously in *State v. Loomis*,[55] a judgment by the Wisconsin Supreme Court held that a trial court's use of an algorithmic risk assessment in sentencing did not violate the defendant's due process rights (even though the methodology used to produce the assessment at stake was not disclosed), nevertheless introduced a procedural safeguard to alert judges about the limitations of such assessments. Another interesting US case regarded litigation in Washington, D.C. challenging the use of the Structured Assessment of Violence and Risk in Youth (SAVRY) risk assessment tool in a criminal juvenile sentencing proceeding: the tool had determined that a young person who had been promised to be given probation in exchange of pleading guilty was nevertheless 'high risk', and had to be incarcerated (Richardson, Schultz, Southerland, 2019, 9). The defence lawyers challenged the SAVRY assessment contesting its scientific robustness, and won the argument, convincing the judge to disallow the use of the tool in the specific case at stake (ibid., 10).[56]

The **UK** provides a good example of developments in this area with the algorithmic 'Harm Assessment Risk Tool' (HART)' developed in 2017 by Durham Constabulary to assess the risk of individuals reoffending, in order to support custody decision-making (Babuta, Oswald & Rinik, 2018, 6). The tool generates a risk score that becomes one among a number of factors for human officers to take into account when making their overall risk assessment (idem). The tool generated controversy *inter alia* for originally relying on the use of consumer segmentation data from a private company, later put aside (Grace, 2019, 6).

Generally speaking, the use of AI in judicial systems is critically dependent on the **availability of data**, which has led to recognising an open data approach to judicial decisions as a prerequisite for the work of legal tech companies specialising in search engines or trend analysis (so-called 'predictive justice') (Ronsin & Lampos, 2018, 16). The processing of such data raises however a number of issues, some of

[54] Cf. Appendix II accompanying the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, adopted by the CEPEJ during its 31st Plenary meeting (Strasbourg, 3-4 December 2018), CEPEJ(2018)14.

[55] *881 N.W.2d 749 (Wis. 2016)*.

[56] Other relevant cases include *Louisiana v. Hickerson*, concerning the use by law enforcement authorities in the city of New Orleans of a risk-assessment database called Gotham, created by the company Palantir (Richardson, Schultz, Southerland, 2019, 13); The database had been in principle deployed to identify individuals likely to become a perpetrator or victim of gun violence, to whom awareness messages about their lifestyle were to be sent, but appeared to have played a role in investigations leading to a prior trial against Mr. Hickerson (ibid., 14).

which concern data protection law, but also others which concern the possibility for change in the formation of case-law (idem).

Researchers have noted that although this type of tools are currently being used for limited purposes, there is potential for the technology to do much more, and the lack of a regulatory and governance framework for its use is concerning. (Babuta, Oswald & Rinik, 2018, 7).

3.4. AI and borders

There are a variety of instances in which algorithms are already relevant in a border context. Automated decision systems are becoming more and more prevalent in relation to borders globally, and can include systems that **classify** individuals (e. g. as high risk, or high priority); that **generate scores**, probability assessments, and other indicators supporting human decision-making; that '**flag**' cases for review or investigation; that **provide recommendations** on applications, or even that render full decisions (Molnar & Gill, 2018, 3).

3.4.1. General trends

In the EU, border-related largescale information systems incorporating algorithmic processing are typically **connected, through a variety of data flows, to law enforcement authorities** – national authorities, Europol, or often both. Data emanating from law enforcement authorities might be fed into border-related systems, and data from these systems might eventually be supplied or rendered accessible to law enforcement authorities. **Security and border management** have been major drivers for the growth of both centralised and decentralised information systems in the AFSJ for many years already.[57]

The interest among public authorities in **data** to be processed for migration and asylum purposes appears to be increasing in many Member States. Some of them have for instance introduced over the past years legal changes to their national asylum procedures, *inter alia* to make it possible for authorities to seize and analyse data in personal devices (e.g. smartphones) from asylum seekers,[58] also increasing the applicants' duty to cooperate (EMN, 2019, 6). The data might be analysed to help establishing their identity and travel routes (ibid., 21). Member States are also enhancing border control by investing in technical equipment for border checks (e.g. 'e-gates', biometric ID checks, kiosks, etc.), including facial recognition tools (ibid., 54). Technologies used at the borders are manifold and can include automated surveillance systems with different detection capabilities (e.g., heartbeat detection and thermal cameras) (idem).

Globally, there has been a trend over the years to increase data disclosure obligations for individuals crossing borders. In the US, ongoing litigation is challenging an obligation imposed since 2019 on visa applicants to disclose social media accounts (EFF, 2020).

At EU level, a notable development was the issuing in 2019 by the EDPS of a temporary ban on the production of **social media monitoring** reports by the European Asylum Support Office (EASO). EASO was using the such reports to provide management and relevant stakeholders information '*on shifts in asylum and migration routes and smuggling offers, as well as an overview of conversations in the social media community relating to key issues, such as flight, human trafficking and other asylum systems and processes*' (EDPS, 2019, 30). The EDPS decried this was occurring without the necessary legal basis and

[57] For an overview, see, for instance: COM(2016) 205 final.

[58] In Germany there is ongoing litigation questioning the legality of the measures, in place since 2017, allowing public authorities to access data stored in the mobile devices of asylum seekers in view of preventing asylum fraud (Reuters, 2020).

appropriate safeguards, and has highlighted that *'(s)ocial media monitoring tools in general raise a number of serious data protection concerns',* which in that case *'included a* ***chilling effect*** *- the tendency for users to self-censor their online content if they think it might be monitored -, the high risks posed to the fundamental rights of the individuals and groups monitored,* ***the lack of fairness and transparency*** *involved in processing this data and the vast number of social media users implicated'*.[59]

In EU's AFSJ, large scale information systems increasingly incorporate **algorithmic decision-making**. This is generally presented under a variety of terms in the relevant legislative documents, different from AI, including for instance references to the *'the data-analytics method'* (COM(2018) 302 final, 9). Regardless of terminology, what is generally at stake is that beyond the detection of 'known' specific suspects, some instruments contain an algorithmic profiling functionality which identifies 'unknown' individuals who may be of interest to law enforcement and border management authorities (EU FRA, 2018a, 114).

In 2016, the European Parliament requested the European Commission to launch a Pilot Project for a fundamental rights review of EU data collection instruments and programmes. The project eventually voiced out **concerns on the impact on fundamental rights** of the '**profiling functionalities**' included in both existing and upcoming EU information systems (FGB, 2019, 4).

An important number of developments in this field converge in **eu-LISA**, the EU Agency ensuring the operational management of the EU large-scale Information Technology (IT) systems, and their respective communication infrastructure, in the AFSJ: Eurodac (the European database of digitalised fingerprints of asylum seekers and irregular migrants), the Schengen Information System (SIS) (facilitating the exchange of information on persons and objects between national police, border control, customs, visa and judicial authorities), and the Visa Information System (VIS), which supports the implementation of the EU's common visa policy by enabling dedicated national authorities to enter and consult data, including biometrics, for short-stay visas to the Schengen Area. Eu-LISA is currently developing other upcoming EU-wide information systems: the **Entry/Exit System** (**EES**), the **European Travel Information and Authorization System** (**ETIAS**) and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), as well as their interoperability components, and plays a crucial role in the technical implementation and development of the interoperability of EU information systems as foreseen by the 2019 **interoperability** package.[60]

A more detailed examination of ETIAS can help understanding some of the fundamental rights challenges related to these developments, which are relatively paradigmatic, and thus useful to situate the EES and an upcoming 'upgrade' of VIS.[61] Before that, issues surrounding the algorithmic processing of data related to travelling shall be considered.

[59] *EDPS, Annual Report 2019, Luxembourg: Publications Office of the European Union, 2019,* p. 30.

[60] Cf. Regulation (EU) 2019/817 establishing a framework for interoperability between EU information systems (borders and visa) and Regulation (EU) 2019/818 establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration), OJ L 135, 22.5.2019, p. 27–84; and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85–135..

[61] In 2018, the European Commission published a proposal for a Regulation of the European Parliament and of the Council on upgrading the Visa Information System (VIS) (COM(2018) 302 final). The upgrade presented in the proposal relies notably on introducing the use of *'risk indicators'* containing *'data analytics rules, as well as specific values provided by Member States and statistics generated from other relevant border management and security databases'* (ibid., 9).

3.4.2. PNR

Profiling travellers is not a novelty in the EU. Significant legal and policy discussions have taken place in relation to the processing of **Passenger Name Record (PNR) data**, be it the transfer of such data to **third countries**, or in the context of the **EU PNR system**. Originally, what was especially challenging was the question of how to frame, from a EU law perspective, the use for law enforcement purposes of data originally collected by private companies for commercial purposes.[62] Eventually, questions focused on the substantive requirements in terms of fundamental rights for the processing of data under PNR schemes.

The European Parliament requested to the CJEU an Opinion of an agreement for the transfer of **PNR data to Canada** that had been negotiated with Canadian authorities, in particular regarding the envisaged agreement's compatibility with obligations stemming from the EU Charter. The Opinion, delivered in July 2017, stressed a number of significant failures.[63] Noting the envisaged agreement permitted *'the systematic and continuous transfer of PNR data of all air passengers flying between the European Union and Canada'*,[64] to be used as *'an intelligence tool'*,[65] the Court observed that the PNR data were '*intended to be analysed systematically before the arrival of the aircraft in Canada by automated means,* ***based on pre-established models and criteria'***, as well as automatically verified by cross-checking with other databases,[66] and that those analysis could '*give rise to additional checks at borders in respect of air passengers identified as being liable to present a risk to public security and, if appropriate, on the basis of those checks, to the adoption of individual decisions having binding effects on them'*.[67] It noted that these analyses were to be carried out '***without there being reasons based on individual circumstances*** *that would permit the inference that the persons concerned may present a risk to public security*'.[68]

The CJEU stated that '*the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-established models and criteria and on the databases on which that type of data processing is based'*,[69] and, as a consequence, '*the pre-established models and criteria should be* ***specific*** *and* ***reliable***,[70] *making it possible (…) to arrive at results targeting individuals who might be under a* ***'reasonable suspicion'*** *of participation in terrorist offences or serious transnational crime and* ***should be non-discriminatory***".[71]

[62] Cf. Judgment of the Court (Grand Chamber) of the CJEU of 30 May 2006, *European Parliament v Council of the European Union* (C-317/04) *and Commission of the European Communities* (C-318/04), ECLI:EU:C:2006:346.

[63] CJEU, *Opinion 1/15 of 26 July 2017* ('EU Canada PNR'), ECLI:EU:C:2017:592.

[64] Ibid, para. 127.

[65] Ibid., para. 131.

[66] Idem.

[67] Ibid., para. 132.

[68] Idem.

[69] Ibid., para. 172.

[70] In this regard, and *'since the automated analyses of PNR data necessarily involve some margin of error'*, *'any positive result obtained following the automated processing of that data must (…) be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the air passengers concerned is adopted'* (para. 173).

[71] Idem. In relation to this last point, the CJEU proclaimed that *'in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement'* (para. 174).

The **EU PNR** system was set up by the Directive (EU) 2016/681 (the 'EU PNR Directive') in 2016.[72] It applies as a general rule to data of 'extra-EU flights', although Member States can also extend it to 'intra-EU flights'. The system it puts in place is in a way reminiscent of the general approach described above for the prevention of money laundering, to the extent that data processing obligations are imposed on air carriers, which must be in contact with *ad hoc* national **Passenger Information Units (PIUs)**. In this scenario, however, the risk assessment procedures are not to be undertaken by private companies, which are only responsible for the provision of collected data. PIUs are responsible for collecting, storing and **further processing** such PNR data, for transferring them to the competent authorities, and for exchanging them with the PIUs of other Member States, as well as with Europol.

One of the most discussed issues over the implementation of the EU PNR Directive has been the involvement of **Europol** in the development and dissemination of a *'common sets of **indicators**, **targeting rules and risk profiles'*** (Presidency of the Council, 6300/19, 2019). In 2019, a majority (88%) of Member States declared that it would be a *'a great idea'* if Europol could contribute to the developing targeting rules and indicators, *'due to its central position and its important role in gathering and sharing information on targeting rules and/or risk profiles'*, and act as *'depository'* to the common rules and indicators (ibid., 14). Some Member States, however, noted it should be up to each PIU and Member State to decide if they would invite Europol to develop such sets and to what extent these sets would be considered as obligatory. There were also discussions on whether the idea that Europol could offer a central storage of all indicators and targeting rules used nationally, presumably acceptable by some, was actually a good idea, with some Member States regarding that as a potential information security breach that would jeopardise their (national PIUs) effectiveness (ibid. 9).

The CJEU is expected to rule on the **compatibility of the EU PNR Directive and EU fundamental rights**. A pending case (Case C-817/19) concerns indeed a request for a preliminary ruling from the Belgian Constitutional Court, lodged in October 2019, following action by the association *Ligue des droits humains*, on transposition of the EU PNR Directive in Belgium. The questions submitted to the Court refer notably to the systematic prior assessment of the data of all passengers (Belgian Constitutional Court, 2019), that is, the 'advance assessment' made by comparing passenger data against databases and predetermined criteria, which applies *'in a systematic and generalised manner, regardless of whether there is any objective ground for considering that the passengers concerned may present a risk to public security'*.[73] In January 2020, the District Court of Cologne also submitted to the CJEU a request for a preliminary ruling, in the context of proceedings initiated by the Gesellschaft Für Freiheitsrechte (GFF) and a number of plaintiffs (Turß, 2020). One of the plaintiffs litigating in Germany is the former Head of the Secretariat of the Committee on Civil Liberties, Justice and Home Affairs in the European Parliament (LIBE Committee) (De Capitani, 2019).

3.4.3. ETIAS

The **European Travel Information and Authorisation System (ETIAS)** concerns travel authorisations for third-country nationals exempt from visa requirements to enter the Schengen area, on the grounds of a *'consideration of whether the presence of those third-country nationals in the territory of the Member*

[72] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149.

[73] See application to the CJEU in Case C-817/19.

States would pose a ***security****,* ***illegal immigration*** *or* ***high epidemic risk'***.[74] Member States' designated authorities and Europol can consult data stored in the ETIAS Central System for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.[75] With ETIAS, the relevant considerations to decide on travel authorisation occur prior to the travellers' arrival at external border crossing points. Its use shall be optional only during the first six months from the date on which it starts operations,[76] but compulsory afterwards. A travel authorisation, it must be noted, does not confer an automatic right of entry or stay.[77]

In practice, applicants shall submit an application online or via an app,[78] providing the requested personal data.[79] The submitted data are then compared to the data present already in the ETIAS Central System, but also to data in SIS, EES, VIS, Eurodac, and Europol and Interpol data,[80] and to the ETIAS watchlist.[81] Some personal data are also compared to a series of **risk indicators**: that applies notably to date and place of birth, gender, nationality, first name(s) of the parents of the applicant, home address, education and occupation.[82]

If there is a hit – that is, a coincidence, this information is recorded in the application file.[83] If the hit is due to coincidence for data emanating from SIS, for instance because the applicant has been registered as deserving 'discreet checks or specific checks', a reference to this will be added to the application file.[84] Eventually, in case of hit, it is up to the ETIAS National Unit of the Member State identified as responsible shall to issue or refuse a travel authorisation.[85] When the hit is due to a coincidence with a risk indicator, *'the ETIAS National Unit of the Member State responsible shall assess the security, illegal immigration or high epidemic risk and decide whether to issue or refuse a travel authorisation'*, and *'(i)n no circumstances may the ETIAS National Unit of the Member State responsible take a decision automatically on the basis of a hit based on specific risk indicators'*, as that risk shall be assessed '*individually*'.[86]

Article 33 of the ETIAS Regulation explains that what the system foresees constitutes a type of '**profiling**' as defined in the GDPR: data provided by applicants shall be compared with *'specific risk*

[74] See Art. 1(1) of Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/226, 2OJ L 236, 19.9.2018, p. 1–71 (hereafter, 'ETIAS Regulation').

[75] Art. 1(2) of the ETIAS Regulation.

[76] Art. 83(1) of the ETIAS Regulation.

[77] Art. 36(6) of the ETIAS Regulation.

[78] Art. 15(1) of the ETIAS Regulation.

[79] Art. 17(2) of the ETIAS Regulation.

[80] Interpol data are data from the Interpol Travel Documents Associated with Notices database (TDAWN) and the Interpol Stolen and Lost Travel Document database (SLTD). In response to a question about concerns regarding the abuse for political purposes of the 'red notices' in those databases, the European Commission clarified in 2019 that the connection of to these databases shall be conditioned to Interpol providing necessary guarantees (Answer of Mr Avramopoulos on behalf of the European Commission, Question reference: E-000204/2019, 5 April 2019).

[81] The ETIAS watchlist '*shall consist of data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence'* (Art. 34(1) of the ETIAS Regulation). It is up to Europol or the Member State adding data to the ETIAS watchlist to assess *'whether the information is adequate, accurate and important enough to be included'* (Art. 35(1)(a)). They must also *'assess the potential impact of the data on the proportion of applications manually processed'*, an assessment presumably complex, and in any case to be automated, as eu-LISA is '*shall create a specific tool'* for the purpose of such assessment (Art. 35(2)), the technical specifications of which shall be determined by the European Commission by means of implementing acts (Art. 35(7)).

[82] Art. 20(5) of the ETIAS Regulation.

[83] Art. 20(7) of the ETIAS Regulation. In case of a hit, the ETIAS Central System consults the ETIAS Central Unit, which accesses the file and double checks its validity (Art. 22 of the ETIAS Regulation).

[84] Article 23 of the ETIAS Regulation.

[85] Article 26(2) of the ETIAS Regulation.

[86] Article 26(6) of the ETIAS Regulation.

indicators established by the ETIAS Central Unit' and *'pointing to security, illegal immigration or high epidemic risks'*. The **algorithm** enabling such profiling is called the ***'ETIAS screening rules'***.

It is the European Commission that shall further define, via a delegated act, what must be regarded as '*risks related to security or illegal immigration or a high epidemic risk'*.[87] Shall be taken into account for these purposes, notably, EEE statistics on abnormal rates of overstaying and refusals of entry '***for a specific group of*** *travellers'*, ETIAS statistics on abnormal rates of refusals of travel authorisations due to a security, illegal immigration or high epidemic risk '***associated with a specific group of travellers'***; statistics on correlations between data and overstaying by travellers or refusals of entry; *'information substantiated by factual and evidence-based elements'* provided by Member States on specific security risk indicators or threats, or on abnormal rates of overstaying and refusals of entry for '***a specific group of travellers'***, and information concerning specific high epidemic risks provided by Member States, as well as epidemiological surveillance information and risk assessments provided by the European Centre for Disease Prevention and Control (ECDC) and disease outbreaks reported by the WHO.

On the basis of the risks described will be determined '**risks indicators'**, which will then allow the ETIAS Central Unit to establish 'specific risk indicators consisting of a combination of data including one or several of' these categories of data: (a) age range, sex, nationality; (b) country and city of residence; (c) level of education (primary, secondary, higher or none); (d) current occupation (job group). The Regulation notes that these *'specific risk indicators shall be targeted and proportionate'*. It also forbids using risk indicators 'based solely on a person's sex or age', which leaves certain ambiguity as to whether would be permissible risk factors based on a combination of gender and age (such as 'women older than…', or 'men younger than…'). Risk indicators *'shall in no circumstances be based on information revealing a person's colour, race, ethnic or social origin, genetic features, language, political or any other opinion, religion or philosophical belief, trade union membership, membership of a national minority, property, birth, disability or sexual orientation'*.[88] They can nevertheless, as noted, be based for instance on level of education, or job group. The doors leading to possible undue discrimination are thus not fully closed.[89]

The ETIAS Information System, which includes the ETIAS Central System with the ETIAS watchlist, will be managed by **eu-LISA**.[90] The ETIAS Central Unit shall be in the hands of **Frontex**, the European Border and Coast Guard Agency.[91] It is this Central Unit at Frontex that is entrusted with '*defining, establishing, assessing ex ante, implementing, evaluating ex post, revising and deleting the specific* ***risk indicators'*** used to profile travellers, after consultation of the ETIAS Screening Board.[92] It is the same Central Unit that will be responsible for 'carrying out regular audits' of the implementation of the risk indicators, '*including by regularly assessing their impact on fundamental rights, in particular with regard to privacy and personal data protection'*.[93] The ETIAS Screening Board, which shall have an advisory function, is to work within Frontex and be composed of representatives of the different ETIAS National Units, Frontex itself, and **Europol**.[94] This advisory board may, if it deems it appropriate, *'consult the ETIAS Fundamental*

[87] Article 33(2) of the ETIAS Regulation.

[88] Article 33(5) of the ETIAS Regulation.

[89] Cf. also, in this sense: FGB, 2019, 33.

[90] Art. 6 of the ETIAS Regulation.

[91] Art. 7 of the ETIAS Regulation.

[92] Art. 7(2)(c) of the ETIAS Regulation. In the words of the EU FRA, the ETIAS system will rely on '(a)*n algorithm developed by Frontex'* (EU FRA, 2018a, 114).

[93] Art. 7(2)(e) of the ETIAS Regulation.

[94] Art. 9(1) of the ETIAS Regulation.

Rights Guidance Board[95] *on specific issues related to fundamental rights, in particular with regard to privacy, personal data protection and non-discrimination'.*[96]

Regarding the fundamental rights at stake, the ETIAS Regulation gives special prominence to the **right to non-discrimination**. Its Article 14 is titled 'Non-discrimination and fundamental rights' refers nevertheless, in addition to generally banning any personal data processing that might *'result in discrimination against third-country nationals on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation'*, the need to fully respect '***human dignity and integrity and fundamental rights****, including the right to respect for one's private life and to the protection of personal data'*. It also mentions that *'[p]articular attention shall be paid to children, the elderly and persons with a disability'*, and that *'[t]he best interests of the child shall be a primary consideration'*. It must be emphasised that this provision does not prevent, as such, the determination of risks indicators based on the fact that **certain 'groups of travellers' have been associated with certain higher associated risks**, be it security risks, a presumed propensity to 'overstay', or health risks.

The origins of ETIAS and EES can be traced back to the publication of the Smart Borders package by the European Commission in 2013. That package was followed by the launch of a Smart Borders pilot project, which included a testing phase of the proof of concept with operational tests at different border crossing points. The results of the project presented by eu-LISA echoed a small-scale survey conducted by the FRA, which revealed that a majority of third-country-national travellers had expressed concerns with regard to the reliability of the system, notably in relation to possible malfunctions, and the **difficulties related to rectifying any inaccurate data** (eu-LISA, 2015a, 12). The FRA survey results highlighted that the *'most likely implications of incorrect data in the Entry Exit system concern the risks of persons mistakenly flagged as over-stayers and the use that police, immigration or other officials may make of such information'*, potentially leading to *'the risk of being apprehended and detained'* (eu-LISA, 2015b, 307). The FRA also noted *'that automated systems could be programmed to identify individuals using sensitive data, such as race, ethnicity or health'* and stated that *'(m)easures to avoid* ***discriminatory profiling*** *are, therefore, required'* (idem).

The EDPS has warned that the ETIAS system *'could pose a risk to EU fundamental rights and freedoms'*, and that *'applying data protection safeguards effectively under ETIAS is particularly challenging',* as the planned data processing operations proposed involve exchanges of data between controllers who are subject to different EU data protection rules (EDPS, 2019, 22). It has also cautioned that there is a risk that *'individuals will find it* ***very difficult to exercise their data protection rights*** *effectively'* (idem).

Indeed, in this system the applicable data protection rules are **particularly complex**.[97] According to the ETIAS Regulation, the *'ETIAS Central Unit shall provide the general public with all relevant information*

[95] The ETIAS Fundamental Rights Guidance Board, entrusted with both an advisory and 'appraisal' function, is to consist of the Fundamental Rights Officer at Frontex and representatives of the consultative forum on fundamental rights of Frontex, the EDPS, the EDPB, and the EU FRA. The ETIAS Fundamental Rights Guidance Board shall perform regular appraisals and issue recommendations to the ETIAS Screening Board on the impact on fundamental rights of the processing of applications and profiling under ETIAS, *'in particular with regard to privacy, personal data protection and non-discrimination'*, have access to the mentioned audits, and publish a yearly report (Art. 9(5) of the ETIAS Regulation).

[96] Art. 9(5) of the ETIAS Regulation.

[97] Art. 56 of the ETIAS Regulation. In the context of ETIAS, the EU-DP Regulation shall apply to the processing of personal data by Frontex and eu-LISA; the GDPR shall apply to the processing of personal data by the ETIAS National Units regarding the assessment of applications by border authorities and by immigration authorities, but not when the processing is performed at the ETIAS National Units by competent authorities assessing the applications for the purposes of the prevention, detection or investigation of terrorist offences or other serious criminal offences, in which case the LED shall apply, although when the ETIAS National Unit actually decides on the travel authorisation as such, the GDPR shall always apply. Additionally, the LED shall apply when competent national authorities access the ETIAS Central System for the

in relation to applying for a travel authorisation',[98] which shall include references to the rights of data subjects under the EU-DP Regulation, the GDPR, the Europol Regulation and the LED.[99] It is not clear whether or how such general information will effectively make clear to which processing operations apply which rights exactly, and how applicable rights would be exercised.

The ETIAS Regulation states that, when individuals provide data to the system, they shall be informed of the existing procedures applicable to exercising their rights under Articles 13 to 16 of Regulation (EU) 2001/45 (now replaced by the EU-DPR), and Articles 15 to 18 of the GDPR. It is important to note that **this individual information does therefore not encompass any information about the rights to object to profiling** (Article 21) **and the rights related to automated decision-making** (Article 22) of the GDPR. Are also not mentioned the equivalent rights in the EU-DPR.[100] As a matter of fact, the ETIAS Regulation only explicitly refers about the possible exercise of the rights of access to, of rectification, of completion, of erasure of personal data and of restriction of processing, not to additional rights.[101]

purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences falling under their competence, and the Europol Regulation when it is Europol that accesses the data for equivalent purposes.

[98] Art. 71 of the ETIAS Regulation.

[99] Art. 71(q) of the ETIAS Regulation.

[100] The right to object and rights related to automated individual decisions were in Art. 18 and 19 of Regulation (EU) 2001/45.

[101] Art. 64 of the ETIAS Regulation.

4. IMPACT ON FUNDAMENTAL RIGHTS

Many efforts have already been devoted by a variety of actors to the identification of the impact on fundamental rights of AI systems broadly speaking. The European Commission's *White Paper on AI* notes that **AI *'can do harm'***, and goes on to note that harm might be immaterial, constituting for instance *'loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment'* (COM(2020) 65 final, 10). In an almost equally odd formulation, it also puts forward that the *'main risks related to the use of AI concern the application of rules designed to protect fundamental rights (including personal data and privacy protection and non-discrimination), as well as safety'* (idem, 10). The White Paper eventually concedes more straightforwardly that the *'use of AI can **affect the values on which the EU is founded** and lead to **breaches of fundamental rights'***, be it as a result from flaws in the overall design of AI systems, or from the use of data without correcting possible bias (ibid., 11).

The previous section already provided a series of examples in which developments related to AI systems in the field of law enforcement and justice have been regarded as having an impact on fundamental rights. This section looks closer at some of the issues that are most often raised. It does not attempt to connect specific types of impact with specific developments or areas, as issues – as well as the very rights affected - are generally intertwined: it has been pointed out, for instance, that shortcomings in predictive policing systems can *'create lasting consequences that will permeate throughout the criminal justice system and society more widely'* (Richardson, Schultz & Crawford, 226). It has been stated that lack of rules on automated profiling puts in danger the very notion of **freedom** (Gräf, 2017, 451).

In 2019, the Expert Committee on Human Rights Dimensions of Automated Data Processing and Different forms of AI (MSI-AUT), at the Council of Europe, argued that algorithmic decision-making systems that rely on data-driven profiling techniques may threaten **several human rights** including the rights to a fair trial and to due process, the rights to freedom of expression and information, the right to protection against discrimination in the exercise of rights and freedoms, and the rights to privacy and data protection (MSI-AUT, 2019, 8).

The Council of Europe *Recommendation on the human rights impacts of algorithmic systems* of April 2020 asserts that there are *'**significant human rights challenges** attached to the increasing reliance on algorithmic systems in everyday life, such as regarding the right to a fair trial; the right to privacy and data protection; the right to freedom of thought, conscience and religion; the right to freedom of expression; the right to freedom of assembly; the right to equal treatment; and economic and social rights'*.[102]

There is a general consensus on the fact that AI systems might be deployed in the field of law enforcement and criminal justice renders the possible impact on fundamental rights **even more significant**.[103] Finally, it is important to note that the focus on fundamental rights of this study shall not allow ignoring that the use of AI in this field can also raise other types of questions on their impact.[104]

[102] Recommendation CM/Rec(2020)1, Appendix, paragraph A.4.

[103] In this sense, Consideration of the impact of AI when used in criminal proceedings has for instance been described as *'even more important'* because of their direct impact on the individuals' personal freedoms (Ronsin & Lampos, 2018, 39).

[104] For instance, referring to the impact of predictive policing on police accountability: Hardyns & Rummens, 2017, 214.

4.1. Privacy and data protection

Although the rights to respect for private life and to the protection of personal data are recognised separately in the EU Charter of Fundamental Rights (in Article 7 and 8 respectively), under the ECHR data protection safeguards constitute a dimension of Article 8, on the right to respect for private life.

The European Court of Human Rights (ECtHR) case law on Article 8 of the ECHR and surveillance is extensive.[105] The Court has notably highlighted that the possibility of governments acquiring a detailed profile of the most intimate aspects of citizens' lives by **collating different types of data** '*may result in **particularly invasive interferences** with private life*', making explicit reference in this context *'to the views expressed by the Court of Justice of the European Union and the European Parliament'*.[106] In this sense, it is crucial to keep in mind that AI-related technologies such as facial recognition make it easier to link up personal data across a variety of surveillance systems, and to merge profiles (Datenethikkommission, 2019, 102).

A key issue for the ECtHR is the requirement of **foreseeability** of any surveillance measures. The case in *Liberty*[107] concerned the interception of communications and the subsequent use of 'filtering' techniques, consisting of an **automated sorting system**, operated under human control, aimed at selecting communications on the basis of what was occasionally referred to as '*keyword lists*', '*technical databases*', or '*The Dictionary*'.[108] The Court concluded that the applicable law at the relevant time did not indicate '*with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications*'.[109] In particular, the law failed to '*set out in a form accessible to the public any indication of **the procedure to be followed for selecting** for examination, sharing, storing and destroying intercepted material*', and thus the interference with the rights of the applicants under Article 8 of the ECHR could not be regarded as being '*in accordance with the law*'.[110]

Among the necessary safeguards regularly brought to the fore by the ECtHR stands out the **notification** of individuals subject to surveillance. Notification does not need to take place during a surveillance measure, but might take place afterwards, that is, as soon as it would not jeopardise the purpose of the surveillance measure. Such '*subsequent notification of surveillance measures is inextricably linked to the **effectiveness of remedies** before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers*', has stated the Court.[111]

The recent *Gaughran* judgment, of 13 February 2020,[112] concerned the retention of the DNA profile, fingerprints and photograph of a convicted person.[113] During the proceedings was discussed the

[105] The ECtHR has notably stressed, in relation to the fight against terrorism, that *'it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives'* (*Szabó and Vissy v. Hungary*, judgment of 12 January 2016, paragraph 68).

[106] *Szabó and Vissy*, paragraph 70, in relation to the *Digital Rights Ireland* judgment of the CJEU, and the EP Resolution on the US NSA surveillance programme, concerned inter alia with '*the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillanc e*' as perceived after the 2013 'Snowden revelations' (EP, 2014, 7).

[107] *Liberty and Others v. the United Kingdom*, judgment of 1 July 2008.

[108] Ibid., paragraph 43.

[109] Ibid., paragraph 69.

[110] Idem.

[111] *Weber and Saravia v.* Germany, 29 June 2006, paragraph 135.

[112] *Gaughran v. the United Kingdom*, Application no. 45245/15, ECLI:CE:ECHR:2020:0213JUD004524515, [2020] ECHR 144.

[113] Concretely, the indiscriminate nature of the powers to retain such data, without reference to the seriousness of the offence, or the need for indefinite retention, and in the absence of any real possibility of review. The ECtHR concluded that

question of whether the database storing the photographs could be accessed for the purposes of **facial recognition**, which apparently was not possible initially (paragraph 13), but was possible eventually (paragraphs 37, 68), as the data could be transferred to another database which did have facial recognition functionalities (paragraph 69). In the judgment, the ECtHR explicitly dismissed the argument submitted by the UK government according to which *'the more data is retained, the more crime is prevented*', noting that *'accepting such an argument in the context of a scheme of indefinite retention would in practice be tantamount to justifying the storage of information on the whole population and their deceased relatives, which would most definitely be excessive and irrelevant'* (paragraph 89).

Another very interesting judgment was issued earlier this year in the Netherlands, concerning **risk scoring by public authorities**. In February 2020, the Hague District Court delivered indeed a landmark ruling[114] about the Systemic Risk Indication (SyRI), a tool that the Dutch government had put in place to combat fraud. The proceedings had been initiated by several civil society groups, including the Dutch Section of the International Commission of Jurists and two private individuals. The Dutch legislator defined SyRI as a technical infrastructure with associated procedures through which data could be linked and analysed in order to generate risk reports. The existence of a risk report would mean that a person was deemed worthy of investigation with regard to possible fraud, perpetration of abuse, or non-compliance with legislation. [115]

In its judgement, the District Court noted that *'(n)ew technologies – including digital options to link files and analyse data with the help of algorithms – offer (more) possibilities for the government to exchange data among its authorities in the context of their statutory duty to prevent and combat fraud'*, and stated that *'those new technological possibilities to prevent and combat fraud should be used'* (paragraph 6.4). The Court, however, also observed that *'the development of new technologies also means that **the right to the protection of personal data increasingly gains in significance**'* (paragraph 6.5). As these technologies can interfere extensively with the lives of individuals, but it is difficult for individuals themselves to gauge such effect, the legislator bears a *'special responsibility'* when applying instruments such as SyRi (paragraph 6.85).

The Court's analysis led to the conclusion that SyRI legislation did not meet the requirement laid down in Article 8(2) of the ECHR that only permits interferences with the right to respect for private life that may be regarded as necessary in a democratic society, meaning that they should be necessary, proportionate and subsidiary in relation to the intended purpose. In this context, the Court noted that having examined the system in place in light of basic data processing principles established by the EU Charter and the GDPR, concretely the principles of transparency, purpose limitation and data minimisation, the system was ***'insufficiently transparent and verifiable'*** (paragraph 6.7).

In relation to these gaps, it noted that the legislation in place did not provide clear information on the factual data that could justifiably lead to the conclusion that there was an increased risk (paragraph 6.87), on the functioning of the risk model, on the risk analysis methods, the validation of the risk model

such retention could not be deemed proportionate in the circumstances at stake, which included the lack of any relevant safeguards and the absence of any real review, and thus amounted to a violation of Article 8 of the ECHR.

[114] Judgment of The Hague District Court of 5 February 2020, case number C/09/550982, ECLI:NL:RBDHA:2020:865. The judgment was notably celebrated to the extent that it stopped an initiative based on AI to *'detect fraud before it happens'*, and putting under surveillance for such purpose welfare claimants, including people in most vulnerable situations (Privacy International, 2020c).

[115] The instrument could be used at the request of certain government bodies or other bodies with a public function, such as municipal authorities, the Netherlands Tax and Customs Administration, the Social Affairs and Employment Inspectorate, or the Immigration and Naturalisation Service. Personal data processed by SyRI included data about work, education, taxes, property, housing, administrative measures and sanctions, civic integration, grounds for exclusion from benefits, pension, debt burden, reintegration, social benefits, and some health care insurance data.

and the verification of the risk indicators (paragraph 6.89). It was **unclear how data subjects** ***'could be able to defend themselves*** *against the fact that a risk report has been submitted'* about them, and in general know if the data about them were processed on correct grounds, going against the principle that *'a data subject must reasonably be able to track their personal data'* (paragraph 6.90).

In relation to challenges triggered by AI for privacy and data protection law, the European Commission's *White Paper on AI* argues that the GDPR and the e-Privacy Directive *'address these risks'*, but concedes *'there might be a need to examine whether AI systems* ***pose additional risks'*** (COM(2020) 65 final, 11).[116] It hints to the fact that persons will *'increasingly be subject to actions and decisions taken by or with the assistance of AI systems, which may sometimes be* ***difficult to understand and to effectively challenge*** *where necessary'*, but also that *'AI increases the possibilities to track and analyse the daily habits of people'*, including *'by state authorities or other entities for mass surveillance'* (idem). Moreover, *'AI may also be used to retrace and de-anonymise data about persons, creating new personal data protection risks even in respect to datasets that per se do not include personal data'*, states the EC.

4.2. Freedom of expression and information, and freedom of assembly and association

Some interferences with the rights to privacy and data protection might also simultaneously have a direct negative impact on the rights to freedom of expression and information (Article 11 of the EU Charter), and/or the right to freedom of assembly and association (Article 12 of the EU Charter), which might actually also been affected even when Article 7 or 8 of the EU Charter are not at stake. Notable challenges emerge when AI technologies are deployed to allow for the monitoring of public spaces – for instance, with **live facial recognition**, and the monitoring on communications, for instance in **social media**. Group anonymity can be under special pressure (EU FRA, 2019, 29).

The European Commission's *White Paper on AI* observes that AI-related processing of personal data can trigger new fundamental rights risks that affect rights different than the protection of personal data and privacy, such as the right to freedom of expression, and political freedoms – in particular when AI is used by online intermediaries to prioritise information and for content moderation (COM(2020) 65 final, 11).

This connects to concerns growing over the recent years on the use of automated processes of online content moderation, which can have a serious impact on the right to freedom of expression, but also on the right to non-discrimination.[117] These concerns are further exacerbated by a general problem of lack of transparency with regard to communication processes and the enforcement by Internet services of initiatives against disinformation (Van Hoboken et al., 2019, 124). It is important to stress that in relation to online misinformation often coexist calls to support AI tools for monitoring the veracity of information, and calls to reinforce the transparency of algorithms used, notably towards users (High-Level Group on Fake News and Online Disinformation, 2018).

4.3. Non-discrimination

The risks of bias and discrimination triggered by algorithmic decision-making are very frequently highlighted. The EU Fundamental Rights Agency noted that *'[d]irect or indirect discrimination through the use of algorithms using big data is increasingly considered as one of the most pressing challenges of the use of new technologies'* (EU FRA, 2018b, 3). The Council of Europe's *Recommendation on the Human*

[116] Specifically, in relation to the GDPR, the EC proclaims that it will *'be monitoring and assessing'* its application *'on a continuous basis'* (COM(2020) 65 final, 11).

[117] See, for instance: Committee of Experts on Quality Journalism in the Digital Age (MSI-JOQ), 2019, 15.

Rights Impacts of Algorithmic Systems of April 2020 observes that *'(m)any algorithmic systems use optimisation techniques'* which rely on prioritising certain values over others, which *'may generate adverse effects, particularly for **minorities and marginalised or disadvantaged groups'***.[118]

In relation to 'predictive policing', an important issue concerns the very pertinence of the possible inclusion of algorithmic variables such as criminal history and family background that can make the past behaviour of a certain group decide the fate of an individual, who is, nevertheless, *'a unique human being with a specific social background, education, skills, degree of guilt and distinctive motivations for committing a crime'* (Ronsin & Lampos, 2018, 39). This relates to the danger of creating *'echo chambers within which **pre-existing prejudice** may be further cemented'* (MSI-NET, 2018, 11), and in which individuals might end up being trapped without their knowledge.[119]

Additionally, researchers have shown how some systems used, notably in the US, are built on data produced during periods of flawed, racially biased, and even unlawful practices and policies ('dirty policing') which have inescapably shaped the very production of data, and raise the risk of creating inaccurate, skewed, or systemically biased data (**'dirty data'**) (Richardson, Schultz & Crawford, 2019, 192).[120] Authors have pointed out that the 'predictive policing' relying on historical crime data risk fuelling a cycle of distorted enforcement: as underlined by criminologists, crime reports and statistics gathered by the police are partly a record of law enforcement's responses to what happens in a community, and not necessarily an accurate record of all the crime that occurs in said community (Robinson & Koepke, 2016). Even 'predictive policing' systems which do not appear to use any personal data can have a negative impact. For instance, 'location-related risk prognoses' can lead to excessive police checks in certain neighbourhoods identified as hotspots and therefore to the ethnic or social profiling of population groups living there (Datenethikkommission, 2019, 215).

The General Findings section of the Stop Secret Surveillance Ordinance banning certain uses of facial recognition in San Francisco notes that *'[w]hile surveillance technology may threaten the privacy of all of us, surveillance efforts have **historically been used to intimidate and oppress certain communities and groups more than others**, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective'*.[121]

In relation to non-discrimination and equality issues, the Council of Europe Commissioner for Human Rights' has argued that *'Member states should **apply the highest level of scrutiny when using AI***

[118] Recommendation CM/Rec(2020)1, Appendix, paragraph A.7. In the already introduced judgement about the fraud detection SyRi system, the District Court of The Hague observed that *'given the large amounts of data that qualify for processing in SyRI, including special personal data, and the circumstance that risk profiles are used'*, there was *'a risk that SyRI inadvertently'* generated connections based on bias, for instance related to immigration background (paragraph 6.93). The Court also noted that the analysis of large data sets may lead to *'undesirable results, including unjustified exclusion or discrimination'* (paragraph 6.91), and echoed views supported by the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, according to which SyRI had a discriminatory and stigmatising effect, by spreading negative stereotyping to all occupants of neighbourhoods investigated as problem areas (paragraph 6.92). It was a major concern indeed of Alston that the system actually targeted poor neighbourhoods in the Netherlands, focusing attention on its inhabitants without any concrete suspicion of individual wrongdoing (UN Independent Human Rights Experts Press Service, 2020).

[119] See also: US Department of Justice, 2014, 22 (*'Likewise, the length of a defendant's prison term should not be adjusted simply because a statistical analysis has suggested that other offenders with similar demographic profiles will likely commit a future crime. Instead, equal justice demands that sentencing determinations be based primarily on the defendant's own conduct and criminal history'*).

[120] As a consequence, the systems informed by such data will be problematic unless they offer technical safeguards to adequately mitigate or segregate the 'dirty data', technical safeguards which have not, according to their analysis, be proven to exist (Richardson, Schultz & Crawford, 2019, 226). The researchers emphasised thus the need to develop reliable mechanisms for assessing the harms inherent in the use of historical police data, *'backed by strong public transparency and accountability measures'* (idem).

[121] Stop Secret Surveillance Ordinance, Section 1, § c).

***systems in the context of law enforcement**, especially when engaging in methods such as predictive or preventive policing'* (Council of Europe Commissioner for Human Rights, 11). The Commissioner advocates that *'such systems need to be independently audited prior to deployment for any discriminatory effect that could indicate de facto profiling of specific groups'*, and that *'(i)f any such effects are detected, the system cannot be used'*.

Bias and discrimination can surface at many levels in AI systems.[122] Research exposed, for instance, that commercial products classifying individuals into male and female using automated facial analysis algorithms suffered from substantial disparities in accuracy depending on the colour of the person's skin and their actual gender, with darker-skinned females being the most misclassified group (Buolamwini and Gebru, 2018).

The European Commission's *White Paper on AI* mentions **gender-based discrimination** as one of the main potential risks entailed by AI (COM(2020) 65 final, 1), and puts forward as a possible requirement to mitigate this risk the establishment of *'particular obligations to use data sets that are sufficiently representative, especially to ensure that all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination are appropriately reflected in those data sets'* (ibid. 19). Algorithmic discrimination, however, cannot be prevented or mitigated solely by regulating data sets, or by encouraging diversity in AI-related fields,[123] as it might also be triggered by the design of the algorithms, or the design of the system implementing it.

In relation to gender-based discrimination,[124] it is crucial to note that although EU data protection law has special rules to limit automated individual decision-making based on 'sensitive data',[125] a notion covering a variety of categories of data often used for discriminatory practices, these **data protection rules on 'special categories of data' do not cover data about gender**. Indeed, gender is not a category of data regarded by EU data protection law as deserving special protection as a 'special category of data',[126] and this despite the fact that there is a broad consensus on the reality of AI-related gender-based discrimination.[127]

[122] It is generally acknowledged that in many instances *'discrimination-by-computer does not rest on the use of overtly discriminatory criteria'* (Korff, 2012, 22), but rather *'creeps into the algorithms in much more insidious ways'* (ibid., 23).

[123] In its 2019 Communication on *Building Trust in Human-Centric Artificial Intelligence*, the European Commission noted that diversity in terms of gender *'should be ensured at every stage of AI development'* (COM(2019) 168 final, 2).

[124] In relation to gender discrimination, the *White Paper on AI* refers to preparation by the EC Advisory Committee on Equal Opportunities for Women and Men of an Opinion on Artificial Intelligence (ibid., 11), document which has in the meantime already been published (Advisory Committee on Equal Opportunities for Women and Men Opinion on Artificial Intelligence, 2020). This Opinion underscores the importance of the subject but advances as main recommendation to (further) *'(r)eflect and analyse at the EU and Member State level whether the existing legislative and institutional framework is equipped to deal with arising legal questions related to AI and gender equality and non-discrimination or whether there is any need for reform within the general framework for promotion and protection of human rights'* (ibid., 6). In this context, it notably alludes to the work of the High-Level Expert Group on AI, and concretely to its *Policy and Investment Recommendations for Trustworthy AI*, a document primarily associating gender issues to the need to tackle the gender gap in digital skills by improving education (AI HLEG, 2019b, 32-35). For a more detailed discussion on AI challenges and EU law, see, by the author: González Fuster, 2020.

[125] Article 9(1) of the GDPR lists the special categories of data (often referred to as 'sensitive data', as in Recital (10) of the GDPR): *'Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.'*

[126] Arguably, it is possible to defend that certain data processing practices which would lead to gender-based discrimination would infringe certain principles of data processing, such as the principle of fairness under the GDPR. Recital (71) of the GDPR proclaims that *'to ensure fair and transparent processing'*, the controller should *'secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, 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 that result in measures having such an effect'*.

[127] In this sense, for instance: COMEST, 2019, 21.

4.4. Right to an effective remedy and to a fair trial

AI-related technologies can affect effective remedy rights mainly in two ways: first, they can alter the nature of decisions that individuals might have to contest, bringing in novel challenges, second, they can affect the way in which individuals can actually contest against decisions through the judicial system. The former would refer for instance to the possibility of contesting a measure such a law enforcement intervention based on – or significantly affected by – facial recognition (EU FRA, 2019, 31). The latter concerns AI developments in the justice system itself.

The need to maintain AI 'under human control' is often evoked in policy discussions and the literature in this field. Making visible this control has implications in terms of bringing clarity to who is responsible for fundamental rights violations. The Council of Europe Commissioner for Human Rights' has stressed in this sense that *'states must establish **clear lines of responsibility for human rights violations** that may arise at various phases of an AI system lifecycle'* (Council of Europe Commissioner for Human Rights, 2019, 13). The Commissioner also noted that *'(a)nyone who claims to be a victim of a human rights violation arising from the development, deployment or use by a public or private entity of an AI system should be provided with an effective remedy before a national authority'*, adding that *'states should provide access to an effective remedy to those who suspect that they have been subjected to a measure that has been solely or significantly informed by the output of an AI system in a non-transparent manner and without their knowledge'* (idem).

The use of AI systems in the field of law enforcement and criminal justice can generally raise concerns related to the **fair trial standards** of Article 6 of the ECHR, in particular the presumption of innocence, the right to be informed promptly of the cause and nature of an accusation, the right to a fair hearing and the right to defend oneself in person (MSI-NET, 2018, 10).[128] The possible use of algorithmic systems in the context of justice has been highlighted as a sector in which these systems can **conflict with constitutionally protected rights of overriding importance**, meaning their use might, irrespective of possible protective measures, be permitted only under very restrictive conditions, or prohibited (Datenethikkommission, 2019, 212). In this sense, even legally non-binding proposals for decisions for judgments by algorithmic systems are generally to be regarded as highly problematic from the perspective of the parties concerned (ibid., 213).

4.5. Rights of the child

The EU Charter of Fundamental Rights devotes a special provision to the rights of the child (Article 24), which does not mean that children do not enjoy, additionally, all other fundamental rights enshrined in the EU Charter – such as, for instance, the right to personal data protection. The ECtHR has emphasised that the retention by public authorities of data related to innocent individuals *'may be especially harmful in the case of minors'*, *'given their special situation and the importance of their development and integration in society'*.[129]

There are multiple instances in which minors appear as the direct or indirect target of AI-related initiatives in the field of law enforcement.[130] An especially relevant issue concerns the collection of data

[128] Connected concerns might arise with respect to Article 5 of the ECHR, protecting against arbitrary deprivation of liberty, and Article 7 (no punishment without law) (MSI-NET, 2018, 10). Stressing that the use of AI in judicial systems can potentially interfere with the right to a fair trial, particularly with the right to a natural judge established by law, the right to an independent and impartial tribunal, and equality of arms in judicial proceedings: Ronsin & Lampos, 2018, 11.

[129] *Marper v. the United Kingdom*, judgment of 4 December 2008, applications 30562/04 and 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, paragraph 124.

[130] *The fact that data about minors might appear in law enforcement databases used for risk assessment has already been pointed out above, in relation to the Gangs Violence Matrix (GVM) case.*

about minors in the relation to **borders**. As regards to the processing of data of third-country nationals, and the automated assessment of risks associated to them, it has been pointed out that vulnerable groups, including refugees, face unique risks in case information about them would reach repressive governments in their countries, which might weaponized the data, putting individuals and their families at grave personal risk (Molnar & Gill, 2018, 43).

Developments such as the increased participation of minors in **demonstrations**, notably in relation to climate change (among other reasons, following the impulse of activist Greta Thunberg), trigger important questions as to how to protect specifically their rights in the face of the monitoring of such demonstrations, but also regarding possible online surveillance of the relevant organisational online activities.

The WEF *Framework for Responsible Limits on Facial Recognition* mentions explicitly children's rights (WEF, 2020). It states that although facial recognition should not exclude anyone and should always be accessible to and usable by all groups of people, '*there may be some instances, such as infants and children, in which an exception to this principle is appropriate and an alternative to facial identification should be offered'* (idem, 9).

According to the EU FRA, one of the opportunities for facial recognition in the field of law enforcement is to use it in order to help finding missing children (EU FRA, 2019, 18). It is very unclear, however, how could facial recognition be used for such purposes without disproportionately interfering with the fundamental rights of all children.

5. POLICY DEVELOPMENTS

This section presents relevant **policy considerations concerning the regulation of AI**, focusing on EU-level discussions but placing them in a broader context, notably by reference to Council of Europe developments. European policy initiatives are numerous, and it is beyond the scope of this study to review them all in detail.[131] European initiatives inscribe themselves in an even richer context of global initiatives and debates around AI,[132] which can be policy debates, but are also sometimes markedly more technical and academic.[133]

International initiatives with a strong focus on AI and law enforcement and criminal justice are comparatively less common than others. The Innovation Centre of Interpol and the United Nations Interregional Crime and Justice Research Institute (UNICRI) established a Centre for AI and Robotics, and convened a global meeting on the subject in 2018, leading to the publication of a report in 2019 (Interpol and UNICRI, 2019). The report pointed out that many countries were already then exploring the application of AI and robotics in the context of law enforcement, calling for discussions on their ethical use and social impact (ibid., vi).

Initiatives emanating from the **Council of Europe** are multiple. In 2017, the Parliamentary Assembly of the Council of Europe (PACE) adopted a *Recommendation on Technological Convergence, Artificial Intelligence and Human Rights*, whcih notably proposed that guidelines be drawn up on '*a common framework of standards to be complied with **when a court uses artificial intelligence**'* (point 9.2).

In 2018, the European Commission for the Efficiency of Justice (CEPEJ) adopted a ***European Ethical Charter on the Use of AI in the Judicial Systems and their Environment*** (CEPEJ, 2018), targeting public and private stakeholders responsible for the design and deployment of AI tools and services that involve the processing of judicial decisions and data, as well as public decision-makers in charge of the legislative or regulatory framework, of the development, audit or use of such tools and services. The Charter puts forward five principles: of respect of fundamental rights; of non-discrimination; of quality and security; of transparency, impartiality and fairness; and of 'under user control' (ibid., 5).

CEPEJ's *Ethical Charter* notes that judicial decision processing by AI could in civil, commercial and administrative matters help improving the predictability of the application of the law and consistency of court decisions, but that in criminal matters its '*use must be considered **with the greatest reservations** in order to prevent discrimination based on sensitive data, in conformity with the guarantees of a fair trial'* (ibid., 4).[134]

[131] As part of the background research for the Agency's project on 'Artificial intelligence (AI), Big Data and Fundamental Rights', the EU FRA has collected information on AI-related policy initiatives in EU Member States and beyond in the period 2016-2020. The collection (available here) currently includes over 290 initiatives. A 'policy initiative' was defined broadly to include a range of initiatives that could potentially contribute to policy making and standard setting in the area of AI. This could be, amongst others, actual (draft) legislation, soft-law, guidelines and recommendations on the use of AI, or reports that include conclusions with policy relevance. Civil society has also contributed to debates on the EU regulation of AI. Access Now Europe, for instance, stressed in 2019 that the EU must enforce and develop the highest human rights compliance standards for emerging technologies and AI systems that are designed, developed, or deployed in its territory (Access Now Europe, 2019, 5), and put forward a number of recommendations.

[132] Illustrating global interest in the issue, the Organisation for Economic Co-operation and Development (OECD) adopted in 2019 its Principles on AI. As another example, in the US, in 2016 the Obama White House's Office of Science and Technology launched a 'Preparing for the Future of Artificial Intelligence' initiative on the risks and benefits of AI. More information on the initiative's website.

[133] Coalescing for instance around the keywords Fairness, Accountability and Transparency (FAT).

[134] In relation to civil, commercial and administrative matters, a study accompanying the Charter highlights among the main guarantees to be reaffirmed the right of access to a court, the adversarial principle, equality of arms, the impartiality and independence of judges, and the right to counsel (Ronsin & Lampos, 2018, 34-35).

The Council of the Europe's Commissioner for Human Rights published in 2019 a Recommendation titled ***Unboxing Artificial Intelligence: 10 steps to Protect Human Rights*** which describes a number of steps for national authorities to maximise the potential of AI while preventing or mitigating the negative impact on people's lives and rights (Commissioner for Human Rights of the Council of Europe, 2019). It focuses on 10 key areas of action: human rights impact assessment, public consultations, human rights standards in the private sector, information and transparency, independent oversight, non-discrimination and equality, data protection and privacy, freedom of expression, freedom of assembly and association, and the right to work; access to remedies; and the promotion of AI literacy. The latter is explicitly connected to the need to **promote knowledge and understanding of AI** '*in government institutions, independent oversight bodies, national human rights structures, the judiciary and law enforcement'*, as well as the general public.[135]

In April 2020, the Council of Europe's Committee of Ministers adopted a *Recommendation on the human rights impacts of algorithmic systems*,[136] including ***Guidelines on addressing the human rights impacts of algorithmic systems***. The guidelines are designed to advise States, and public and private sector actors, in all their actions regarding the design, development and ongoing deployment of algorithmic systems, which, the document comments, are often *'neither clearly public nor clearly private'*.[137] To ensure that the human rights and fundamental freedoms of all individuals are effectively protected throughout the technological evolution, States '*shall refrain from violating human rights through the use of algorithmic systems, and shall* ***develop legislative and regulatory frameworks*** *that foster an environment where all actors respect and promote human rights and seek to prevent possible infringements'*.[138]

These 2020 *Guidelines* remark that algorithmic systems are sometimes '*employed* ***for predictive purposes*** *in the context of policing and border control, for the purposes of combatting money laundering and fraud'*.[139] They note that certain applications of algorithmic systems '*can prompt a particular, higher risk to human rights'*, for instance if used by States for their public service or public policy delivery. A similarly heightened risk, the Guidelines explain, '*ensues as a result of use in the context of decision-making processes, by either public authorities or private parties, in situations that carry particular weight or legal consequence*', and thus the use of algorithmic systems in the judicial field for the purpose of legal analysis, prediction or individual risk assessment must be introduced **with great care** and in conformity with the guarantees of a fair trial in Article 6 of the ECHR.[140] The term 'high risk' is introduced in this context to refer to *'the use of algorithmic systems in processes or decisions that can produce serious consequences for individuals or in situations where the lack of alternatives prompts a* ***particularly high***

[135] *The* Recommendation *Unboxing Artificial Intelligence* also contains a checklist to help implement the measures recommended in each key area. The 'do's' include, in relation to access to remedies, the need to assess whether laws 'provide an effective remedy to those claiming to be a victim of a human rights violation arising from the development, deployment or use of an AI system', the need to 'ensure that liability regimes clearly establish who is legally responsible for the whole spectrum of human rights violations that may occur at each phase of an AI system's lifecycle', but also to 'ensure that the judiciary and other relevant national authorities do not place inappropriate weight on the assumed/perceived accuracy or objectivity of an AI system, and that they provide an equality of arms between the victim and the defendant in cases challenging human rights violations caused by AI systems' (Commissioner for Human Rights of the Council of Europe, 2019, 23).

[136] *Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies.

[137] Appendix, paragraph A.12.

[138] Appendix, paragraph A.1. Concretely, as a first step, States should '*review their legislative frameworks and policies as well as their own practices with respect to the procurement, design, development and ongoing deployment of algorithmic systems to ensure that they are in line'* with the presented Guidelines (Recommendation, paragraph 1).

[139] Appendix, paragraph A.8.

[140] Ibid., paragraph A.11.

***probability of infringement of human rights**, including by introducing or amplifying **distributive injustice'**.*[141]

Still in the context of the Council of Europe, work on a Report on *Justice by Algorithm: The role of Artificial Intelligence in policing and criminal justice systems* was launched following a motion emanating from the Committee on Legal Affairs and Human Rights in 2018 of the Parliamentary Assembly (PACE).[142] The **Council of Europe's Ad hoc Committee on AI (CAHAI)** was set up in order to examine the advisability, feasibility and potential elements of a legal framework for the development, design and application of AI. The EU contributes to the CAHAI in an observer capacity.

5.1. Introduction

Recent years have been particularly rich in EU-level policy developments explicitly connected to AI. Especially since 2018, EU institutions have been delimiting the contours of what increasingly took the shape of an **AI agenda**.[143] This sub-section considers in more detail input to such debate on AI from the European Commission and the European Parliament,[144] and grants special attention to the role of ethics and the funding of AI in this context.

A number of other EU-level developments, not formally connected to AI policy discussions, might be regarded as having a potentially significant incidence on the impact AI on EU fundamental rights in the field of law enforcement and criminal justice. Generally speaking, it must be noted that over the recent years the **AFSJ** has witnessed **a major transformation in the ways it enables data processing**. This shift has been described as a movement from a 'silo-based approach', whereby different information systems operate as separate entities, and where a strict interpretation of the principle of purpose limitation is crucial, towards a new approach where **interoperability** is the keyword. Typically, data originally processed for non-law enforcement purposes might be made available for law enforcement processing. The Europol Regulation, the interoperability package, and the ETIAS Regulation have been singled out as examples of this trend (Coudert, 2017).

Regarding **facial recognition**, a particularly relevant development is the interest in facial recognition in the context of **Prüm** Decision,[145] based on the principle of cross-border searches. Coinciding with Prüm's 10th anniversary, the Council encouraged Member States experts *'to evaluate the Prüm workflow for further developments with a view to possible new biometric technologies, e.g. face recognition systems'* (General Secretariat of the Council, 2018). Some partially publicly available documents[146] echo the establishment of a Focus Group on Face Recognition connected to the Council's Working Party on

[141] Idem. The Guidelines submit that *'States should take a precautionary approach and require the refusal of certain systems when their deployment leads to high risks of irreversible damage or when, due to their opacity, human control and oversight become impractical'* (Ibid., paragraph A.15).

[142] Motion for a Recommendation *Justice by algorithm – The role of Artificial Intelligence in policing and criminal justice systems*, Doc. 14628, 26 September 2018.

[143] In a way that was not dissimilar to the progressive emergence, bridging Digital Single Market and Security policies, of an EU cybersecurity agenda and policy.

[144] Other EU institutions are also playing an important role in the area. In February 2019, the Council adopted conclusions on AI calling for *'stronger development, deployment and uptake of Artificial Intelligence applications in all economic sectors, with the aim of making Europe a global leader in Artificial Intelligence'*, while stressing *'the need for establishing appropriate cyber security requirements for AI and for ensuring accountability and the protection of fundamental rights'* (Council of the EU, 6177/19, 7 and 8).

[145] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11. Prüm is one of the EU AFSJ data processing initiatives that has since the start being openly about data processing for law enforcement purposes, based on the development of decentralised tools for information exchange.

[146] Available public information about these developments is limited, and some available insights are tributary to leaks (cf., e.g., Campbell and Jones, 2020).

Information Exchange and Data Protection (DAPIX) (Presidency of the Council, 2019). Other documents evoke the consideration by said Focus Group of the preliminary results of a feasibility study on amending the current Prüm legislation, a study carried out by a consultancy firm on behalf of the European Commission which presumably presented as a proposal the possibility to create a central database for facial recognition in the EU – a proposal nonetheless rejected by the experts of the Focus Group, notably on the basis of its lack of operational benefits (Austrian Delegation to the Council, 2019, 9).

Some EU-funded research efforts are already moving in this direction.[147] The *Towards the European Level Exchange of Facial Images* (TELEFI) Project,[148] according to its website, is undertaking a study on how facial recognition is currently being used for the investigation of crime across EU Member States, giving particular consideration *'to the potential for implementing the exchange of facial images within the Prüm framework'*. The project focuses on the use of facial recognition in criminal investigations, but is carrying out research on a variety of databases in order to *'provide a future opportunity to consider whether these additional databases could be legally cross-used for criminal investigations/proceedings and transnational data exchange'*.[149]

5.2. European Commission

AI-related developments have until now primarily inscribed themselves within **Digital Single Market** discussions.[150] In its 2018 Work Programme, the European Commission announced under the heading '*A connected Digital Single Market'* its commitment to *'look to make the most of artificial intelligence that will increasingly play a role in our economies and societies'* (COM(2017) 650 final, 5).[151] In the 2020 Work Programme it was under the heading ***'A Europe fit for the Digital Age'*** that the Commission announced it was going to put forward a White Paper on Artificial Intelligence *'to support its development and uptake and ensure full respect of European values and fundamental rights'*, in view of '*(m)aking the most of artificial intelligence'* while establishing *'an ecosystem of trust to ensure it develops within clearly defined ethical boundaries'* (COM(2020) 37 final, 4). The establishment of '*A connected Digital Single Market'* was one of the priority police areas of Jean-Claude Juncker (Juncker, 2014, 6); the Digital Single Market has been defined as *'one in which the free movement of goods, persons, services and capital is ensured'* (COM(2015) 192 final, 2).[152]

[147] As noted for instance in: Monroy, 2020.

[148] Funding via the European Union Internal Security Fund-Police (Grant Agreement: 821284), duration from January 2019 to September 2020; more information on the TELEFI website.

[149] See 'About TELEFI Project'.

[150] The European Commission's involvement in supporting AI and AI policy encompasses many initiatives. For instance, it hosts and facilitates the European AI Alliance, where representatives of businesses, consumer organisations, trade unions, and other representatives of civil society bodies, are supposed to interact with the experts of the (AI HLEG) in a forum-style setting, and to feed into the stakeholders dialogue. Additionally, a pilot project was commissioned by the European Commission on algorithmic awareness building, following calls by the European Parliament, and was active in 2018 (see the website: https://algoaware.lpweb.eu/). In 2018, the European Commission launched AI Watch, a knowledge service to monitor the development, uptake and impact of AI for Europe. AI Watch is supported by the Joint Research Centre (JRC) of the European Commission in collaboration with the Directorate-General for Communications Networks, Content and Technology (DG CONNECT). AI Watch has announced it monitors also the usage and impact of AI technologies used in public services and in public organizations.

[151] The 2019 Work Programme noted, under the same title, that the European Commission would continue to '*work on the emerging challenge of Artificial Intelligence by enabling coordinated action across the European Union'* (COM(2018) 800 final, 3).

[152] It expanded on the fact that already in 1995 the EU legislator had established the principle of the free movement of personal data inside the EU (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50), notably to, in 2018, establish the free movement of non-personal data.

These constitute only a few of the highlights in a rather long history of support by the European Commission of **data processing as key enabler of European economy's growth**, the origins of which can be traced back to the 1970s.[153] The year 2018 was particularly prolific in relation to AI policy. The European Commission published a Communication embracing the notion of 'human-centric AI' and a three-pronged approach to boost the EU's technological and industrial capacity and AI uptake across the economy; prepare for socio-economic changes, and ensure an appropriate ethical and legal framework (COM(2018) 237 final). The Commission also developed together with Member States a coordinated plan on AI to create synergies, pool data, and increase joint investments (COM(2018) 795 final).

Even if previously the term AI as such had not been particularly prominent, there is a clear continuity with prior discussion around 'big data'. In its 2014 Communication ***Towards a Thriving Data-driven Economy***, the European Commission described '**big data**' as referring *'to large amounts of different types of data produced with high velocity from a high number of various types of sources'*, and observed that handling such data required *'new tools and methods, such as powerful processors, software and algorithms'* (COM(2014) 442 final, 4), noting also the advent of *'a new industrial revolution driven by digital data, computation and automation'* (ibid., 2).

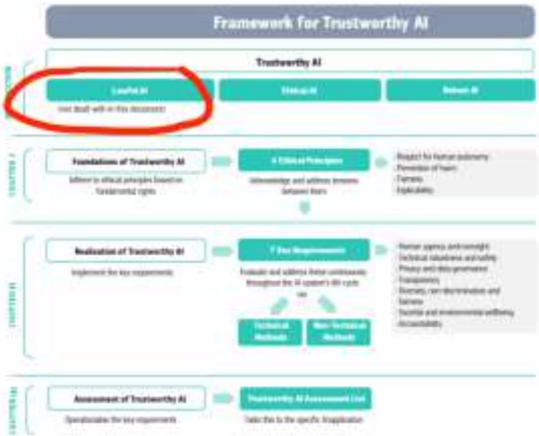
In the 2019 Communication ***Building Trust in Human-Centric Artificial Intelligence***, the 'trust' mentioned in the title was overtly connected by the European Commission primarily to testing *'the practical implementation of ethical guidance for AI development and use'* (COM(2019) 168 final, 1). AI applications, stated the EC, *'should not only be consistent with the law, but also adhere to **ethical principles'***, and respect citizens' fundamental rights. The exact relations between these ideas were not clearly defined, but the inferred point of action was that *'there is a need for **ethics** guidelines that build on the existing regulatory framework'*, which is why the EC had set up a High-Level Expert Group tasked with drafting such guidelines (COM(2019) 168 final, 2).

The **High-Level Expert Group on Artificial Intelligence** (AI HLEG) had delivered in 2018 the first draft of its *Ethics Guidelines on Artificial Intelligence*, and published a revised document in 2019 following an open consultation which generated extensive feedback (AI HLEG, 2019a). The AI HLEG *Ethics Guidelines on AI* list requirements of 'trustworthy' AI systems, requirements which were put through a piloting process expected to conclude with the publication of a further revised document in 2020.

The role granted to law and fundamental rights in the AI HLEG's *Ethics Guidelines* is relatively elusive, and potentially misleading. The AI HLEG indeed declares that '**trustworthy AI**' should be **lawful, ethical**, **robust**, but notes that its *Ethics Guidelines* do *'not explicitly deal'* with the lawfulness component of trustworthy AI, opting instead to offer guidance on the ethical and robustness components (AI HLEG, 2019a, 2). A footnote further clarifies that the Guidelines' statements are *'not meant to provide legal advice or to offer guidance on compliance with applicable laws'*, while however, at the same time, acknowledging that *'many of these statements are to some extent already reflected in existing* laws' (idem). Later in the document, another footnote insists on the fact that it *'does not provide any advice on ensuring legal compliance (lawful AI)'* (ibid., 3). The Figure below illustrates how the AI HLEG openly affirms to put aside considerations of lawfulness in relation to AI.

[153] Already then, as the European Commission delineated the contours of its seminal Community data policy, it observed however that the 'data banks' under development could held police data and that, therefore, rules on access to such information were 'vital' (SEC(73) 4300 final, 13).

Figure 2: AI HLEG Framework for Trustworthy AI


Framework for Trustworthy AI
Trustworthy AI
Lawful AI
Ethical AI
Robust AI
Foundations of Trustworthy AI
4 Ethical Principles
Realisation of Trustworthy AI
7 Key Requirements
Technical Methods
Non-Technical Methods
Assessment of Trustworthy AI
Trustworthy AI Assessment List

Source: Figure from: AI HLEG, 2019a, 8. Circle in red by the author of this study.

There is no real solid substantive justification in the AI HLEG Guidelines themselves as to why no consideration would be given by this group to the requirements of 'lawful AI'. Somehow puzzlingly, the same Expert Group insists on the fact that '**trustworthy AI**' would be crucial to reap the benefits of AI '*in a way that is aligned with our foundational values of respect for human rights, democracy and the rule of law*' (AI HLEG, 2019a, 4). More confusingly, the same document *Ethics Guidelines* eventually announces it shall '*briefly touch upon*' the requirements of 'lawful AI', only to note that that it proceeds on the assumption that all relevant legal rights and obligations, which are not detailed, *'remain mandatory and must be duly observed'* and that the full realisation of ethical and robust AI may (or may not) '*go beyond existing legal obligations'* (ibid., 6), whichever they might be.

The most ambivalent choice of the *Ethics Guidelines*, nevertheless, is probably the identification of what are called the 'foundations of trustworthy AI' with a 'fundamental-rights based approach' (AI HLEG, 2019a, 7). Such as a proposal is accompanied by a footnote arguing that fundamental rights '*underpin the legally enforceable rights guaranteed by the EU Treaties and the EU Charter'*,[154] and are as such an element of 'lawful AI' to the extent that they are legally binding. However, the footnote maintains that fundamental rights can '*also be understood as reflecting special moral entitlements of all individuals arising by virtue of their humanity, regardless of their legally binding status*', and in that sense they also form part of 'ethical AI' (idem). As an inescapable logical consequence, it must be understood that **whenever the AI HLEG alludes to fundamental rights, it might or might not be referring to rights that are legally binding**. To the extent that it openly asserts to focus on 'ethical AI' as opposed to 'lawful AI', as a matter of fact most often fundamental rights as discussed by the AI HLEG might not necessarily be related to legally binding rights.[155] This is, from a legal perspective, peculiarly **troublesome**.

This takes place, as a matter of fact, amidst a constant vagueness about the distinction between 'ethical and robust AI', on the one hand, and 'lawful AI', on the other. In this sense, the seven key requirements finally put forward by the AI HLEG, supposedly unconcerned with 'lawful AI', are not deprived of references to legal instruments such as the GDPR (AI HLEG, 2019a, 17). Relegating elemental considerations around the basics of regulation of AI to multiple footnotes, and sustaining an almost constant blurring between what is lawful and what is ethical, the AI HLEG *Ethics Guidelines*

[154] The exact ambitions of this sentence, according to which fundamental rights underpin the fundamental rights established by the EU Charter of Fundamental Rights, remains unclear.

[155] As confirmed notably in AI HLEG, 2019a, 10.

unfortunately did not, in any case, help establishing an intelligible policy debate about the regulation of AI in the EU and its impact on (legally binding) fundamental rights.

The European Commission officially welcomed the work of the AI HLEG in its 2019 Communication *Building Trust in Human-Centric Artificial Intelligence*, in which however it omitted the fact that the AI HLEG *Ethics Guidelines* **had not discussed applicable law as such**. On the contrary, according to the EC the Guidelines had identified key requirements of 'trustworthy AI' based on its three components: **law**, ethical principles, and robustness (COM(2019) 168 final, 3). Furthermore, the EC even celebrated that many already existing EU law provisions *'of course already reflect one or several of these key requirements, for example safety, personal data protection, privacy'* (idem). This only added an extra layer of unclarity to whether and how the discussed ethical guidelines might or not be something different from legal rules. Further entertaining the ambiguity, the EC stated that *'(e)thical AI is a win-win proposition'* visibly linking it to *'(g)uaranteeing the respect for fundamental values and rights'* (COM(2019) 168 final, 8).

In 2019, in *A Union that strives for more: My agenda for Europe*, the by then candidate to the Presidency of the European Commission announced that under in her *'first 100 days in office'* as President she would *'put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence'* (Von der Leyen, 2019, 13). This was a key element of the top-level ambition of moving towards a *'A Europe fit for the digital age'*, in the sense of a Europe *'grasping the opportunities from the digital age within safe and ethical boundaries'* (idem). The plan of putting forward legislation in 100 days eventually evolved into putting forward a White Paper. In the weeks preceding its publication, there were rumours that the document might have considered as a possibility working towards a general ban of facial recognition in public areas, an idea that was eventually not featured as such in the published document (Yun Chee, 2020).

The European Commission published its ***White Paper on Artificial Intelligence*** on 19 February 2020 (COM(2020) 65 final). The White Paper proclaims that '*(g)iven the major impact that AI can have on our society and the need to build trust, it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection'* (ibid., 2). The future regulatory framework for AI in Europe, states the document, shall create an ***'ecosystem of trust'*** which constitutes ***'a policy objective in itself'*** (ibid., 3), which might, nevertheless, also contribute to other objectives such as creating *'a frictionless internal market for the further development and uptake of AI as well as strengthening Europe's industrial basis in AI'* (ibid. 10).

The announced regulatory framework shall notably ensure socially *'optimal outcomes and compliance with EU legislation, principles and values'*, an objective *'particularly relevant in areas where citizens' rights may be most directly affected, for example in* ***the case of AI applications for law enforcement and the judiciary'*** (ibid., 10). It shall be built on an examination of *'whether current legislation is able to address the risks of AI and can be effectively enforced, whether adaptations of the legislation are needed, or whether new legislation is needed'* (idem). One of the ways in which AI can bring benefits to Europe is, according to the White Paper, *'by* ***equipping law enforcement authorities with appropriate tools*** *to ensure the security of citizens'* (COM(2020) 65 final,2).

The White Paper on AI was presented together with two Communications, one on *Shaping Europe's Digital Future* in general, and another specifically about the *European Data Strategy.*[156] The Communication ***Shaping Europe's digital future*** connected the advent of a 'true digital

[156] The White Paper was also accompanied by a Report of the European Commission on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (COM(2020) 64 final).

transformation' to the need to make sure that digital applications and products are secure, an aim to be pursued *inter alia* by '***ensuring that law enforcement and judicial authorities can work effectively by developing new tools*** *to use against cybercriminals'* (COM(2020) 67 final, 5).

The Communication on a ***European Data Strategy*** (COM(2020) 66 final) further develops policies around data that have been over the years connected to notions such as a 'common European data space', the 'data strategy', the 'data economy', originally '*embedded in the Digital Single Market strategy'* and later '*applied to AI'* (Penner, 2019). It addresses restrictions on the free flow of data, including legal barriers on the location of data for storage and/or processing purposes, and a series of issues relating to data such as ownership, access, reuse, portability and liability. It emphasises the value of the availability of data (COM(2020) 66, 6). Noting that data might be used '*for the public good'*, it states that data '*created by society'* can, '*where necessary and proportionate, to ensure more efficient fight against crime'* (idem). As part of such Strategy, the European Commission intents to fund the establishment of EU-wide common, interoperable data spaces in strategic sectors (ibid., 16), such as '**common European data spaces for public administration'** aimed *inter alia* at **addressing law enforcement needs** and at enabling '*innovative 'gov tech', 'reg tech' and 'legal tech' applications supporting practitioners as well as other services of public interest'* (ibid., 22).

According to the European Commission's June 2020 Communication on the two years of application of the GDPR, the *White Paper on AI* '***opened up a public debate*** *on the specific circumstances, if any, which might justify the use of artificial intelligence for remote biometric identification purposes (such as facial recognition) in public places, and on common safeguards'* (COM(2020) 264 final, 10).

Reactions to the White Paper had been varied. Some, for instance, questioned whether the confirmed commitment towards European values is compatible with keeping pace with international competitors such as the US and China (Scott, 2020). The **Secretariat of the Council of Europe** submitted responses to the European Commission's consultation on the White Paper, in which was highlighted that the 'framework of trust' to be created between all stakeholders should have as **a prerequisite** the respect for regulatory frameworks and fundamental rights, and the meaningful implementation of the relevant existing regulation (Secretariat of the Council of Europe, 2020, 5). The document comes back to the issue of fundamental rights to state that AI-related research efforts should '*focus on fundamental rights so as to promote the development of legislation, ethical standards and guidelines on AI compliant with such rights'*, and promote digital humanities (ibid., 7).

The **EDPS** formally reacted to the *White Paper on AI* on 29 June 2020 (EDPS, Opinion 4/2020). In its Opinion, the EDPS notably stressed that any future regulatory framework for AI shall apply '*to both to EU Member States and to EU institutions, offices, bodies and agencies'* (ibid. 2). Regarding the substance, the EDPS called in particular for an approach to determining the level of risk in the use of AI applications that should be both '*more robust and more nuanced'* (ibid., 11), in the sense that it should be layered instead of an 'all or nothing' approach (ibid., 13).

The EDPS Opinion also supports the idea of '*a* ***moratorium*** *on the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals'* (idem). The moratorium shall coincide with work towards '*appropriate safeguards, including a comprehensive legal framework in place to guarantee the proportionality of the respective technologies and systems for the specific use case'* (idem). In the EDPS' view, some AI applications, such as for instance live facial recognition, '*interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms'* (ibid., 7), implying they might not be permissible at all. The EPDS centres part of its analysis around **Remote Biometric Identification (RBI)**, which might rely or not on AI, and includes live facial recognition in public places but is not limited to it. These systems, the EDPS observes, '*are easily hidden, frictionless, often are presented as mere "experiment" but could easily be turned into ubiquitous and pervasive surveillance complex*' (ibid., 20).[157]

As regards to **predictive policing**, the EDPS states that it '*may have negative effects like over- policing on collectives, as well as on individuals*', and calls in this context to devising '*inclusive governance models which would empower organizations representing civil society (e.g. NGOs and other non-profit associations) so they also can help assessing the impact of AI applications on specific collectives and the society in general*' (ibid., 9). In relation to **non-discrimination**, the EDPS stresses that AI might have specific risks for 'vulnerable groups', and puts forward that in the absence of a formally adopted legal definition of vulnerable groups, a 'context-specific, pragmatic approach' shall be endorsed, to encompass '*children, elderly, and persons with disabilities, ethnic minorities or historically marginalised groups, women, LGBTQIA+ communities, workers and others at risk of exclusion*' (ibid., 21). Finally, in its reaction to the *White Paper* the EDPS also observed that some AI-related measures put forward in the context of the fight against the pandemic represent in themselves, or enable, a kind of 'function creep' which can have '*a chilling effect in democratic societies*' (ibid., 20).

Regarding EU data protection law, the European Commission's Communication marking the two years of application of the GDPR echoed the ongoing bilateral dialogues between the EC and Member States to ensure the appropriate implementation on the GDPR (COM(2020) 264 final, 14). The Communication notably acknowledged that private companies active in the European market might be called to **share data for law enforcement purposes** '*on the basis of a legitimate request*', and that such requests might lead to facing conflicts of law or generating **tensions with EU fundamental rights**.[158]

In April 2020, the European Commission made public the establishment of an Expert Group on Artificial Intelligence in the domain of Home Affairs to assist European Commission's DG for Migration and Home Affairs in the preparation of legislative proposals or **policy initiatives concerning AI in the domain of Home Affairs**; to establish cooperation and coordination between the Commission and Member States or stakeholders on questions relating to the implementation of EU legislation, programmes and policies in the field of AI in the domain of Home Affairs; and to bring about an exchange of experience and good practice in the field of AI in the domain of Home Affairs. It will be composed of representatives of Member States' and Schengen Associated Countries' authorities.[159]

[157] The significance of the challenges connected to RBI do not exclude, the EDPS nuanced, that similar technologies not aimed at identifying individuals can also raise serious concerns: that would be the case, for instance, of real time so-called 'detection' of emotions (EDPS, Opinion 4/2020, 20).

[158] The European Commission announced in this context that '*[t]o improve such transfers, the Commission is committed to develop appropriate legal frameworks with its international partners to avoid conflicts of law and support effective forms of cooperation, notably by providing for the necessary data protection safeguards, and thereby contribute to a more effective fight against crime*' (COM(2020) 264 final, 13). This notably translates into a commitment '*to assess how cooperation between private operators and law enforcement authorities could be facilitated, including by negotiating bilateral and multilateral frameworks for data transfers in the context of access by foreign criminal law enforcement authorities to electronic evidence*' (ibid., 18).

[159] Commission Expert Group on Artificial Intelligence in the domain of Home Affairs (ref. E03727 at the Register of Commission's Expert Groups and Other Similar Entities).

5.3. European Parliament

The European Parliament has been considering AI in multiple policy contexts – for instance, it adopted in February 2020 a *Resolution on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services* (P9_TA(2020)0032).[160]

In 2017 the European Parliament adopted a ***Resolution on fundamental rights implications of big data*** (on privacy, data protection, non-discrimination, security and law-enforcement), which called on the European Commission, the EDPB and other DPAs *'to issue guidelines, recommendations and best practices in order to further* ***specify the criteria and conditions for decisions based on profiling and the use of big data for law enforcement purposes'*** (EP, P8_TA(2017)0076, paragraph 25). The Resolution emphasised that *'the trust of citizens in digital services can be seriously undermined by government mass surveillance activities and the unwarranted accessing of commercial and other personal data by law enforcement authorities'* (ibid., paragraph 27), and stated that *'legislation permitting public authorities to gain access to the contents of electronic communications on a generalised basis must be regarded as compromising the essence'* of the right to privacy as established by Article 7 of the EU Charter (ibid., paragraph 28).[161]

The European Parliament has also witnessed a series of specific initiatives related to AI. The creation of budget for an Observatory on Artificial Intelligence was requested but rejected by the EP Committee on Budgets, leading later to concerns regarding the possible continuation of such initiative as a working group (EP, P9_TA-PROV(2020)0084, paragraph 27).

Ongoing work on a ***Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters*** (LIBE, 2020/2016(INI) was already mentioned. The document notably includes a call for a **moratorium on the deployment of facial recognition systems for law enforcement**, as well as a set of recommendations including the establishment of compulsory fundamental rights impact assessments, and the creation of a clear and fair legal regime for assigning legal responsibility for the potential adverse consequences produced by advanced digital technologies in the field.

On 18 June 2020, the European Parliament took the decision to set up a special committee on artificial intelligence in a digital age. The committee is due to begin its activities after the summer recess.

5.4. The role of ethics

The softening, or blurring, of boundaries between **law and ethics** described in relation to the *Ethics Guidelines* of the AI HLEG is not exclusive to the Group's endeavours, but rather a more pervasive trend in European discussions around digital regulation. In this context, a certain type of *'post-compliance ethics'*, opening up a space characterised as potentially *'unlimited'*, has been particularly noticeable in EU-level debates over the past years (Floridi, 2018). The intersections between data, ethics, AI and EU policy are complex, and do not systematically help delineating a consistent picture of what could be a

[160] Its paragraph 10 includes a reference to the legal profession: (the EP) *'(u)nderlines that while automated decision-making processes can improve the efficiency and accuracy of services, humans must always be ultimately responsible for, and able to overrule, decisions that are taken in the context of professional services such as the medical, legal and accounting professions, and for the banking sector; recalls the importance of supervision or independent oversight by qualified professionals in cases of automated decision-making where legitimate public interests are at stake'*.

[161] The Resolution also echoed the fact that *'intelligence services of third countries and Member States have increasingly been relying on the processing and analytics of such* [big data] *datasets, which are either not covered by any legal framework or, most recently, have been the subject of legislation the compatibility of which with Union primary and secondary law raises concerns and is yet to be ascertained'* (EP, P8_TA(2017)0076, paragraph D).

role of ethics in this field, in particular in relation to the (certainly different, possibly complementary) role of law.[162]

Work on AI and ethics is globally **extremely voluminous**, resulting from many years of '*intense efforts*' of a '*diverse set of stakeholders*' including both public authorities and private companies (Jobin, Ienca & Vayena, 2019). In terms of content, although relevant documents typically mobilise coinciding terminology – referring for instance to transparency, justice and fairness, responsibility, freedom and autonomy, trust, dignity, sustainability, or solidarity – this does not necessarily mean that there is a consensus on the meaning of these notions, or their implications (idem). AlgorithmWatch launched an AI Ethics Guidelines Global Inventory to compile frameworks and guidelines that seek to set out principles of how systems for automated decision-making can be developed and implemented 'ethically', and it compiles more than 160 guidelines.[163]

Ethics already played a significant role in global discussions around **big data** a few years ago, especially in relation to research.[164] Discussions on AI and ethics have surfaced in all fields.[165] An additional, whole strand of literature regards the possibility to embed ethics requirements into the design of AI systems.[166] According to some authors, the focus on ethics as the main prism through which to address AI's risks might only constitute 'a phase', preceding a different, regulatory phase (Lapinski, 2018). There is any case scepticism about the added value of 'the move to ethical principles' in terms of measurable effects, and also because they often lack enforcement mechanisms (AI Now Institute, 2018, 9). The frequent use of the word 'ethics' in connection with algorithms may be, it has been stated, '*an indicator for a tactical move by some actors who want to avoid strict regulation by pointing to non-formal normative concepts*' (MSI-NET, 2018, 42).[167] Some initiatives have framed themselves visibly as different from ethics-centred approaches – for instance, by openly embracing human rights considerations as prime focus.[168]

A number of European **national AI strategies** devote particular attention to ethical issues (Van Roy, 2020; regarding Cyprus, 20; Czech Republic, 24; Finland, 35; France, 36; Germany, 42). In Denmark, the

[162] According to a 2019 guide published by The Alan Turing Institute, '*AI ethics is a set of values, principles, and techniques that employ widely accepted standards of right and wrong to guide moral conduct in the development and use of AI technologies*' (Leslie, 2019, 3). The main connection between AI ethics and the law would be that AI ethics moral vocabulary draws on human rights discourse, which in its turn '*draws inspiration from the UN Declaration of Human Rights*' (ibid., 8). The guide calls for such development to be accompanied by an 'ethical platform' requiring a set of actionable principles, called FAST Track Principles, composed of four notions: Fairness, Accountability, Sustainability, and Transparency (ibid., 7).

[163] As explained by two contributors of the team working on such inventory, '*AI ethics*' as found in that database '*are often positioned between instrumental-economic and ethical perspectives. AI ethics in this sense is rather business ethics*' (Gießler & Haas, 2020).

[164] This was notably the case after the so-called 'emotional contagion Facebook scandal' of 2013, regarding the algorithmic manipulation of emotions of Facebook users for research purposes. At that time, US scholars were particularly interested in the fact that the research had not been subject to standard research ethics procedures because it was not publicly funded but corporate research, which in the US has strong legal implications insofar as research ethics are concerned. Thus, there were notably calls to bring closer research ethics and corporate ethics, concretely around data and big data practices (boyd, 2016).

[165] In February 2020, for instance, the US Department of Defense adopted five principles for the 'ethical development' of AI capabilities (US Department of Defense, 2020). As another example, in 2019 the French Armed Forces Ministry published a report of the AI Task Force calling for the establishment of a ministerial committee to, in particular but not exclusively, on the ethical issues that AI applications in the military sphere could raise (AI Task Force, 2019).

[166] Which is connected to be question of whether one can somehow operationalise in mathematical or computational terms 'ethics requirements'; arguing for instance that designing AI systems, as well as designing fairness requirements into them, is not a purely mathematical exercise but involves a series of important trade-offs, very much like human decision-making in the criminal justice system in general: McNamara, et al, 2019,112.

[167] In some cases, embracing ethics in this context is openly portrayed as a way further promoting the spread of AI, to be endorsed by those who '*favour security over interests such as privacy*' (McCarthy, 2019).

[168] Such is the case for example of the *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems* of May 2018.

government emphasised the need to develop and use AI '*within the relevant legislation, and with respect for the rights of citizens*', which would inter alia require that '*businesses and the public authorities must have strong focus on **data ethics'*** (Ministry of Finance and Ministry of Industry, Business and Financial Affairs of the Danish Government, 2019, 8). In Belgium, AI 4 Belgium published a report noting it is '*important to introduce ethical guidelines to support the development, deployment and use of AI*' (AI 4 Belgium Coalition, 2019, 14), and suggested *'a new role could be created to monitor compliance with these ethical principles: **the digital ethicist'*** (ibid., 15).

In 2018, Germany's Federal Government set up the Data Ethics Commission *(*Datenethikkommission), and mandated it to develop ethical benchmarks and guidelines as well as specific recommendations for action, aiming at protecting individuals, preserving social cohesion, and safeguarding and promoting prosperity in the information age, to tackle concretely a number of key questions clustered around algorithm-based decision-making (ADM), AI and data (Datenethikkommission, 2019, 13). The Data Ethics Commission openly stated that, in particular for issues with heightened implications for fundamental rights, regulation is necessary and **cannot be replaced by ethical principles** (ibid., 15).

In many cases, there is currently at least some degree of **ambiguity** when **EU institutions** touch upon the role of law and ethics in relation to AI. In the *A Union that strives for more* 2019 document of Von der Leyen, there was much emphasis on the importance of '*ethical boundaries*' and the need for a coordinated '*European approach on the human and ethical implications of Artificial Intelligence*', together with a call for legislation (Von der Leyen, 2019, 6). There was also a reference to preserving 'ethical standards' that appear to have a connection with the GDPR, as if, perhaps, the GDPR was about ethical standards (idem).

The role of ethics in this field as inferred from the contributions of the European Parliament is variable. In the European Parliament's 2017 ***Resolution on Fundamental Rights Implications of Big Data***, it called for '*Member States' law enforcement authorities that make use of data analytics to uphold the highest standards of **ethics** when analysing data*', as a way of contributing to non-discriminatory practices (P8_TA(2017)0076, paragraph 32). The Resolution adopted by the European Parliament on 12 February 2020, on automated decision-making processes and consumer protection, describes '*ethical guidance, such as the principles adopted by the Commission's High- Level Expert Group on Artificial Intelligence*' as a '*starting-point*' (paragraph D) to move towards '*a common EU approach to the development of automated decision-making processes' that would help secure the benefits of those processes and mitigate the risks across the EU, avoid fragmentation of the internal market, and enable the EU to better promote its approach and its values around the world*' (paragraph E). The EDPS, which has as main tasks to monitor compliance and provide guidance about data protection law, devoted in the past years particular attention to 'digital ethics'.[169] Somehow as a counterpoint, the Council discussed the possibility to actively encourage the *'development of **AI ethics into a discipline of its own'*** (Council of the EU, 12224/19, 3).

The ambivalent relation between ethics and fundamental rights also surfaces in other *fora*, including the Council of Europe. The 2018 CEPEJ's ***European Ethical Charter on the Use of AI in the Judicial Systems and their Environment*** (CEPEJ, 2018) sets out as first principle the 'Principle of respect for fundamental rights', described as ensuring '*that the design and implementation of artificial intelligence*

[169] The report published in 2018 by its Ethics Advisory Group (EAG) listed a series of challenges that such Group regarded as relevant for digital ethics, among which was mentioned 'predictive policing'. The EAG observed 'predictive policing' '*comes with a new set of challenges*', such as limited predictability of law enforcement decision-making processes, or risks of bias (EAG, 2018, 29). '*Police may risk becoming more interested in the patterns than in the substance, more concerned with the prediction than in observable facts*', noted the EAG (idem). The report was prepared *'in anticipation of the'* GDPR (ibid., 7), but does not mention the LED, or make any other particular reference to data processing for law enforcement purposes.

tools and services are compatible with fundamental rights' (ibid., 6). The ***Guidelines on Artificial Intelligence and Data Protection*** published in January 2019 by the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) refer to 'ethical values' as an element of the 'wider view' to be adopted when considering the possible outcomes of data processing. In this sense, the Guidelines state such wider view should *'consider not only human rights and fundamental freedoms but also the functioning of democracies and social and ethical values'* (T-PD(2019)01, 1).

The Preamble to the Council of Europe's *Recommendation on the Human Rights Impacts of Algorithmic Systems* of April 2020 points out that even if *'ongoing public and private sector initiatives intended to develop ethical guidelines and standards for the design, development and ongoing deployment of algorithmic systems'* constitute *'a highly welcome recognition of the risks that these systems pose for normative values'*, these initiatives nevertheless *'do not relieve Council of Europe member States of their obligations as primary guardians'* of the **ECHR**.

5.5. EU-funded support of AI

Much of the EU support of AI and related technologies takes place through funding. EU funds support AI, including law enforcement related AI, through a variety of means – some of them are openly related to research in this area, while others do not primarily have a research component. Investment in AI has been a priority for the European Commission, which **doubled its investments in AI** in Horizon 2020 and had put forward plans for significant investment from Horizon Europe and the Digital Europe Programme (COM(2019) 168 final, 1).[170]

Some AI-related funded projects deployed with the support of EU funding have generated controversy. It is the case, for instance, of a 'smart policing' project launched in 2019 by the Greek Police in cooperation with a telecommunications operator, involving the delivery of 'smart devices' with integrated software enabling facial recognition and automated fingerprint identification, among other functionalities, supported by Internal Security Fund (ISF) 2014-2020 of the European Commission (Chelioudakis, 2020). Another example is the City of Marseille's project called *'Big Data de la tranquillité publique'*, launched in 2016 to foster the collection of data from institutional partners in order to prevent certain events before they would happen, co-funded by the EU through the European Regional Development Fund (**FEDER**) scheme[171] - developments currently at the centre of local contestation against surveillance, notably organised by the NGO La Quadrature du Net (Meaker 2020).

Current funding of AI research in this field is marked by two issues with potentially problematic fundamental rights implications: first, the **lack of solid specific guidance accompanying the submission and selection** of proposals, and, second, the serious limitations regarding the **transparency of funded research**, including, most notably, information about their compliance with legal and ethics requirements.

Regarding the first point, research proposals are typically submitted, in addition to a scientific evaluation, to an 'Ethics Appraisal Procedure'[172] appraising compliance with '**ethics requirements'**. These requirements refer to a series of issues globally entrenched in research ethics, among which the European Commission places **data protection**. In a gesture that can result in more confusion than

[170] The President of the European Commission stated before her nomination that she would *'make sure that we prioritise investments in Artificial Intelligence, both through the Multiannual Financial Framework and through the increased use of public-private partnerships'* (Von der Leyen, 2019, 13).

[171] See page *Le Big Data de la tranquillité publique*.

[172] This is the procedure applied for Horizon 2020 projects, more information on the relevant webpage.

clarity, 'ethics reviewers' carrying out reviews for the European Commission may decide, during the relevant procedures put in place, to incorporate into the grant agreement to be signed by the relevant consortium a series of 'ethics requirements', some of which might refer, for instance, to the necessity to comply with specific GDPR provisions, despite this being, as such, a legal obligation.

Although some of the ethics reviewers might have been recruited on the grounds of their data protection expertise, not all of them necessarily have precise knowledge on EU data protection law, and in any case they are systematically invited to attempt to agree, if possible, on a consensual decision to pick up certain pre-written statements on '**data protection requirements'**. The wording of these requirements appears to be a legacy of past review activities, and might in many cases not be fully applicable to the case at stake, as the actual obligations of the relevant data controllers and processors are to be analysed taking into account the specific national laws applicable to them. As a result, the utility of the whole exercise is questionable, and can often result in perplexity among the selected applicants, nevertheless faced sometimes with no other option than to attempt to comply with the imposed 'ethics requirements' resulting from this procedure in order to obtain the sought funding.

The most detailed advice made available to applicants suffers from a number of **weaknesses**. Guidance is provided in a document presented as 'reference document' on 'ethics and data protection' at the relevant website, but bearing a disclaimer according to which *'it does not constitute official EU guidance'* (EC, 2018, 1). The document insists on the need to rely on the consent of data subjects to process personal data about them,[173] which might actually not be the case. Another statement warns that *'if your proposal uses data processed or provided by authorities responsible for preventing, investigating, detecting or prosecuting criminal offences, Directive (EU) 2016/680 may also apply'*: actually that would be the case only if said authorities would be, in the context of the research project, carrying out activities for the mentioned purposes – if processing data for research purposes, it is still the GDPR that applies.[174]

That document also proclaims that*: 'If the goal of the project is to **develop surveillance technologies or techniques for law enforcement purposes**, your proposal should explain why the surveillance can be deemed necessary and proportionate in a democratic society, in accordance with EU values, principles and laws'* (EC, 2018). This issue, however, is not mentioned at all in relevant 'ethics issues check-list', and is also absent from the guidance provided to applicant to self-assess compliance with ethics requirements (EC, *Horizon 2020 Programme Guidance,* 2019). It is thus unclear how often it might be considered, if at all.

Regarding transparency of funded research, it must be noted that generally research proposals foresee the publication of some results, while planning for others a 'confidential' or 'EU restricted' status. Confidentiality of some results is often necessary, especially in the realm of security. The European Commission has however, in principle, the ability to impose that some of the activities and results of the funded project shall be open to public scrutiny. The European Commission has published guidance, prepared by Directorate-General for Migration and Home Affairs (DG HOME), which advised for the **classification of certain types of research and research results** in certain specific fields, such as for instance border security, in Horizon 2020 projects (EC, H2020 Programme Guidance, Version 2.2, 2020).

Such guidance does not mention any need to classify deliverables with information regarding legal and ethical standards. It actually also does not recommend classifying research in the domain of

[173] In this sense: *"Whenever you collect personal data directly from research participants, you must seek their informed consent by means of a procedure that meets the minimum standards of the GDPR"* (EC, 2018, 10). As it is widely known and has recently been again confirmed by the EDPB, the GDPR foresee different legal grounds on which research can be based (EDPB, Guidelines 03/2020, 2020).

[174] See Art. 2(1) of LED.

'intelligent surveillance', defined as '*the use of pattern recognition and other artificial intelligence techniques to analyse data obtained from more conventional security devices, with the aim of identifying behaviour deemed suspicious or anomalous with regard to the given legal and social context*'.[175]

What is striking insofar as EU-funded research on AI and security is concerned, however, is the lack of public information available on many of the funded projects, including on their **compliance with legal and ethics standards**. In this sense, the NGO Privacy International has argued that it '*is unclear how some of the funded projects being supported – such as those aimed at monitoring potential migrants to Europe – comply with EU rules, including on data protection*' (Privacy International, 2020a).

A particularly commented case was the Horizon 2020-funded project iBorderCtrl, aiming at creating an automated border security system incorporating 'automated deception detection', in spite of concerns about the scientific and ethical opportunity of such an approach. Also commented was the fact that despite the existence of concerns around the project many of its results remained hidden from public scrutiny (Leufer & Jansen, 2020). In May 2020, results of funded activities such as deliverables on the 'ethics of profiling' and 'the risk of stigmatization of individuals', or a 'EU wide legal and ethical review' are described at the project website as submitted to the European Commission but 'confidential', and thus not available to other researchers or the public.[176]

Lack of transparency can dramatically affect the trust of the population in the role of the EU in supporting AI in law enforcement and criminal justice.

Example 1: Real-time surveillance of public space

The project *Artificial Intelligence and Computer Vision for Real-time Diagnosis of Public Spaces* was funded in 2019 (H2020-SMEInst-2018-2020-1) to bring to the market a solution for **real time diagnosis of public spaces**, including the Urban Security Eye product line, targeting detection of terrorism, suspicious behaviour and insecure spots (EC, 2019, 90). The website of the coordinator claims that their products are '***so anonymous that GDPR becomes irrelevant***', but does not appear to offer any specific further clarification about legal and ethical implications of their work.

Example 2: Autonomous robots at the borders

The project ROBORDER aims at developing fully-functional autonomous **border surveillance systems** with **unmanned mobile robots including** aerial, water surface, underwater and ground solutions, with multimodal sensors. An '*heterogenous robot system*' shall be enhanced with detection capabilities for early identification of criminal activities at border and coastal areas. All deliverables concerned with ethics issues, including an '***Ethical Code***', appear to have been regarded as **fully confidential** and thus not accessible even partially according to the project website.

[175] The document does however note that although *'(c)lassification is currently not foreseen in this area'*, *'(t)his may change in the future'* (EC, H2020 Programme Guidance, Version 2.2, 2020).
[176] See the list of project deliverables here.

Example 3: Pre-occurring crime prediction and prevention

The InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services (CONNEXIONS) project describes itself as a solution encompassing the entire lifecycle of law enforcement operations, from ‘pre-occurrence crime prevention and prevention’ to ‘post-occurrence’ investigations. It appears to be concerned *inter alia* with multilingual automatic speech recognition of online material, and its use cases cover threats at public events such as football matches and festivals. According to its description at the Community Research and Development Information Service (CORDIS), the project, launched in September 2018, planned to ‘***adopt ethics and privacy by-design principles***’. No public deliverable appears to be available online in July 2020.

Example 4: Intelligent dialogue-empowered bots for early terrorist detection

TENSOR was a Horizon 2020 project was about developing a platform to help law enforcement agencies in the early detection of terrorist activities, radicalisation and recruitment – as explained on the project website. The platform was described as integrating ‘a set of **automated and semi-automated tools’**, including tools for the monitoring of online content but also ‘Internet penetration through intelligent dialogue-empowered bots’. A whole funded Work Package of the funded project was devoted to developing ‘the legal and ethical framework that will underpin’ such developments ; the project’s flyer asserted such work would *‘ensure that the solutions are **shaped by the privacy and data protection laws that protect the freedom of citizens** across Europe in their use of the internet’*. The project ended in November 2019. In July 2020, the project website announced as publicly available a total of four deliverables, none of them about the relevant legal and ethical framework, and **none of them actually downloadable** (see here).

6. COVID-19 OUTBREAK RESPONSE

The COVID-19 outbreak has had dramatic effects all over the world, and the responses to the crisis have triggered, at least potentially, **a variety of fundamental rights implications**. This section highlights some of the issues that appear as particularly relevant for a reflection on the impact on EU fundamental rights of AI in the field of law enforcement and criminal justice. The section focuses on two main themes: first, data-driven responses which have a major impact on the collection and processing – and potentially, availability - of data about individuals, and, second, initiatives undertaken directly by law enforcement authorities.

Many other issues might nevertheless influence developments in this field. Among them, there are efforts to accelerate the **digitalisation of public services**, and most notably the administration of justice. [177] The work of law enforcement has also been affected, notably by changing the prominence of certain types of crimes (such as, for instance, those related to domestic abuse). According to Interpol, '*cybercriminals are capitalizing on the anxiety caused by COVID-19 through various cyberattacks such as data-harvesting malware, ransomware, online scams and phishing*' (Interpol, 2020).

There has been a general trend to adopt or re-purpose technological solutions, pursuing multiple objectives, and building on quick adaptations by private companies (Gershgorn, 2020). Generally speaking, **the processing of data and surveillance practices** have increased around the world. In China, facial recognition software was adapted to detect the wearing of masks already in February (Jain, 2020);[178] in Moscow, facial recognition would have been used to enforce quarantine obligations since March (Habersetzer, 2020). In the US, the company Athena Security started marketing also in March a 'Fever Detection COVID19 Screening System' allegedly detecting fever 'through AI', although not using facial recognition as such (Cox, 2020).[179] In Singapore, municipal authorities decided to test a four-legged robot marketed by the US robotics design company as a tool to remind park visitors to keep a safe distance from one another, notably by broadcasting pre-recorded messages (Vincent, 2020).

Some measures have directly concerned issues related to **automated decision-making**. In April 2020, US civil society organisations expressed concerns with the use of the risk assessment tool Pattern, originally conceived to attribute scores on 'general recidivism', in order to determine which incarcerated individuals would receive 'priority treatment' in transfer and release decisions in the context of the Covid-19 outbreak (Cook, 2020). The organisations expressed that algorithmic recidivism risk scores should not inform assessment of medical risk, or play any role in determining who receives access to adequate healthcare. They also stressed that the tool had been previously assessed as '*likely to perpetuate racial disparity in decision-making*', and suffered from '*assumptions built into its design*

[177] Already at the beginning of April 2020, the EU Justice ministers agreed to intensify efforts to guarantee the digitalisation of their judicial procedures, as well as a secure digital channel for all judicial cooperation procedures (European Commission, 7 April 2020). Quick moves to online solutions created problems in some Member States; in Italy, for instance, an association of criminal lawyers requested the involvement of the Italian DPA to assess the implications of a forced switch of certain criminal justice procedures to digital issues, in particular through the use of Skype for Business e Teams, both of Microsoft Corporation (Unione Camere Penali Italiane, 2020).

[178] Facial recognition is as such not necessarily prevented by the fact that individuals might wear masks, as technology providers have worked to offer products designed for this scenario (Yang, 2020).

[179] According to the media, Clearview AI would be currently proposing to public authorities in the US 'contact tracing' solutions using images from surveillance cameras, through which it would be able to gather information on the identity of individuals' contacts (Thomsen, 2020; cf. also Grind, McMillan & Mathews, 2020). It is unclear whether what is being offered would be real-time facial recognition technology for purposes of contact tracing in response to the COVID-19 pandemic (Markey, 2020).

encode bias against Black people, Latino people, poor people, unhoused people, and people with mental illness' (ibid., 2).

The possibility of put mobile **applications ('apps')** at use sparked remarkable creativity in many. *'We've had ideas for apps from people as young as 14 or 15, from individuals, from small start-up companies, from huge, globally-based companies'*, declared on 25 March 2020 the Executive Director of the WHO Health Emergencies Programme, Michael Ryan, before adding: *'It's been the most outstanding and most amazing outpouring of support and collaboration that I have seen in my career'* (WHO, 2020, 1). Multiple types of apps have been developed in response to the outbreak, including self-assessment apps, apps for the collection of data for the purposes of research, apps related to the notion of 'immunity certificates', and 'contact tracing' apps, as well as apps combining different of these functions.[180] Deployed apps have been made available to the public accompanied by a variety of measures and approaches to the management of the crisis.[181]

Systems monitoring the temperature of individuals have proliferated. Italy, for instance, adopted in March 2020 rules foreseeing the real-time measurement of temperature to access a variety of spaces, for workers but also for others.[182]

While data processing and surveillance measures where increasing, some fundamental rights safeguards were put under pressure. In May 2020, the Hungarian government suspended the application of a number of GDPR data subject rights as part of the coronavirus emergency measures, and established time limits for the exercise of remedy rights, including the right to lodge a complaint and the right to an effective judicial remedy as guaranteed by the GDPR. Civil society representatives contacted the EDPB, calling on them to ask the European Commission to launch an infringement procedure against Hungary (Massé, 2020, 16).[183]

Generally speaking, assessments of Covid-19-related developments are cautious, and place emphasis on the need to monitor them closely. Some have warned about the possible strengthening of *'the temptation of adopting technology-enabled mass surveillance to secure society'* (Renda, 2020). In its reaction to the European Commission's *White Paper on AI*, the EDPS has observed that some AI-related measures put forward in the context of the fight against the pandemic represent in themselves, or enable, a kind of 'function creep' which can have *'a chilling effect in democratic societies'* (EDPS, Opinion 4/2020, 20).

[180] In some cases, apps made available were pre-existing apps, re-purposed in the context of the outbreak. In Colombia, the NGO Fundación Karisma analysed the three local apps and discovered an important set of technical vulnerabilities, as well as serious gaps in terms of transparency (Labarthe & Velásquez, 2020b). The NGO pointed out for instance that the most popular app was actually built on an app developed by Brazil to track in 2014 other diseases such as dengue and zika, and requested data not relevant in the current situation (Labarthe & Velásquez, 2020a).

[181] South Korea, for instance, put in place a 'track and trace' model relying on testing and rigorous isolation, as well as public dissemination of person's private lives. Public authorities have indeed publicly shared information on the movements of persons tested infected, presumably to help others assess whether they might be infected. In practice, this has led to problematic disclosures, as well as instances of blackmail (Kim, 2020a). Eventually, media reports linking a series of infections to gay clubs generated fear of a backlash against an already discriminated community (Kim, 2020b).

[182] See: Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro tra Governo e parti sociali del 14 marzo 2020, section 2.

[183] The EDPB discussed the issue on 8 May 2020 (EDPB, 8 May 2020), but concluded that further explanation was necessary and has thus requested that the Hungarian Supervisory Authority to provide further details on the scope and the duration of the measures, as well as its opinion on the necessity and proportionality of these measures.

6.1. Data-driven responses

An important dimension of EU's response to the outbreak might be described as data-driven, or data-based (Zanfir-Fortuna, 2020).[184] Concretely, two major types of data-driven measures have been discussed and supported at EU level: the use of **location data**, as made available by telecommunication providers to public authorities, and the use of ***ad hoc* apps**,[185] notably apps relying on **'contact tracing'** by Bluetooth.

On 24 March 2020, the European Commission revealed that it had explored with telecommunications operators the possibility to collaborate to tackle the coronavirus outbreak. Thierry Breton, the Internal Market Commissioner, had discussed with the heads of Europe's telecommunications companies and the Global System for Mobile Communications association (GSMA) to explore options for sharing geolocation metadata in order to map and forecast the spread of the virus.[186] Many Member States would have taken location-tracking measures in response to the spread of the coronavirus disease, mainly by working with telecommunications companies to map population movements using so-called 'anonymised' and aggregated location data (Dumbrava, 2020).

The Dutch DPA is strongly critical of the very possibility to regard as 'anonymous' the location data at stake. In this sense, it made public in April 2020 a document on the anonymity of aggregated telco location data which concluded that *'(a)nonimisation* [sic] *is hard. Anonimisation* [sic] *of location data is almost undoable'* (Autoriteit Persoonsgegevens, 2020). When announcing that the EDPB had published guidance on the matter, the Dutch DPA stressed again the importance it attaches to this message.[187] The concerns of the Dutch DPA with inappropriate anonymisation are *inter alia* connected to **the possible interest in any stored data by the police** and security services (DutchNews, 2020).

On 8 April 2020, the European Commission published a ***Recommendation on a common Union toolbox*** *for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data* (C(2020) 2296 final), which argued it *'is therefore necessary to develop a common approach to the use of digital technologies and data in response to the current crisis'* (ibid., 1).

Regarding **location data**, it explained that *'(c)ertain companies* ***including telecommunications providers and major technology platforms*** *have published or made available to public authorities* ***anonymised and aggregated location data'*** (ibid., 5). Regarding apps, it noted that, since the beginning of the COVID-19 crisis, a variety of mobile applications had been developed, *'some of them by public authorities'* (ibid., 3), and highlighted that *'w)arning and tracing applications are useful for Member States for* ***contact tracing*** *purposes and can play an important role in containment during de-escalation scenarios'* (ibid., 4). The Recommendation already hinted that *'(i)n order to detect proximity*

[184] An overview of key documents adopted by EU institutions, agencies and bodies on these matters can be found at VUB's Data Protection Law & Covid-19 Observatory; concretely, here.

[185] China had originally deployed a system based on creating a record of 'proximity events' between individuals through mobile apps, and displaying a green, amber or red code with direct implications in terms of movement restrictions (Ferretti et al., 2020, 5). Building on such an initiative, researchers proposed an algorithmic-based model that would enable automated recommendations of *'risk-stratified quarantine and physical distancing measures'*, as well as eventual refinements of the algorithm to recommend, for instance, the quarantining of whole households or areas (ibid.). The researchers advocating for this approach put forward a series of possible requirements to obtain the trust of the population, among which can be cited *'the use of a transparent and auditable algorithm'* and *'careful oversight of and effective protections around the uses of data'* (ibid.).

[186] The European Commission's approach to the use of telecommunications data has been described as being 'largely based' on an approach put in place since mid-March by the Belgian 'Data against Corona' taskforce (Mascini, 2020). It relies on telecommunication operators making available location data about mobile phone users in order to elaborate pictures of mobility trends, using data regarded as 'anonymised'.

[187] By linking to its own document in a footnote; see the announcement.

encounters between users of different contact tracing applications (a scenario most likely to happen among people moving across national/regional borders), interoperability between applications should be envisaged' (ibid., 5).[188]

For these reasons, the European Commission announced the setting up 'a process for developing a common approach, referred to as a Toolbox, to use digital means to address the crisis', with a focus on a '***pan-European approach for the use of mobile applications***, *coordinated at Union level'*, and '***a common scheme for using anonymized and aggregated data*** *on mobility of populations'* (ibid., 7).

The use of contact tracing apps is sometimes referred to as **'digital' contact tracing**, opposed to **'manual' contact tracing**. The latter would describe the practice of re-tracing, with the help of humans, the contacts of infected persons or persons that are believed to have potentially been infected. The former would consist of automatically keeping track of 'proximity events' between devices, that might be regarded as probably implying a contact. Both so-called 'manual' and 'digital' contact tracing trigger significant interferences with the fundamental rights to privacy and data protection, in a number of ways.[189] 'Manual' contact tracing, in this sense, typically implies that the person infected is faced with a set of particularly intrusive questions about who they have met in the days before the testing, and which kind of contacts they have had, if any.

From an EU fundamental rights perspective, the main difference between so-called 'manual' and 'digital' contact tracing is that the first one is based on an intervention that takes place, in principle, only after a person has been tested positive, or presents symptoms, or has been in contact with somebody who has been tested positive or has symptoms – and thus affecting what could be regarded, in principle, a minority of persons.[190] Contact tracing via apps, in contrast, **aims at initiating the collection of data about the relevant contacts of individuals in advance**, targeting a number of persons as broad as possible, in a **preventive approach**, *'just in case'* information about such contacts would later be of use. From this standpoint, in principle **the more individuals are engaged in data collection, the better**. Some experts have claimed in this sense that the desirable goal from this perspective would be *'an app that is used by every inhabitant of all the European Member States'* (Mascini, 2020).

Developments at EU followed then quickly, notably with the adoption on 15 April 2020 of a document titled ***Common EU Toolbox for Member States: Mobile applications to support contact tracing in the EU's fight against COVID-19*** by the eHealth Network (eHealth Network, 15 April 2020).[191] On 16 April

[188] The Recommendations specified: *'National health authorities supervising infection transmission chains should be able to exchange interoperable information about users that have tested positive with other Member States or regions in order to address cross-border transmission chains'* (C(2020) 2296 final). There have been concerns that some Member States might require from those wishing to enter into their own territory the use of a certain app, or of a certain types of apps, and which might require that at least nearby Member States offer appropriate solutions. These concerns were for instance voiced at parliamentary discussions in Luxembourg (Chambre des Députés du Grand-Duché de Luxembourg, 2020).

[189] Additionally, one does not exclude the other, and the distinction between them might be occasionally blurred, for instance when public authorities publicly call the population, including healthy individuals, to keep personal diaries of all the persons they encounter. In the EU, DPAs have already provided some input of proposed or deployed apps, as well as on 'manual' contact tracing. The Belgian DPA, in a first analysis of a legislative proposal concerning the creation of a database for public authorities in the context of the fight against the spread of COVID-19, primarily concerned with 'manual' contact tracing but potentially also of use for app-enabled contact tracing, concluded that the proposal did not satisfy the requirements of necessity and proportionality (Belgian DPA, 29 April 2020).

[190] Depending of the level of spread, such minority might constitute a large number of persons; all these persons, nevertheless, would correspond to a category of persons deemed of interest for a special reason.

[191] The eHealth Network is a voluntary network providing a platform of Member States' competent authorities dealing with digital health; it was set up under Directive 2011/24/EU, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45–65.

2020, the European Commission published its ***Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*** (C/2020/2523).

In a **Resolution** adopted on **17 April 2020**, the **European Parliament** made reference to what was then the European Commission's *'plan to call on telecoms providers to hand over anonymised and aggregated data in order to limit the spread of COVID-19'*, as well as to *'national tracking programmes already in force, and of the introduction of apps allowing authorities to monitor movements, contacts and health data'* (P9_TA(2020)0054, paragraph 51). The European Parliament stressed the importance of guaranteeing that **any such measures would be compliant with EU data protection law**, and called on the European Commission and the Member States *'to* ***publish the details*** *of these schemes and allow for public scrutiny and full oversight'* by DPAs (paragraph 53). In relation to contact tracing apps, it notably demanded all **storage of data to be decentralised**, and for the functioning of the apps to be transparent, allowing verification of underlying protocols and the code itself (paragraph 52).

On 13 May 2020, the eHealth Network published ***Interoperability guidelines for approved contact tracing mobile applications in the EU*** (eHealth Network, 13 May 2020), proposing guidelines for cross-border interoperability *'of approved contact tracing mobile apps and associated procedures'* (ibid., 3). The Guidelines also announced that the European Commission was to set up 'a Wiki space (confluence page) also to engage with app developers (ibid., 10).

On 16 June 2020, the European Commission announced that Member States had *'agreed on a set of technical specifications to ensure a safe exchange of information between national contact tracing apps based on a decentralised architecture'* (EC, 16 June 2020). The announcement appears to refer to a document by the eHealth Network addressed to the Member States and the European Commission on **detailed interoperability** elements (eHealth Network, 16 June 2020). The eHealth Network also published another documented about interoperability, dated from 12 June 2020 (and titled *Interoperability specifications for cross-border transmission chains between approved apps:* ***Basic interoperability*** *elements between COVID+ Keys driven solutions*) (eHealth Network, 12 June 2020), which notably states that *'(i)n order to reduce the data downloaded by the user's apps,* ***the apps should be able to identify the countries where a user has been*** *during the past 14 day'* (ibid., 6).

The **EDPB** published in June 2020 a *Statement on the data protection impact of the* ***interoperability of contact tracing apps*** (EDPB, 16 June 2020). The statement stressed the importance of transparency issues, noting that interoperability leads to additional processing and disclosure of data to additional entities (ibid., 2).

In July 2020, the European Commission published an overview of the situation (EC, July 2020), according to which a **vast majority of Member States** have implemented or are planning to implement voluntary and temporary mobile apps that support contact tracing as part of public health strategies to combat the COVID-19 pandemic (ibid., 4) – relying both on 'decentralised' and 'centralised' approaches. Additionally, many Member States were identified as having implemented or planning to implement other mobile applications such as symptom checkers (idem). Although some Member States have adopted specific legislation related to such apps, some deny the need for such specific legislation (ibid., 8). Regarding interoperability, the overview document referred to the plans by the European Commission to 'set up a gateway service' to facilitate data transfers between national contact tracing apps and servers (ibid. 12).

According to the European Commission, Member States are currently *'working on a common approach for modelling and predicting the evolution of the COVID-19 pandemic through anonymised and aggregated mobility data'* (EC, July 2020).

These developments are of relevance for a discussion of AI in the field of law enforcement and criminal justice primarily because they set in motion novel data practices, potentially encompassing unprecedented availability of certain types of data, which could eventually be made accessible for law enforcement related purposes.

6.2. Law enforcement initiatives

A particularly visible use of technology by law enforcement authorities during the pandemic has concerned drones. In Italy, for instance, some monitoring practices with drones were exceptionally authorised *inter alia* on the grounds that there was a limited risk of hurting individuals, as there were less individuals in public spaces due to lockdown measures (Dotta, 2020). The way in which drones appear to have been used to ensure compliance with movement restriction measures related to Covid-19 has been decried by civil society in some Member States, such as Greece (Chelioudakis, 2020).

In France, the Conseil d'État published on 18 May 2020 a Decision on surveillance by drones, following action by two civil society organisations - La Quadrature du Net, and La Ligue des Droits de l'Homme (Conseil d'État, 2020). The decision concerned measures allowing to capture images by drone, in order to contribute to compliance with lockdown and social distancing measures. The drones at stake are equipped with a camera and a speaker allowing to transmit messages to the public. According to the authorities responsible for their use, the drones did not capture any personal data, notably because the images were only monitored live, in real time, and the team of persons watching them could not identify the individuals being watched. The Conseil d'État, however, observed that regardless of this argumentation, the fact was that the drones' cameras were equipped with a zoom, and that the devices could fly low enough as to allow for obtaining a detailed picture of people, obliged to consider the data potentially collected as personal data (ibid., paragraph 16).

7. POLICY RECOMMENDATIONS

There is broad consensus on the fact that AI systems in the field of law enforcement and criminal justice can have a **particularly serious impact on EU fundamental rights**. In this field, AI systems can touch the very heart of the relation between individuals and public authorities, bringing with them often the participation of private companies, potentially precipitating data flows across jurisdictional borders, and setting in motion a myriad of novel questions on how critical decisions are taken, how can they be explained, and how can they be contested. AI systems in this field may affect basic safeguards designed to guarantee individual freedom and to prevent the abuse of power. It is thus logical that when discussing possible scenarios for a possible regulation of AI, there is often a '*general consensus*' on the need to define at least some '*clear red lines on certain extremely high-risk scenarios*' which would have a significant impact on individuals and society.[192]

In her 2019 political statement, Ursula Von der Leyen proclaimed, referring to the plans to move towards '*A Europe fit for the Digital Age*', that '*(a)s we increase investment in disruptive research and breakthrough innovation, we must accept that failure will be part of our path*' (Von der Leyen, 2019, 13). In 2017, the European Commission had somehow similarly stated that '*(e)xperimentation is an important part of the exploration of emerging issues in the data economy*' (COM(2017) 9 final, 17). Although these approaches might be of some value from an economic perspective in certain contexts, accepting failure and embracing experimentation cannot be the most appropriate formula when fundamental rights are manifestly at stake.

This study has shown that the progressive deployment of AI in the field of law enforcement and criminal justice, although still embryonic to some extent, has already sparked calls for caution, as well as instances of mistrust and resistance. The study has also shown that although there have been already many EU-level efforts directed at setting up a **trustworthy ecosystem** for the advent of AI, such efforts have not yet been fully informed by a detailed acknowledgement of the specificities of the legal framework in this field.

Taking into account the findings of the study, the recommendations below can be put forward.

7.1. Assess fully the relevance and gaps of the existing legal framework

As described, many discussions on the possible need for a legislative intervention in relation to AI are grounded on interpretations of the data protection safeguards that the GDPR provides to individuals. In general, but especially in relation to personal data processing in the field of law enforcement and criminal justice, it is not sufficient to circumscribe the pertinent assessment to a reading of the GDPR.

It is imperative, first, to consider also EU legal instruments, such as the LED and the EU-DPR. But it is also equally necessary to move beyond the analysis of EU legal instruments, notably towards an assessment of national legislation that either specifies the GDPR or implements the LED, as Member States might have adopted exemptions or derogations that modulate the safeguards eventually available to individuals when data about them are processed for law enforcement or criminal justice purposes. Furthermore, it is equally indispensable to take into account the **enforcement** of relevant provisions, and the experiences of different actors involved.[193] Finally, it remains to be seen whether

[192] Reference to such a general consensus at a multi-stakeholder workshop on AI and facial recognition celebrated in Brussels in February 2020: Wiewiórowski, 2020.

[193] There might be significant gap between certain visions of the presumed strengths of the EU data protection legal framework in light of the advent of AI, on the hand, and the reality as perceived by individuals whose fundamental rights are at stake. In this sense, for instance, although Article 22 of the GDPR is supposed to offer significant safeguards against automated decision-making (when it applies), the latest Eurobarometer study on data protection law revealed that a

any eventual weaknesses can be effectively tackled by means different from a legislative intervention, and whether perhaps strengthening consistency mechanisms might be a sufficient solution.[194]

7.2. Adapt initiatives to the specificities of the field

Some general principles commonly regarded as key for a trustworthy ecosystem for AI might face specific challenges in the field of law enforcement and criminal justice. It is the case, for instance, of **transparency.** It is thus important to take into account such specificities since the start, rather than developing a general framework for trustworthy AI, the impact of which in the field of law enforcement and criminal justice would eventually be cancelled, or seriously undermined, by exemptions or derogations adopted in the name of law enforcement or criminal justice needs. This might require, for instance, thinking about specific governance mechanisms that would be efficient enough to compensate other possible limitations of transparency.

The Council of Europe's *Guidelines on Addressing the Human rights Impacts of Algorithmic Systems* explicitly refer to this tension, notably in reference to recommended human rights impact assessments.[195] The Guidelines suggest that such impact assessments '*should be conducted as openly as possible and with the active engagement of affected individuals and groups*', and when high-risk algorithmic systems are concerned '*the results of ongoing human rights impact assessments, identified techniques for risk mitigation, and relevant monitoring and review processes should be made publicly available, without prejudice to secrecy safeguarded by law'*.[196] More specifically, *'(w)hen secrecy rules need to be enforced, any confidential information should be provided in a separate appendix to the assessment report'*, which should be **accessible to relevant supervisory authorities**.[197]

It is also important to note that any possible limitations of transparency towards data subjects make even more important compliance with other legal principles, such as **legal certainty** and **predictability**.[198]

7.3. Consider the need for special rules for certain practices

The many issues triggered by facial recognition, and most notably **live facial recognition in public spaces**, demand urgent attention and possibly a specific response. This should not detract the attention, however, from the possible need to regulate also beyond such specific practices. In this sense, calls for a regulatory framework for algorithmic decision-making for law enforcement purposes appear as very pertinent in light of the findings of this study.[199]

majority of individuals in the EU had never heard about their right to have a say when they are subject to automated decisions (Kantar, 2019, 23). The need for more clarity on the interpretation of Article 22 of the GDPR has been already highlighted by many (cf. for instance, Datenethikkommission, 2019, 28, 192).

[194] Such an assessment shall nevertheless also take into account that consistency beyond the GDPR is less formally developed, but also that even under the GDPR consistency mechanisms appear not to be fully efficient at the moment (cf. for instance, noting lack of efficiency in regards to identifying consistent criteria for data protection assessments: Belgian Data Protection Authority (DPA), 2020, 3.

[195] Recommendation CM/Rec(2020)1, Appendix, paragraph B.5.3.

[196] Idem.

[197] Idem.

[198] As stated by Recital (26) of Regulation (EU) 2016/794 in relation to law enforcement cooperation, that is an area '*where data subjects are usually unaware when their personal data are being collected and processed and where the use of personal data may have a very significant impact on the lives and freedoms of individuals'*.

[199] In relation to the UK: Babuta, Oswald and Rinik, 2018, vii.

7.4. Clarify the role of ethics

Ethical frameworks and guidance might be helpful to help delivering a trustworthy ecosystem for AI, but currently there is **much confusion** as to what should be the relation between such ethical frameworks or guidance and fundamental rights safeguards. Such confusion, if further sustained, might be in the end detrimental to the protection of fundamental rights, to the extent that it can divert attention from the necessity of safeguarding certain legal obligations. Most notably, ethical frameworks might not deliver the necessary safeguards in terms of access to remedies.

7.5. Reinforce trust in EU-funded AI efforts

Governments, it has been pointed out, should be *'the first'* to use AI in a manner that safeguards and promotes data protection and fundamental rights in general (Mantelero, 2019, 3); they must uphold particularly high standards because they have a direct obligation to do so, but also because state activity is, in general, expected to set an example for the whole of society (Datenethikkommission, 2019, 212). These reflections can be extended to cover the special responsibility that public authorities – including EU institutions, agencies and bodies – have towards the support of AI research and solutions with public funds.

Transparency, oversight and accountability requirements must be particularly high when EU funds are used to support AI research that can have a serious impact on EU fundamental rights, such as **security-related AI research**. Ethics reviews and assessments must be based on up-to-date, appropriate, pertinent guidance, and be accompanied by clear **transparency requirements**, in order to guarantee that the research funded is appropriately putting forward trustworthy solutions and is duly open to public scrutiny, especially insofar as compliance with legal and 'ethical' standards are concerned.

As research in this area is expected to be increasingly significant in the upcoming years, delivering specific guidance to improve trust in EU-funded research is crucial, and thus progress in terms of openness is essential. The EDPS could play a major role by stepping up its role in the overview of certain data processing operations funded with the support of EU funds. The EDPB could provide better, more detailed guidance, especially for research efforts that cross national borders.[200]

7.6. Screen developments related to the Covid-19 outbreak

In response to the Covid-19 outbreak, a variety of data-based and technology-driven solutions have been embraced, not necessarily immediately accompanied by the pertinent technical and legal safeguards. This can potentially lead to a situation of increased vulnerability in front of cybersecurity attacks, including threats targeting sensitive data. It can also lead to situations of increased vulnerability due to risks of misuse of power. Even if many of the endorsed initiatives do not explicitly have a law enforcement dimension, they nevertheless enable the processing of data that might, eventually, be made available for law enforcement purposes, thus creating special risks for individuals' fundamental rights. Moreover, due to the virus outbreak and the subsequent management of the crisis, fundamental rights have sometimes been restricted in serious ways. This obliges to be particularly vigilant, in order to prevent weakened fundamental rights from being irreparably damaged by the crisis, but also by its responses.

[200] Also stressing the opportunity of concrete guidance on AI-related research, in particular in cross-border projects: Datenethikkommission, 2019, 20.

REFERENCES

- Access Now Europe, *The European human rights agenda in the digital age*, November 2019.
- Advisory Committee on Equal Opportunities for Women and Men, *Opinion on Artificial Intelligence – opportunities and challenges for gender equality*, 18 March 2020.
- AI 4 Belgium Coalition, *AI 4 Belgium Report*, 2019.
- AI Now Institute, *AI Now Report 2018*, December 2018.
- AI Task Force, *Artificial Intelligence in Support of Defence*, Ministère des Armées (France), September 2019.
- Alfter, B., 'Denmark', in M. Spielkamp, *Automating Society: Taking Stock of Automated Decision-Making in the EU*, AlgorithmWatch and BertelsmannStiftung, January 2019, pp. 46-54.
- Amnesty International, *Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database*, May 2018.
- Arroyo, V. and D. Leufer (2020), 'Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazil', *Access Now*, 29 June 2020.
- Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, Adopted on 4 April 2017 as last Revised and Adopted on 4 October 2017, WP 248 rev.01.

  ---, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, Adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, WP251rev.01.
- Association for Computing Machinery (ACM) US Technology Policy Committee (USTPC), *Statement on Principles and Prerequisites for the Development, Evaluation and Use Of Unbiased Facial Recognition Technologies*, 30 June 2020.
- Austrian Delegation to the Council, *Note to Working Party on Information Exchange and Data Protection (DAPIX) on Next generation Prüm (Prüm.ng) - Reports from focus groups / Report on face recognition*, 13356/19, Brussels, 30 October 2019.
- Autoriteit Persoonsgegevens, *On the anonymity of aggregated telco location data*, April 2020.
- Babuta, A. and M. Oswald, *Data Analytics and Algorithms in Policing in England and Wales Towards A New Policy Framework, Occasional Paper*, Royal United Services Institute for Defence and Security Studies, February 2020.
- Babuta, A., M. Oswald & C. Rinik, *Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges*, Whitehall Report 3-18, Royal United Services Institute for Defence and Security Studies, September 2018.
- Barik, S., 'Sweden permits police-use of facial recognition technology', *Medianama*, 29 October 2019.
- Belfiore, R., 'The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters', in S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, Springer, 2013, pp. 355-370.

- Belgian Data Protection Authority, *Evaluation of the GDPR under Article 97 – Questions To Data Protection Authorities/European Data Protection Board: Answers From The Belgian Supervisory Authority*, 2020.

  ---, *Objet: Demande d'avis concernant un avant-projet d'arrêté royal n° XXX portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19 (CO-A-2020-042),* Avis n° 36/2020 du 29 avril 2020.

- Blatt, J. J., 'Some Observations on the Clearview AI Facial Recognition System – From Someone Who Has Actually Used It …', 6 May 2020.

- Boddington, P., *Towards a Code of Ethics for Artificial Intelligence*, Springer, 2017.

- Boucher, P., *Why Artificial Intelligence matters (Briefing)*, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) PE 634.421, March 2019.

- boyd, d., 'Untangling research and practice: What Facebook's "emotional contagion" study teaches us', *Research Ethics*, *12*(1), 2016, pp. 4–13.

- Brkan, M., 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond', *International Journal of Law and Information Technology*, 27:2, 2019.

- Brundage, M., et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, February 2018.

- Buolamwini, J. and T. Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification', *Conference on fairness, accountability and transparency*, Proceedings of Machine Learning Research, 81, 2018.

- Campbell, Z. and C. Jones, 'Leaked Reports Show EU Police Are Planning a Pan-European Network of Facial Recognition Databases', *The Intercept*, 21 February 2020.

- Carrera, S. and M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, No. 2020-01, Center for European Policy Studies (CEPS), February 2020.

- Castro, D., M. McLaughlin & E. Chivot, 'Who Is Winning the AI Race: China, the EU or the United States?', *Centre for Data Innovation,* 19 August 2019.

- Chambre des Députés du Grand-Duché de Luxembourg, *Covid-19 : vers un traçage numérique ?*, 28 April 2020.

- Chelioudakis, E., 'Greece: Technology-led policing awakens', *About Intel: European Voices on Surveillance*, 29 June 2020.

- Commissioner for Human Rights of the Council of Europe, *Unboxing Artificial Intelligence: 10 steps to protect Human Rights – Recommendation*, May 2019.

- Committee of Experts on Internet Intermediaries (MSI-NET), *Study on The Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) and Possible Regulatory Implications,* (Rapporteur: Benjamin Wagner), DGI(2017)12, March 2018.

- Committee of Experts on Quality Journalism in the Digital Age (MSI-JOQ), *Draft Recommendation CM/Rec(20XX)XX of the Committee of Ministers to member States on promoting a favourable environment for quality journalism in the digital age: 7th draft as of 26 September 2019*, Council of Europe, MSI-JOQ(2018)08rev6, 2019.

- Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament, *Draft Report on Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, Rapporteur: Tudor Ciuhodaru, LIBE, 2020/2016(INI), 8 June 2020.
- Conseil d'État, *Surveillance par drones (décision)*, 18 mai 2020.
- Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), *Practical Guide on the Use of Personal Data in the Police Sector*, Strasbourg, 15 February 2018, T-PD(2018)01.
- Cook, S., *Letter to Attorney General Barr on The use of the PATTERN risk assessment in prioritizing release in response to the COVID-19 pandemic*, 3 April 2020.
- Cope, S. and Hussain, S., 'EFF to Court: Social Media Users Have Privacy and Free Speech Interests in Their Public Information', *Electronic Frontier Foundation (EFF*), 30 June 2020.
- Coudert, F., 'The Europol Regulation and Purpose Limitation: From the 'Silo-Based Approach' to… What Exactly?', *European Data Protection Law (EDPL)*, Vol. 3, Number 3, 2017, pp. 313-324.
- Council of the EU, *Note from Permanent Representatives Committee (Part 1) to Council on Artificial intelligence - b) Conclusions on the coordinated plan on artificial intelligence (Adoption),* 6177/19, Brussels, 11 February 2019.

  ---, *Note from the Presidency to the Standing Committee on Operational Cooperation on Internal Security (COSI) on The future direction of EU internal security: new technologies and internal security - Preparation of the Council debate*, 12224/19, COSI 184 ENFOPOL 400 CYBER 257 JAI 949, Brussels, 18 September 2019.
- Cox, J., *Surveillance Company Says It's Deploying 'Coronavirus-Detecting' Cameras in US*, *Motherboard: Tech by The Vice,* 17 March 2020,
- Cox, J. and J. Koebler, 'Surveillance Firm Banjo Used a Secret Company and Fake Apps to Scrape Social Media', 9 March 2020, *Motherboard: Tech by The Vice.*
- Data Ethics Commission of the German Federal Government (Datenethikkommission), *Opinion (*English version), Berlin, December 2019.
- Datainspektionen, *Datainspektionen inleder tillsyn med anledning av Clearview AI*, 6 March 2020.
- Datakalab, *Politique de protection des données personnelles dans le cadre de la mise en œuvre du dispositif de détection de masques de protection respiratoire*, April 2020.
- Davies, B., M. Innes, and A. Dawson, *An evaluation of South Wales Police's use of Automated Facial Recognition*, Police Science Institute Crime and Security Research Institute, Cardiff University Institute, September 2018.
- De Brouwer, S., 'European Parliament shows (again) its stance on Artificial Intelligence', *Access Now Blog*, 14 February 2020.
- De Capitani, E., *Complaint and application for a temporary injunction (Geulen & Klinger)*, 13 May 2019.
- Dodd, V., 'MET removes hundreds from gangs matrix after breaking data laws', *The Guardian*, 15 February 2020.
- Dotta, G., 'ENAC: autorizzati i droni per il monitoraggio', *Punto Informatico*, 24 March 2020,
- Dumbrava, C., 'Tracking mobile devices to fight coronavirus', *European Parliamentary Research Service Blog*, 21 April 2020.

- DutchNews, 'Privacy watchdog slams coronavirus phone data mapping plan', *DutchNews.nl*, 3 July 2020.

- eHealth Network, *Common EU Toolbox for Member States: Mobile applications to support contact tracing in the EU's fight against COVID-19* (Version 1.0), 15 April 2020.

  ---, *Interoperability guidelines for approved contact tracing mobile applications in the EU*, 13 May 2020.

  ---, *Interoperability specifications for cross-border transmission chains between approved apps - Basic interoperability elements between COVID+ Keys driven solutions*, V1.0, 12 June 2020.

  ---, *To the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps - Detailed interoperability elements between COVID+ Keys driven solutions*, V1.0, 16 June 2020.

- Ethics Advisory Group (EAG), *Towards a digital ethics*, European Data Protection Supervisor (EDPS), 2018.

- European Commission (EC), *Community policy on data processing: Communication of the Commission to the Council*, SEC (73) 4300 final, 21 November 1973.

  ---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a thriving data-driven economy*, COM(2014) 442 final, 2 July 2014.

  ---, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, Brussels, 6 May 2015.

  ---, *Communication from the Commission to the European Parliament and the Council: Stronger Smarter Information Systems for Border and Security*, COM(2016) 205 final, Brussels, 6 April 2016.

  ---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy*, COM(2017) 9 final, Brussels, 10 January 2017.

  ---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2018: An agenda for a more united, stronger and more democratic Europe*, COM(2017) 650 final, Strasbourg, 24 October 2017.

  ---, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe*, COM(2018) 237 final, Brussels, 25 April 2018.

  ---, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulatio a and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA*, COM/2018/302 final, Brussels, 16 May 2018.

  ---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2019: Delivering what we promised and preparing for the future*, COM(2018) 800 final, Strasbourg, 23 October 2018.

  ---, *Ethics and data protection*, 14 November 2018 (EC, 2018).

---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Coordinated Plan on Artificial Intelligence* Brussels, COM(2018) 795 final, 7 December 2018.

---, *Horizon 2020 Programme Guidance: How to complete your ethics self-assessment, Directorate-General for Research & Innovation*, Version 6.1, 4 February 2019.

---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence,* COM(2019) 168 final, Brussels, 8 April 2019.

---, *Communication from the Commission to the European Parliament and the Council - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250 final, Brussels, 29 May 2019.

---, *A Community of Users on Secure, Safe and Resilient Societies: Mapping Horizon H2020 and EU-Funded Capacity-Building Projects under 2016-2018 Programmes*, October 2019.

---, *H2020 Programme Guidance: Guidelines for the classification of information in research projects*, Directorate-General for Migration and Home Affairs, Version 2.2, 7 January 2020.

---, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Work Programme 2020: A Union that strives for more*, COM(2020) 37 final, Brussels, 29 January 2020.

---, *Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics*, COM(2020) 64 final, Brussels, 19 February 2020.

---, *White Paper On Artificial Intelligence -A European approach to excellence and trust*, COM(2020) 65 final, Brussels, 19 February 2020.

---, *Communication to the European Parliament, to the Council, the European Economic and Social Committee and the Committee of the Regions, A European data strategy*, COM(2020) 66 final, Brussels, 19 February 2020.

---, *Communication to the European Parliament, to the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future*, COM(2020) 67 final, Brussels, 19 February 2020.

---, *Daily News*, 7 April 2020.

---, *Commission Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, C(2020) 2296 final, Brussels, 8 April 2020.

---, *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*, C/2020/2523, 16 April 2020.

---, *Daily News*, 16 June 2020.

---, *Communication to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 final, Brussels, 24 June 2020.

---, *Communication from the Commission to the European Parliament and the Council: Way forward on aligning the former third pillar acquis with data protection rules*, Brussels, COM(2020) 262 final, 24 June 2020.

---, *Mobile applications to support contact tracing in the EU's fight against COVID-19: Progress reporting June 2020*, July 2020.

- European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, adopted by the CEPEJ during its 31st Plenary meeting (Strasbourg, 3-4 December 2018), CEPEJ(2018)14.

- European Data Protection Board (EDPB), *Facial recognition in school renders Sweden's first GDPR fine*, 22 August 2019.

  ---, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak*, 21 April 2020.

  ---, *Draft Agenda 26th session of plenary meeting*, 8 May 2020.

  ---, *Statement on the data protection impact of the interoperability of contact tracing apps*, adopted on 16 June 2020.

- European Data Protection Supervisor (EDPS), *Annual Report 2019*, 2019.

  ---, *Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust*, 29 June 2020.

  ---, *Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services*, 2 July 2020.

- European Migration Network (EMN), *Annual Report on Migration and Asylum 2018*, May 2019.

- European Parliament (EP), *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, (2013/2188(INI)), 12 March 2014.

  ---, *Resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)),* P8_TA(2017)0076, 14 March 2017.

  ---, *Resolution on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services*, P9_TA(2020)0032, 12 February 2020.

  ---, *Resolution of on EU coordinated action to combat the COVID-19 pandemic and its consequences*, P9_TA(2020)0054, 17 April 2020.

  ---, *Decision on discharge in respect of the implementation of the general budget of the European Union for the financial year 2018, Section I – European Parliament (2019/2056(DEC))*, P9_TA(2020)0084, 13 May 2020.

- European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), *Testing the borders of the future: Smart Borders Pilot: The results in brief*, 2015 (2015a).

  ---, *Smart Borders Pilot Project: Technical Report Annexes: Volume 2*, (2015b).

- European Union Agency for Fundamental Rights (EU FRA), *Preventing unlawful profiling today and in the future: A guide*, Handbook, 2018 (2018a).

  ---, *#BigData: Discrimination in data-supported decision making*, FRA Focus, 2018 (2018b).

---, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, FRA Focus, November 2019.

---, *AI policy initiatives (2016-2020)*, April 2020.

- Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT), *Responsibility and AI: A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework* (Rapporteur: Karen Yeung), DGI(2019)05, Council of Europe, September 2019.
- Ferretti, L., et al., 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', *Science*, Vol. 368, Issue 6491, 8 May 2020.
- Fight for the Future, 'Backlash forces UCLA to abandon plans for facial recognition surveillance on campus', *Medium*, 19 February 2020.
- Floridi, L., 'Soft Ethics and the Governance of the Digital', *Philosophy & Technology*, Volume 31, 2018, pp. 1-8.
- Fondazione Giacomo Brodolini (FGB), *Fundamental rights review of EU data collection instruments and programmes: Final report*, 2019.
- Franko Aas, K., *Sentencing in the age of information: from Faust to Macintosh*, Routledge, New York, 2005.
- Fürsteneau, M., 'Germany's facial recognition pilot program divides public', *DW*, 24 August 2017.
- Garvie, C., A. Bedoya, and J. Frankle, 'The Perpetual Line-Up. Unregulated Police Face Recognition in America', *Georgetown Law Center on Privacy & Technology*, 18 October 2016.
- Gates, K. A., *Our biometric future: Facial recognition technology and the culture of surveillance*, New York University Press, 2011.
- General Secretariat of the Council, *Note to Delegrations on Council Conclusions on the implementation of the "Prüm Decisions" ten years after their adoption*, 11227/18, Brussels, 18 July 2018.
- Gershgorn, D., 'Facial Recognition Companies See the Coronavirus as a Business Opportunity', *One Zero*, 19 March 2020.
- Gießler, S. and L. Haas, 'Ethics between business lingo and politics: Why bother?', AI Ethics Guidelines Global Inventory, April 2020.
- González Fuster, G., *Feedback to the Consultation on the White Paper on Artificial Intelligence (AI) focusing on AI & gender: An EU law perspective*, 14 June 2020.
- Grace, J., 'Algorithmic impropriety in UK policing?', *Journal of Information Rights, Policy and Practice*, 3(1), 2019.
- Gräf, E., 'When Automated Profiling Threatens Our Freedom: A Neo-Republican Perspective', *European Data Protection Law (EDPL)*, Vol. 3, Number 4, 2017, pp. 441-451.
- Grind, K., R. McMillan and A. W. Mathews, 'To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits', *Wall Street Journal*, 17 March 2020.
- Habersetzer, N., 'Moscow Silently Expands Surveillance of Citizens', *Human Rights Watch*, 25 March 2020.

- Hamon, R., H. Junklewitz & I. Sánchez, *Robustness and Explainability of Artificial Intelligence: From technical to policy solutions*, JRC Technical Report, Joint Research Centre (JRC), EUR 30040 EN, 2020.
- Harcourt, B. E., *Against prediction: Profiling, policing, and punishing in an actuarial age*, University of Chicago Press, 2008.
- Hardyns, W., and A. Rummens, 'Predictive policing as a new tool for law enforcement? Recent developments and challenges', *European Journal on Criminal Policy and Research*, 24(3), 2017, pp. 201-218.
- Hennessy, M., 'Explainer: What happened with the Graham Dwyer data retention case in the Supreme Court?', *The Journal*, 24 February 2020.
- High-Level Expert Group on Artificial Intelligence (AI HLEG), *Ethics Guidelines for Trustworthy Artificial Intelligence (AI),* 8 April 2019 (2019a).
- ---, *Policy and Investment Recommendations for Trustworthy AI*, 26 June 2019 (2019b).
- High-Level Group on Fake News and Online Disinformation, *A multi-dimensional approach to disinformation*, European Commission, March 2018.
- Hill, K., 'The Secretive Company That Might End Privacy as We Know It', *The New York Times*, 18 January 2020.
- Information Commissioner's Office (ICO), *The Office of the Australian Information Commissioner and the UK's Information Commissioner's Office open joint investigation into Clearview AI Inc.*, Statement, 9 July 2020.
- Innovation Centre of the International Criminal Police Organization (Interpol) and United Nations Interregional Crime and Justice Research Institute (UNICRI), *Artificial Intelligence and Robotics for Law Enforcement*, 2019.
- Interpol, *INTERPOL launches awareness campaign on COVID-19 cyberthreats*, 6 May 2020.
- IT-Pol, *Danish DPA approves Automated Facial Recognition*, European Digital Rights Initiative (EDRi), 19 June 2019.
- Jain, R., 'Baidu's Face Detection AI Will Help China Identify People Without Masks', *International Business Times*, 17 February 2020.
- Jelinek, A., *EDPB response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI*, 10 June 2020.
- Jobin, A., M. Ienca, and E. Vayena, 'The global landscape of AI ethics guidelines', *Nature Machine Intelligence*, 2019, 1, pp. 389–399.
- Juncker, J. C., *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*, Strasbourg, 15 July 2014.
- Kantar, '*Special Eurobarometer 487a – March 2019: The General Data Protection Regulation'*, March 2019.
- Kayser-Bril, N., 'Unchecked use of computer vision by police carries high risks of discrimination', *AlgorithmWatch*, 28 April 2020.
- Kim, N. 'More Scary Than Coronavirus': South Korea's Health Alerts Expose Private Lives, *The Guardian*, 6 March 2020.

---, 'Anti-gay backlash feared in South Korea after coronavirus media reports', *The Guardian*, 8 May 2020.

- Koebler, J., E. Maiberg, and J. Cox, 'This Small Company Is Turning Utah Into a Surveillance Panopticon', *Motherboard: Tech By Vice*, 4 March 2020.
- Korff, D., *Comments on Selected Topics in the Draft EU Data Protection Regulation*, London/Cambridge, 2012.
- Labarthe, S. and A. Velásquez, *CoronApp, Medellín me Cuida y CaliValle Corona al laboratorio -O cómo se hackea CoronApp sin siquiera intentarlo-*, 17 April 2020 (2020a).
- ---, *Covid Apps in Colombia, Karisma's digital security and privacy evaluation*, 28 April 2020 (2020b).
- Lapinski, I., 'When algorithms decide your rights', *Digital Freedom Fund*, December 2018.
- La Quadrature du Net, *La reconnaissance faciale des manifestant·e·s est déjà autorisée*, 18 November 2019.
- Lee, T. B., 'Detroit police chief cops to 96-percent facial recognition error rate', *Ars Technica*, 30 June 2020.
- Leslie, D., *Understanding Artificial Intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector,* The Alan Turing Institute, 2019.
- Leufer & Jansen, 'The EU is funding dystopian Artificial Intelligence projects', Euractiv, 22 January 2020.
- Light, F., 'Russia Is Building One of the World's Largest Facial Recognition Networks', *The Moscow Times*, 12 November 2019.
- Lynch, S., 'The Challenges of Facial Recognition Technologies', *Human-Centered Artificial Intelligence - Stanford University,* 23 April 2020.
- Mac, R., C. Haskins & L. McDonald, 'Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA', *Buzzfeed News*, 27 February 2020.
- Mantelero, A., *Report on Artificial Intelligence - Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), Strasbourg, 25 January 2019, T-PD(2018)09Rev.
- Markey, E. J., *Letter from Senator Edward J. Markey to Hoan Ton-That, Founder & Chief Executive Officer of Clearview AI*, 30 April 2020.
- Mascini, L., 'EU expert on European response to virus: 'Telecom data for tracking corona can be made anonymous', *Innovation Origins*, 11 April 2020.
- Massé, E., *Two Years under the EU GDPR: An Implementation Progress Report*, Access Now, May 2020.
- Mayor's Office for Policing and Crime (MOPAC), *Equality Impact Assessment, Gang Violence Matrix, Version 4*, 2018.
- McCarthy, O. J, 'AI & Global Governance: Turning the Tide on Crime with Predictive Policing', *United Nations University, Centre for Policy Research,* 26 February 2019.

- McNamara, Daniel, et al., 'Trade-offs in algorithmic risk assessment: An Australian domestic violence case study' in Daly, A., M. Mann, and S. K. Devitt, *Good Data*, Institute of Network Cultures, Theory on Demand Vol. 29, 2019, pp. 96-116.
- Meaker, M., 'Marseille's fight against AI surveillance', *Coda*, 26 March 2020.
- Ministry of Finance and Ministry of Industry, Business and Financial Affairs of the Danish Government, *National Strategy for Artificial Intelligence*, March 2019.
- Molnar, P. and L. Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*, International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto), 2018.
- Monroy, M., 'Prüm Decision: European criminal police offices agree on face recognition system', *Security Architectures and Police Collaboration in the EU*, 11 March 2020.
- Mozur, P., 'One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority', *The New York Times*, 14 April 2019.
- Oswald, M., and J. Grace, 'Intelligence, policing and the use of algorithmic analysis: a freedom of information-based study', *Journal of Information Rights, Policy and Practice*, 1.1, 2016.
- Parliamentary Assembly of the Council of Europe, *Recommendation 2102 (2017) on Technological Convergence, Artificial Intelligence and Human Rights*, adopted on 28 April 2017.
- Peeters, B., 'Facial recognition at Brussels Airport: face down in the mud', *CITIP Blog*, 17 March 2020.
- Penner, K., *Report – Automating Society: Europe*, 29 January 2019.
- Perry, L. W., et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Rand Corporation, 2013.
- Peters, J., 'IBM will no longer offer, develop, or research facial recognition technology', *The Verge*, 8 June 2020.
- Porter, J. 'Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech', *The Verge*, 6 February 2020.
- Presidency of the Council, *Note to Working Party on Information Exchange and Data Protection (DAPIX) on Next generation Prüm (Prüm.ng) - Planning of focus groups, 5556/19*, Brussels, 15 February 2019.
- ---, *Note to Working Party on Information Exchange and Data Protection (DAPIX) on Monitoring the Implementation of Directive (EU) 2016/681 on the use of passenger name record (PNR) data – State of play and way forward*, 6300/19, Brussels, 15 February 2019.
- Privacy International, '*MONITORYOU: the MilliONs beIng spenT by the eu on develOping surveillance tech to taRget YOU'*, 20 January 2020 (2020a).

  ---, '*One Ring to watch them all'*, 25 January 2020 (2020b).

  ---, *The SyRI case: a landmark ruling for benefits claimants around the world'*, 24 February 2020 (2020c).

  ---, *This UK Government-Funded AI Programme Wants to Make 'Face Recognition Ubiquitous' (But Sure, We're Probably Being Paranoid About Face Surveillance)*, 3 March 2020 (2020d).

- Renda, A., 'Will privacy be one of the victims of COVID-19?', *Centre for European Policy Studies* (CEPS), 23 March 2020.
- Reuters, 'Germany: Refugees sue the government for invasion of privacy', *DW*, 5 May 2020.
- Richardson, R., J. Schultz and K. Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice', 94 *N.Y.U. L. Rev. Online* 192, February 2019, pp. 192-233.
- Richardson, R., J. M. Schultz, & V. M. Southerland, *Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems*, AI Now Institute, September 2019.
- Robinson, D., and L. Koepke, 'Stuck in a pattern: Early evidence on 'predictive policing', *UpTurn*, 2016.
- Ronsin, X. and V. Lampos, *In-depth study on the use of AI in judicial systems, notably AI applications processing judicial decisions and data*, Appendix I accompanying the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, adopted by the CEPEJ during its 31st Plenary meeting (Strasbourg, 3-4 December 2018), CEPEJ(2018)14, 2018.
- Rubio, I., 'Las claves de la polémica por el uso de reconocimiento facial en los supermercados de Mercadona', *El País*, 7 July 2020.
- Sartor, G. and F. Lagioia (2020), *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) PE 641.530 – June 2020.
- Samoili, S. et al., *AI Watch - Defining Artificial Intelligence: Towards an operational definition and taxonomy of artificial intelligence*, JRC Technical Reports, European Union, 2020.
- Secretariat of the Council of Europe, *Submission to the Consultation on the "White Paper on Artificial Intelligence – a European approach to excellence and trust"*, 19 June 2020.
- Scott, M., 'Europe is fighting tech battle with one hand tied behind its back', *Politico*, 24 February 2020.
- Singer, N. and M. Isaac, 'Facebook to Pay $550 Million to Settle Facial Recognition Suit', *The New York Times*, 29 January 2020.
- Temme, M., 'Algorithms and Transparency in View of the of GDPR', *European Data Protection Law (EDPL)*, Vol. 3, Number 4, 2017, pp. 473-485.
- Thomsen, M., 'Federal government and three states are in talks with controversial facial recognition company Clearview AI to track coronavirus patients and see who they have been in contact with, *Daily Mail*, 2 May 2020.
- Turß, D., *European Court of Justice to decide on mass processing of passenger data*, 22 January 2020.
- Unione Camere Penali Italiane, *Processo penale da remoto e protezione dei dati personali. L'Unione scrive al Garante*, 14 April 2020.
- United Nations (UN) Independent Human Rights Experts Press Service, *Landmark ruling by Dutch court stops government attempts to spy on the poor – UN expert*, Press release, 5 February 2020.
- United Nations (UN) Special Rapporteur on Extreme Poverty and Human Rights, *Report of the Special Rapporteur on extreme poverty and human rights*, A/74/493, 2019.

- United States (US) Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018.

  ---, *DOD Adopts Ethical Principles for Artificial Intelligence*, Press Release, 24 February 2020.

- United States (US) Department of Justice, *Predictive Analytics in Law Enforcement: A Report by the Department of Justice*, EPIC-16-06-15-DOJ-FOIA-20200319-Settlement-Production-pt1, November 2014.
- Vaas, L., 'Boston bans government use of facial recognition', *Naked Security by Sophos*, 6 July 2020.
- Van Brakel, R. (2019), 'Belgium', in M. Spielkamp, *Automating Society: Taking Stock of Automated Decision-Making in the EU*, AlgorithmWatch and BertelsmannStiftung, January 2019, pp. 39-44.
- Van Hoboken, J., et al., *The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising: Final report*, Institute for Information Law (IViR), University of Amsterdam, 2019.
- Van Roy, V., *AI Watch - National strategies on Artificial Intelligence: A European perspective in 2019*, EUR 30102 EN, Publications Office of the European Union, Luxembourg, 2020.
- Vincent, J., Spot the robot is reminding parkgoers in Singapore to keep their distance from one another, *The Verge*, 8 May 2020.
- Von der Leyen, U., '*A Union that strives for more: My agenda for Europe – Political guidelines for the next European Commission 2019-2024*', 2019.
- Wagner, J. and A. Benecke, 'National Legislation within the Framework of the GDPR', *European Data Protection Law (EDPL)*, Vol. 2, Number 3, 2016, pp. 353-361.
- Wiewiórowski, W., 2020, 'AI and Facial Recognition: Challenges and Opportunities', *European Data Protection Supervisor (EDPS) Blog*, 21 February 2020.
- Wilson, D., 'Algorithmic patrol: The futures of predictive policing', in A. Završnik (ed.), *Big Data, Crime and Social Control*, Routledge, London and New York, 2017, pp. 108-127.
- World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), *Preliminary Study on The Ethics Of Artificial Intelligence*, UNESCO, 26 February 2019.
- World Economic Forum (WEF), *A Framework for Responsible Limits on Facial Recognition Use Case: Flow Management, Pilot project*, White Paper, February 2020.
- World Health Organisation, *COVID-19 virtual press conference - 25 March 2020*, 2020.
- Yang, Y., 'How China built facial recognition for people wearing masks', *Ars Technica*, 18 March 2020.
- Yun Chee, F., 'EU drops idea of facial recognition ban in public areas: paper', *Reuters*, 30 January 2020.
- Zanfir-Fortuna, G., 'European Union's Data-Based Policy Against the Pandemic, Explained', *Future of Privacy Forum*, 30 April 2020,
- Završnik, A., 'Big data: What is it and why does it matter for crime and social control?' in A. Završnik (ed.), *Big Data, Crime and Social Control*, Routledge, London and New York, 2017, pp. 3-28. (2017a)

  ---, Završnik, A., 'Algorithmic crime control' in A. Završnik (ed.), *Big Data, Crime and Social Control*, Routledge, London and New York, 2017, pp. 131-153 (2017b).

ANNEX – A COMPARISON BETWEEN 'ALGORITHMIC DATA RIGHTS' IN THE GDPR AND THE LED

This Annex offers a succinct review of the **rights granted to data subjects** by the GDPR and by the LED **in relation to profiling and automated decision-making**. These rights might be referred to as 'algorithmic data rights' to the extent that they are the ones most directly concerned with algorithmic data processing. It is necessary to underline that this does not mean that other data subject rights might not be relevant too. It is also important to stress that these rights might not systematically apply when processing related to law enforcement and criminal justice are at stake, as both the GDPR and the LED allow for restrictions and derogations. The main purpose of this review is to illustrate that these rights, which are **at the core of the intersection between EU data protection law and AI**, have been given substance **differently in the GDPR and the LED**.

Representatives of EU DPAs, gathered as Article 29 Working Party, elaborated in 2017 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* which were later endorsed by the EDPB (A29WP, 2017/2018). There exist no equivalent guidelines about the LED. The Guidelines emphasise in any case that '*profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards'* (ibid., 5).

The risks identified evolve around the **opacity** and **discrimination**. **Opacity** might affect the very fact that one is being profiled, and the nature of such profiling (idem). Concerns about opacity are primarily addressed in the GDPR through the principle of transparency, which takes precisely as starting point that '*the process of profiling is often invisible to the data subject'* (ibid., 9). Additionally, opacity relates to the fact that *'(i)ndividuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes'* (idem). **Discrimination** concerns are multiple: profiling can perpetuate existing stereotypes and segregation, locking a person into a specific category, and restricting them to suggested preferences. Also, being placed in the wrong category might lead to unjustified discrimination (ibid., 5).

Concerns about discrimination are primarily addressed in the GDPR through the **principle of fairness**, also present in Article 4(1)(a) of the LED. The Guidelines stress that *'(p)rofiling may be unfair and create discrimination'* (ibid., 10). The GDPR has a number of provisions which aim at ensuring that profiling and automated individual decision-making (whether or not it includes profiling) are not used in ways that have an unjustified impact on individuals' rights, most notably, in addition to specific transparency and fairness requirements, accountability obligations; specified legal bases for the processing; rights for individuals to oppose profiling and specifically profiling for marketing purposes; and, if certain conditions are met, the obligation to carry out a data protection impact assessment (ibid., 6). Recital (26) of the LED points out: *'The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)'.*

According to the Guidelines, *'(g)iven the core **principle of transparency** underpinning the **GDPR**, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works'* (ibid., 16). '*In particular*', they specify, '*where the processing involves profiling-based decision making (irrespective of whether it is caught by Article 22 provisions), then the fact that the processing is for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject'* (idem). Recital (60) of the GDPR states indeed that '*the data subject should **be informed of the existence of profiling** and **the consequences** of such profiling'*, as part of the GDPR principle of transparency (ibid., 17).

The **principle of transparency** is **not explicitly mentioned** as such in the **LED**. It does not appear in Article 4, which lists the Principles relating to processing of personal data: Article 4(1)(a) merely states that *'Member States shall provide for personal data to be (…) processed lawfully and fairly'*. There is a reference to transparency in the Recitals of the LED, concretely at Recital (26), which states that *'(a)ny processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law'*. There is not, in the LED, any explicit reference to the fact the data subject should be informed of the existence of profiling and the consequences of such profiling.

In addition to a right to be informed, there exists a **right of access** – also mentioned in Article 8 of the EU Charter, together with the right to rectification. The Guidelines state that Article 15 of the GDPR, on the right of access, *'gives the data subject the right to obtain details of* ***any personal data used for profiling****, including the categories of data used to construct a profile'*, and specified that *'(i)n addition to general information about the processing, pursuant to Article 15(3), the controller has a duty to make available the data used as input to create the profile as well as access to* ***information on the profile*** *and details of* ***which segments*** *the data subject has been placed into'* (ibid., 17).

Said Article 15 of the GDPR refers to the obligation imposed on data controllers to *'provide* ***a copy*** *of the personal data undergoing processing'*. The right of access under the LED does not foresee an equivalent obligation imposed on data controllers to provide a copy of the data at stake. Recital (43) of the LED indicates that data controllers might comply with the right of access by providing to the data subject *'a full summary of those data'*.

Data subjects have the right to **rectification** and **erasure**. The Guidelines note that in the GDPR *'(t)he rights to rectification and erasure apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person)'* (ibid., 18). The right to rectification and to erasure are also present in the LED, although the provision establishing them also indicates that in certain cases a refusal by the data controller is permissible. Member States must make sure that when such is the case the data controller informs the data subject in writing about the refusal, although Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information under certain conditions (Article 16(4) of the LED).

Data subjects have a right to **object**. Under Article 21 of the GDPR, the right to object applies to the cases where processing of personal data is *'based on point (e) or (f) of Article 6(1), including* ***profiling*** *based on those provisions'*, that is, when the processing is 'necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller' (Article 6(1)(e) of the GDPR) or 'proc*essing is necessary for the purposes of the* ***legitimate interests*** *pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child)* (Article 6(1)(f) of the GDPR). There is no equivalent right to object under the LED.

Article 22 of the GDPR, still in the GDPR Chapter about data subject rights, is titled *Automated individual decision-making, including profiling,* and its first paragraph states that *'The data subject 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'*. The Guidelines take the view that the use of the term 'right' here does not imply that Article 22(1) applies only when actively invoked by the data subject. Instead, Article 22(1) of the GDPR would establish **a general prohibition for decision-making based solely on automated processing**, applying nevertheless in a limited number of circumstances (the decision based solely on automated processing, and has a legal effect on or similarly significantly affects someone), and subject to exceptions. According to the Guidelines, Article 22 of the GDPR provides that under the GDPR *'as a rule, there is a general prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant* *effect'*, although *'there are exceptions to the rule'*, even if *'where one of these exceptions applies, there must be measures in place to safeguard the data subject's rights and freedoms and legitimate interests'* (ibid., 19).

Article 22(1) of the GDPR applies to decisions based solely on automated processing, including profiling, which produce legal effects concerning or similarly significantly affect the data subject. The Guidelines clarify that *'(p)rocessing that might have little impact on individuals generally may in fact have a significant effect for certain groups of society, such as minority groups or vulnerable adults'* (ibid., 22).

The safeguards to be applied when automated decision-making based solely on automated processing, which produces legal effects or similarly significantly affects the data subject is allowed encompass a **right to be informed** (specifically, to be provided with meaningful information about the logic involved, as well as the significance and envisaged consequences for the data subject), and other safeguards such as **the right to obtain human intervention** and **the right to challenge the decision** (addressed in Article 22(3)) (ibid., 20).

In the LED, there is a reference for Member States having to establish that decisions based solely on automated processing, including profiling, which produce an **adverse legal effect** concerning the data subject or significantly affects them, shall be prohibited unless authorised by an EU or Member State law to which the controller is subject *'and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller'* (Article 11(1) of the LED). Automated decisions producing adverse legal effects are thus **not fully prohibited** under the LED, but conditioned to the existence of a legal provision providing for some safeguards. Article 11 of the LED, contrary to Article 22 of the GDPR, appears outside of the Chapter on data subject rights. There is no explicit reference to the need to foresee a right to challenge the decision, although there is a mention to this issue in Recital (38), which portrays the possibility to challenge a decision as a suitable safeguard when evaluating personal aspects of an individual is based solely on automated processing and which produces adverse legal effects, or significantly affects them.

In relation to these safeguards, the Guidelines noted that *'(a)ny processing likely to result in a high risk to data subjects requires the controller to carry out a **Data Protection Impact Assessment (DPIA)**'*, which might be *'particularly useful for controllers who are unsure whether their proposed activities will fall within the Article 22(1) definition, and, if allowed by an identified exception, what safeguarding measures must be applied'* (ibid., 20). Both the GDPR and the LED foresee that DPIAs are necessary in some cases (cf. Article 35 of the GDPR, and Article 27 of the LED). The requirements for DPIAs are however not the same. The GDPR notably establishes that *'(w)here appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing'* (Article 35(9) of the GDPR), whereas the LED does not have an equivalent provision.

Under the GDPR, it is possible to exceptionally undertake the processing described in Article 22(1) where the decision is (a) necessary for the performance of or entering into a contract, (b) authorised by EU or Member State law to which the controller is subject laying down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) based on the data subject's explicit consent. Regarding (b), Recital (71) of the GDPR notes that this might refer to *'fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller'*.

In line with Article 22(4) of the GDPR, automated decision-making covered by Article 22(1) of the GDPR that involves special categories of personal data is only allowed under the following cumulative conditions of falling under an applicable Article 22(2) exemption; and falling under point (a) or (g) of Article 9(2), which refer to the need of explicit consent of the data subject; or necessity for reasons of substantial public interest, on the basis of EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject. In both cases, the controller must put in place suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. In Article 11 of the LED there is no reference to consent. Under this provision, decisions covered by Article 11 of the LED shall not be based on special categories of personal data, '*unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place'*.

Moving specifically to the rights of the data subject related to decisions falling under Article 22 of the GDPR, the Guidelines noted that *'(g)iven the potential risks and interference that profiling caught by Article 22 poses to the rights of data subjects, data controllers should be* ***particularly mindful of their transparency obligations'*** (ibid., 24). Articles 13(2)(f) and 14(2)(g) of the GDPR require data controllers to provide information about '*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.*

As explained by the Article 29 Working Party, this means that under the GDPR data controllers must **inform the data subject** that they are engaging in this type of activity, provide meaningful information about the logic involved, and explain the significance and envisaged consequences of the processing. According to the Guidelines, even when automated decision-making and profiling do not fall under Article 22(1) of the GDPR, *'it is nevertheless good practice to provide the above information'* (AWP29, 2017/2018, 25). Moreover, it adds that in any event data controllers '*must provide sufficient information to the data subject to make the processing fair'* (idem, in reference to Recital (60)).

Under the LED, there are **no equivalent information obligations**. The provision detailing the 'Information to be made available or given to the data subject', that is, Article 13 of the LED, does not include any reference to profiling or automated decision-making. The only explicit reference to profiling in the Recitals of the LED is the allusion to the fact that profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms *'should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter'* (Recital (38) of the LED).

Regarding the relation between the decisions falling under Article 22 of the GDPR and the **right of access**, Article 15(1)(g) establishes that data subjects exercising their right of access shall have the right to receive information on '*the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'*. There is no reference here to the need to provide a detailed explanation as to why a specific decision was taken.

The Guidelines noted, in reference to the GDPR, that *'by exercising their Article 15 rights, the data subject can become aware of a decision made concerning him or her, including one based on profiling'* (ibid., 27). In that case, '*(t)he controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision'* (idem). This refers to instrumentality of transparency obligations and data subject rights in EU data protection law: it is by being informed about certain data processing practices that the data subject will be in a position to further exercise their rights.

Regarding suitable safeguards, the Guidelines pointed out in relation to the GDPR that the requirement of 'human intervention' relates to the fact that *'(a)ny review must be carried out by someone who has the appropriate authority and capability to change the decision'*, and that *'(t)he reviewer should undertake a* *thorough assessment of all the relevant data, including any additional information provided by the data subject'* (ibid., 27).

Suitable safeguards under the GDPR include, in addition to the **right to obtain human intervention**, the **right for the data subject to express their point of view** and the **right to contest the decision**. The Guidelines stated that the controller *'must provide a simple way for the data subject to exercise these rights'*, and that they emphasise the 'need for transparency about the processing', as *'the data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis'* (ibid., 27).

Other safeguards highlighted by the Guidelines include safeguards aimed at mitigating the risk of errors or bias in collected or shared data, or in the automated decision-making process, that can result in *'incorrect classifications; and assessments based on imprecise projections; that impact negatively on individuals'* (ibid., 27). These safeguards can include *'carrying out frequent assessments on the data sets they process to check for any bias, and develop ways to address any prejudicial elements, including any over-reliance on correlations'* or *'(s)ystems that audit algorithms and regular reviews of the accuracy and relevance of automated decision-making including profiling'* (ibid., 28). In addition, controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special categories of data, measures which should be used on a cyclical basis: not only at the design stage, but also continuously and making sure the outcome of such testing feeds back into the system design (idem). All this is connected to **Recital (71) of the GDPR**, which mentions the need to use appropriate mathematical or statistical procedures.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, examines the impact on fundamental rights of Artificial Intelligence in the field of law enforcement and criminal justice, from a European Union perspective. It presents the applicable legal framework (notably in relation to data protection), and analyses major trends and key policy discussions. The study also considers developments following the Covid-19 outbreak. It argues that the seriousness and scale of challenges may require intervention at EU level, based on the acknowledgement of the area's specificities.

PE 656.295
IP/C/LIBE/IC/2019-083

Print ISBN 978-92-846-6938-7 | doi: 10.2861/138135 | QA-04-20-418-EN -C
PDF ISBN 978-92-846-6939-4 | doi:10.2861/ 880024 | QA-04-20-418-EN -N