European Parliament

# Person identification, human rights and ethical principles

## Rethinking biometrics in the era of artificial intelligence

STUDY

Panel for the Future of Science and Technology

**EPRS | European Parliamentary Research Service**

Scientific Foresight Unit (STOA)

PE 697.191 – December 2021

EN

# Person identification, human rights and ethical principles

## Rethinking biometrics in the era of artificial intelligence

As the use of biometrics becomes commonplace in the era of artificial intelligence (AI), this study aims to identify the impact on fundamental rights of current and upcoming developments, and to put forward relevant policy options at European Union (EU) level.

Taking as a starting point the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI, presented by the European Commission in April 2021, the study reviews key controversies surrounding what the proposal addresses through the notions of 'remote biometric identification' (which most notably includes live facial recognition), 'biometric categorisation' and so-called 'emotion recognition'.

Identifying gaps in the proposed approaches to all these issues, the study puts them in the context of broader regulatory discussions. More generally, the study stresses that the scope of the current legal approach to biometric data in EU law, centred on the use of such data for identification purposes, leaves out numerous current and expected developments that are not centred on the identification of individuals, but nevertheless have a serious impact on their fundamental rights and democracy.

## AUTHORS

This study has been written by Professor Gloria González Fuster and Michalina Nadolna Peeters of the Law, Science, Technology and Society (LSTS) Research Group at Vrije Universiteit Brussel (VUB) at the request of the Panel for the Future of Science and Technology (STOA) and managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

## ADMINISTRATOR RESPONSIBLE

Mihalis Kritikos, Scientific Foresight Unit (STOA)

To contact the publisher, please e-mail stoa@ep.europa.eu

## LINGUISTIC VERSION

Original: EN

Manuscript completed in December 2021.

## DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PE 697.191
ISBN: 978-92-846-8818-0
doi: 10.2861/384495
QA-01-21-551-EN-N

http://www.europarl.europa.eu/stoa (STOA website)
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

# Executive summary

This study explores **biometrics** in the era of **artificial intelligence** (AI), focusing on the connections between person identification, human rights and ethical principles. As such, it covers a subject of the greatest political and societal prominence. Among the many controversies in this area, certainly one of the most salient is the discussion surrounding facial recognition, and more specifically about the potential risks stemming from the use of **live facial recognition technology in public spaces**. The potentially negative impact of the widespread use of such technology has indeed mobilised a strong response from parts of civil society in Europe and globally.

From a policy and legislative viewpoint, in the European Union (EU) this discussion is currently being framed in terms of regulating possible uses of **remote biometric identification**. Live facial recognition technology uses facial templates that allow for the unique identification of individuals, and thus constitute – due to such capability for 'unique identification' – **biometric data** for the purposes of applicable EU data protection law.

For many years, the exploration of possible normative frameworks to accompany and duly channel the advent of AI has primarily turned around ethical considerations and principles. In 2020, however, the European Commission started openly and decidedly moving towards the adoption of a new legal framework for AI as main priority in this regard. For this purpose, the European Commission notably published in April 2021 a proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI (COM(2021) 206 final) (hereafter also 'the proposed AI act' or 'the proposed AIA').

The proposal puts forward rules that apply to a variety of AI systems. Demonstrating the importance of biometric technologies, three types of AI systems, explicitly defined in the proposal and subject to specific rules, are in fact defined in the very text of the proposal on the basis of their connection with **biometric data**: these are 'remote biometric identification systems', 'emotion recognition systems' and 'biometric categorisation systems':

- **remote biometric identification systems** are defined as AI systems used 'for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified';
- **emotion recognition systems** are defined as AI systems used 'for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data', and
- **biometric categorisation systems** are defined as AI systems used 'for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data'.

These notions are however not yet fully consolidated at EU level, and thus one of the objectives of the study is to unpack their rationale, scope and possible limitations.

The proposed regulation defines '**biometric data'** as '**personal data** resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic data' (COM(2021) 206 final 42). This definition of biometric data is exactly the same as the one featured in the main instruments of EU data protection law, where the processing of biometric data for the purpose of uniquely identifying a natural person is regarded as constituting the processing of a special category of data that deserves the most stringent level of protection.

## Scope and structure of the study

This study has been prepared on the basis of desk research. The focus of the study is the EU framework, although due consideration has also been given to international developments when relevant. The study first provides an overview of current trends in biometrics and AI, including technological considerations and information about notable uses, as well as specific information in relation to remote biometric identification, emotion recognition and biometric categorisation. Second, it presents the regulatory framework, illustrating that ongoing developments in the area of biometrics and AI do not occur in a legal vacuum, but amid pre-existing legal provisions and overarching EU fundamental rights obligations. Third, it reviews current policy discussions, in particular in the EU and as embodied by the European Commission's proposal for a regulation on AI, and then puts forward policy options.

## Biometrics and AI

Biometric data are increasingly used in a great variety of contexts. At EU level, the processing of biometric data has been actively encouraged and directly supported over the past years in the context of EU-level large-scale information technology (IT) systems in the area of freedom, security and justice (**AFSJ**). These systems, initially set up by the EU for asylum and migration management but increasingly also serving internal security, almost systematically rely on the massive collection of biometric data.

The review of ongoing technological and societal developments at the crossroads of biometrics and AI shows that, although **identification** is a crucial notion for biometrics, there are many developments aimed not primarily at identification but at the **categorisation** of individuals, assigning them to different categories, for instance on the basis of age or gender. It is however not always clear how the processing occurring for the purposes of categorisation is linked to identification, or to what extent such practices can always be separated.

Most notably, it is sometimes unclear, first, whether the data processed for categorisation purposes concern an identified or identifiable person at all, and whether such data should thus be regarded as personal data for the purposes of EU law. Second, it is sometimes unclear whether the data at stake – which often **relate to the body** – constitute or not biometric data, which requires taking into account whether the data allow for the identification of the individual (even if they are processed for the purpose of categorisation). Complicating the situation further, sometimes the categorisation of individuals is in practice a step taken towards their identification.

## Regulatory framework

There is currently no European legislation relating exclusively to biometrics. The most directly relevant specific rules of EU law are to be found in EU data protection law. In addition, the whole existing EU fundamental rights architecture is fully applicable to the use of biometric technologies.

A review of this architecture and of the most relevant rules on biometrics and on automated decision-making in EU data protection law, as well as of the most important case law in this area emanating from the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR), shows that ongoing technological developments are taking place amid – and possibly also somehow *despite* – **existing rights and principles**, which might thus possibly need to be reinforced, clarified, or at least fine-tuned.

## Impact on fundamental rights

AI-enabled biometric technologies pose significant risks to numerous **fundamental rights**, but also to **democracy** itself. In this sense, for instance, the **pervasive tracking of individuals in public**

**spaces** constitutes not only a major interference with their rights to respect for private life and to the protection of personal data, but can also impact negatively on their rights to freedom of expression, and to freedom of assembly and association, altering the way in which certain individuals and groups are able to exercise social and political protest. The deployment of facial recognition technologies during peaceful assemblies can discourage individuals from attending them, limiting the potential of participatory democracy. **Bias** and **discrimination** are a well-documented issue in this field, and can be the result of a variety of factors.

Different uses of biometric technologies can have different specific types of impact on fundamental rights. The deployment of remote biometric identification in public spaces, in this sense, is particularly problematic as it potentially concerns the processing of individuals' data – without their cooperation or knowledge, on a massive scale.

## Regulatory trends and discussions

There is an ongoing – even if not fully systematic – shift from the discussion of ethical frameworks for AI to the regulation of AI systems by **law**. It appears nevertheless clear to many actors that an improved framework is needed to guarantee the fairness, transparency and accountability of AI systems, an objective that can be pursued by enhancing representation at various levels of decision-making.

Developments in the United States (US) are numerous and illustrate a variety of approaches, most notably targeting facial recognition. In Europe, the Council of Europe has been particularly active in this area and is currently working on a possible new legal framework at its level for the development, design and application of AI, based on recognised Council of Europe standards in the field of human rights, democracy and the rule of law. In 2021, there was registered a **European citizens' initiative** named 'Civil society initiative for a ban on biometric mass surveillance practices', calling for strict regulation of the use of biometric technologies in order to avoid undue interference with fundamental rights.

The European Commission published its **proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI** (COM(2021) 206 final) on 21 April 2021. The proposal is based on Articles 16 and 114 of the TFEU, on personal data protection and the internal market, respectively. The proposed AI regulation prohibits the use of some AI systems (listed in the proposed Article 5), and qualifies other AI systems as 'high-risk', detailing the rules applicable to such 'high-risk' systems.

The area of **biometric identification and categorisation of natural persons** is in principle 'high risk', but under this heading (heading 1), only a concrete group of AI systems are mentioned: 'AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons'. There is, however, no reference to biometric categorisation being recognised as 'high risk'. Potentially, it is possible to imagine there might exist AI systems that involve the processing of **biometric data** in all other areas listed as 'high risk'.

The AI regulation proposed by the European Commission foresees, as a general principle, 'the **prohibition of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement**'. Nevertheless, such real-time remote biometric identification systems **can be used** as far as such use is strictly necessary for certain objectives and under certain conditions.

The proposed AI regulation explicitly excludes from its scope of application **AI systems that are components of existing and upcoming EU-wide large-scale IT systems**, if the systems were placed on the market or put into service during the first year of application of the regulation, or before that date. This rule would, however, not be applicable if the legal acts establishing such EU-wide large-scale IT systems would lead 'to a significant change in the design or intended purpose of the AI system or AI systems concerned' (proposed Article 83(1) AIA). The proposed text notes, despite the proposed regulation not being applicable as such to the systems mentioned, that the requirements that it lays down must 'be **taken into account**, where applicable' in the evaluation of these large-scale IT systems as provided for in those respective acts (idem), but it is unclear what such 'taking into account' would imply.

## Policy options

In light of the findings of the study, the following policy options are put forward:

- **Delimit better the regulation of biometrics and biometric data:** the proposed AIA reproduces the definition of 'biometric data' present in EU data protection law since 2016. The interpretation of the definition is not completely clear, and there are significant uncertainties as to how to apply EU data protection rules to biometric data. The definition, in any case, does not appear to cover all the problematic practices that are often framed in the literature and even by policy-makers as related to biometrics. It is thus important to shed further light on the scope and relevance of the definition, but also to think critically about the impact of conditioning some other notions put forward in the AIA (such as 'biometric categorisation' or 'emotion recognition') to the processing of biometric data defined in such a way.

- **Improve the future qualification of new AI systems as high-risk:** it is necessary to envisage a faster, clearer and accessible path to qualifying additional AI systems as high-risk systems in the future. Civil society organisations could be given a role to raise the alarm of major risks, especially insofar as the affected persons would potentially be in vulnerable positions.

- **Explicitly ban certain uses of live facial recognition:** the proposed AI regulation fails to prohibit real-time remote biometric identification in public spaces for law enforcement purposes, despite conceding that it triggers even more risks than 'high-risk' AI systems. The regulation should at least formally and effectively ban **the persistent tracking of individuals in public spaces by means of remote biometric identification**, as it has major consequences for fundamental rights and democracy.

- **Regulate 'post' remote biometric identification in the same manner as 'real-time' remote biometric identification:** the proposed AI regulation fails to address properly the risks connected with the retroactive identification, using facial recognition, of individuals whose images have been recorded while they were in public spaces. In practice, the risk of persistent tracking and its associated adverse impact on fundamental rights and democracy are, however, at least equivalent to the risk associated with 'real-time' remote biometric identification. 'Post' remote biometric identification of natural persons recorded while in public spaces should be subject to the same rules as the 'real-time' equivalent.

- **Establish at EU level the necessary safeguards for real-time remote biometric identification:** the proposed AI regulation leaves it up to the Member States to define, by law the exact conditions for the use of in principle prohibited but actually permitted real-time remote biometric identification in public spaces for law enforcement purposes. The only detailed condition is the need for prior authorisation granted by a judicial authority or by an independent administrative authority. Substantive safeguards for the prohibited but exceptionally permitted uses of real-time remote biometric identification, if any, must be specified at EU level in the future AIA itself, as opposed to being left to the discretion of the Member States.

- **Ban AI systems assigning to categories that constitute sensitive data based on biometric data:** the proposed AI regulation gives a definition of 'biometric categorisation system' that is unclear and conceptually problematic, most notably to the extent that it seems to endorse the idea that it is possible – scientifically, ethically and legally – to use AI systems to assign natural persons to a sexual or a political orientation. If a reference to the use of similar AI systems persists in the draft, it should be phrased clearly as a prohibition.

- **Clarify the regulation of 'emotion recognition':** the status of 'emotion recognition' in the proposal for a regulation on AI is not entirely clear. The proposed definition of emotion recognition seems to imply that emotions and intentions of individuals can be inferred from biometric data. This would only possibly make sense if biometric data are understood in a broad sense, not limited to data concerned with the unique identification of individuals. In addition, the list of high-risk systems in Annex III includes various references to systems used 'to detect the emotional state of a natural person', without clarifying if these would correspond to what is defined as 'emotion recognition' systems or would potentially be something else.

- **Increase transparency towards individuals as a necessary means to guarantee rights and remedies:** the proposed AI regulation privileges imposing obligations on actors other than the users of AI systems, who are only subject to a limited number of provisions. The use of extremely high-risk systems in particular should be conditioned to additional obligations imposed on users towards individuals, notably in terms of transparency both prior to the use and during the use. Transparency is crucial for the exercise of rights and the effectiveness of remedies. Limitations to transparency should be compensated with measures that guarantee the accountability of such limitations.

- **Do not allow for special exemptions to general rules for EU large-scale databases:** the use of biometrics and AI in EU large-scale IT systems is massive, raising serious risks for fundamental rights. The fact that the European Commission's proposal for a regulation on AI deliberately leaves out of its scope of application certain AI systems to be used in the AFSJ is of great concern. It is essential that large-scale IT systems in the AFSJ comply fully with the highest standards of EU law.

# Table of contents

**1. Introduction** **1**

**2. Methodology and resources** **2**

2.1. Scope of the study 2

2.2. Methodology and use of resources 5

**3. Synthesis of the research work and findings** **6**

3.1. Biometric technologies and AI 6

3.1.1. Biometric technologies 6

3.1.2. A variety of areas of use 10

3.1.3. Remote biometric identification 13

3.1.4. Biometric categorisation 16

3.1.5. Emotion recognition 19

3.2. Overview of the regulatory framework 22

3.2.1. General fundamental rights framework 22

3.2.2. EU data protection law 23

3.2.3. Fundamental rights case law 27

3.3. Impact on fundamental rights 32

3.4. Regulatory trends and current policy debates 36

3.4.1. Overview of global discussions 37

3.4.2. Council of Europe 39

3.4.3. EU recent developments 40

3.4.4. Towards a regulation on AI 41

**4. Policy options** **53**

**5. References** **60**

## List of figures

Figure 1 – Types of AI systems defined by the processing of biometric data (in light of the proposed AI Act) 5

Figure 2 – Identification and categorisation, EU fundamental rights and values 36

# 1. Introduction

This study explores **biometrics** in the era of **artificial intelligence** (AI), focusing on the connections between person identification, human rights and ethical principles. As such, it covers a subject of the greatest political and societal prominence. Our societies are nowadays indeed at a crucial moment in grappling with the impact on fundamental rights of the continuously increasing and evolving uses of AI. These are occurring not only due to technological progress, but also in conjunction with an equally increasing institutional support of AI technologies, typically accompanied by narratives that highlight AI's potential for societal advances and for economic growth.

Among all the controversies that have surfaced in these debates, certainly one of the most salient is the discussion about facial recognition (FRA 2020(b) 130), and more specifically about the use of live facial recognition technologies in **public spaces**. The potential negative impact of a widespread use of such technologies has indeed strongly mobilised part of civil society globally, and also specifically in Europe (cf. for instance EDRi 2020(a)). From a policy and legislative viewpoint, in the European Union (EU) this discussion is currently framed in terms of regulating possible uses of **remote biometric identification** – as live facial recognition technologies use facial templates that allow for the identification of individuals, and thus constitute, for the purposes of applicable EU data protection law, **biometric data**.

After many years of explorations of the normative framework possibly needed to properly accompany AI, which was until very recently primarily turning around ethical considerations and principles, the European Commission started openly moving in 2020 towards the adoption of a new legal framework for AI. To this purpose, it notably published in April 2021 a proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI (COM(2021) 206 final) (hereafter also 'the proposed AI Act' or 'the proposed AIA'). The initiative is extremely important for the future of AI regulation and thus for the future of AI in Europe, but also potentially globally. The global significance of the proposal was already perceptible in some of the earliest reactions following its publication (cf. for instance Haeck 2021).

It has been noted that, in this important initiative, 'biometrics technologies feature heavily' (Kind 2021). Indeed, although the proposal puts forward rules that apply to a variety of AI systems, the three types of AI systems that are explicitly defined and subject to specific rules are in fact defined in the text of the proposal on the basis of their connection with biometrics: these are '**remote biometric identification systems'**, '**emotion recognition systems'**, and '**biometric categorisation systems'**. The AI systems that are targeted through these three notions certainly raise particularly serious questions in relation to their impact on fundamental rights.

This study takes the three mentioned types of AI systems as a guiding thread for the exploration of the impact of biometrics and AI on fundamental rights, in order to facilitate a reflection on the possible policy options currently available, and about the opportunities they each offer. This does not mean, however, that the distinctions between the proposed types systems are always fully clear, or even that their exact relation with biometrics is not unproblematic. As a matter of fact, questioning the pertinence and possible limitations of the proposed categories and their definitions is also one of the objectives of the study. All in all, the study's ambition is to throw light on the evolution of the intersections between AI and biometrics, highlighting some of issues that most urgently require attention from a human rights and ethical perspective.

# 2. Methodology and resources

This section describes the scope of the study, including some key terminological considerations, presents the methodology followed, and explains the use of resources.

## 2.1. Scope of the study

The study focuses on current developments that, building on the use of **biometrics** and **AI**, present specific challenges related to human rights and ethical principles. **Facial recognition** is arguably the most paradigmatic development in this area, developing precisely at the crossroads of AI and biometrics. Not all uses of facial recognition, however, trigger the same type of legal and ethical challenges. In this sense, for instance, the impact of using facial recognition for authentication of users of certain devices based on the consent of the individuals concerned is not comparable to the impact of facial recognition being deployed in public spaces, particularly for identification purposes. More generally, there can be many uses of biometric data which do have important fundamental rights implications,[1] for example in relation to identity management, but these fundamental rights implications might not be implications directly connected to the use of AI.

A few terminological considerations are necessary. The term AI itself can be interpreted differently by different actors. In relation to 'biometrics', terms such as **biometric systems**, **biometric technologies**, and **biometric recognition** are commonly used to cover the range of automated technologies that use biometric identifiers to identify, verify, or confirm a person's identity. To think about biometrics nowadays nevertheless requires to also consider **systems that produce other kinds of inferences from bodily data (**Kak 2020 6), also in ways which technically might not fall under the most commonly used definitions of 'biometrics'.

To delimit in practice the scope of the study, and in light of its final objective, which is to put forward pertinent policy recommendations at EU level, have been taken into account as main references the definitions put forward in the European Commission's proposal for a regulation on AI, in particular those related to AI systems and more specifically to AI systems and biometrics.

The European Commission's proposed regulation on AI defines '**AI systems'** as **software** that can, for a given set of human-defined objectives, **generate outputs** such as content, predictions, recommendations, or decisions influencing the environments they interact with, and that is developed with one or more of the following techniques and approaches (COM(2021) 206 final 39):

> '(a) **machine learning** approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
>
> (b) **logic- and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
>
> (c) **statistical approaches**, Bayesian estimation, search and optimization methods.'

These techniques and approaches are listed in an Annex accompanying the proposal, Annex I. In line with the proposed text, the European Commission would be empowered under the future regulation on AI to adopt delegated acts amending the techniques and approaches listed, 'in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein' (COM(2021) 206 final 43).

[1] See notably, for instance: Privacy International 2017.

The European Commission's proposed regulation defines '**biometric data'** as '**personal data** resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm the unique identification of that natural person**, such as facial images or dactyloscopic data' (COM(2021) 206 final 42).

This definition of biometric data is exactly the same as the one featured in the main instruments of EU data protection law; the General Data Protection Regulation (GDPR)[2] (cf. Article 4(14) GDPR), the Law Enforcement Directive (LED) on Data Protection[3] (cf. Article 3(13) LED), and the Regulation on Data Protection for EU institutions and bodies[4] (cf. Article 3(18) EU DP Regulation).

The integration of this definition of biometric data in EU data protection law is relatively recent, and its interpretation is not deprived of complexity. A Recital in the GDPR stresses that shall only be regarded as biometric data for the purposes of EU data protection law the personal data that permit **the unique identification** or authentication of an individual **through a specific technical means**, noting that:

> 'the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person' (Recital (51) GDPR).[5]

It is very important to already highlight that at least in some contexts the term 'biometric data' is used, at least by certain actors, also **in a broader sense**, which does not necessarily involve allowing a possible unique identification. Policy documents sometimes discuss AI systems relying on biometrics as such together with systems that track **certain bodily features that might not be technically, and/or legally, be regarded as biometrics** in a narrow sense. This is the case for instance when is discussed the collection of data of micro-expressions, heart rate or temperature data (CAHAI(2020)23 8).

In some cases, the boundaries between biometric data and other data are not clear. In this sense, the European Data Protection Supervisor (EDPS) and the Spanish Data Protection Authority (Agencia Española de Protección de Datos, AEPD) co-authored in 2020 a paper that argues, for instance, that the 'processing of mouse movement used to determine whether a robot is accessing a website involves treating biometric information to differentiate human from machine', and would thus constitute biometric data processing even if the individual moving the mouse cannot be uniquely identified (EDPS and AEPD 2020 3), and even if the purpose of the processing is not to uniquely identify anybody, but to determine whether they are a human being.

There are also **other definitions of biometric data** in EU law, beyond the mentioned data protection law instruments. For instance, Regulation (EU) 2018/1862 on the Schengen Information

[2] 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), OJ L 119, 4.5.2016, pp. 1–88.

[3] 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, OJ L 119, 4.5.2016, pp. 89–131.

[4] 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, pp. 39–98.

[5] Arguing that Recital (51) GDPR brings confusion to the notion of biometric data in EU data protection law, as opposed to clarity: Jasserand-Breeman 2019 156.

System (SIS)[6] adds to the definition the explicit mention of 'photographs' (in addition to facial images), and of DNA profiles.[7] For the purposes of Regulation (EU) 2019/817[8] ' 'biometric data' means fingerprint data or facial images or both'. Regulation (EU) 2019/816 defines for its purposes 'facial image' as 'a digital image of a person's face'.[9]

In relation to DNA profiles, it must be noted that currently EU data protection law regulates DNA data primarily through the category of 'genetic data'.[10] Notwithstanding the fact that the processing of DNA data can have serious implications for fundamental rights, their discussion is not directly related to the core developments addressed in this study, and thus DNA data will only be mentioned when specifically relevant.

The European Commission's proposal for an AI Act provides definition for three different types of AI systems explicitly connected to the processing of biometric data: **remote biometric identification systems**, defined as AI systems used 'for the purpose of identifying natural persons at a distance through the comparison of **a person's biometric data with the biometric data contained in a reference database**, and without prior knowledge of the user of the AI system whether the person will be present and can be identified' (proposed Article 3(36) AIA), **emotion recognition systems**, defined as AI systems used 'for the purpose of identifying or inferring emotions or intentions of natural persons **on the basis of their biometric data**' (proposed Article 3(34) AIA), and **biometric categorisation systems**, defined as AI systems used 'for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, **on the basis of their biometric data**' (proposed Article 3(35) AIA) (COM(2021) 206 final 42) (see Figure 1).

[6] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312, 7.12.2018.

[7] Cf.: '"biometric data" means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, namely photographs, facial images, dactyloscopic data and DNA profile', Art. 3(12) of Regulation (EU) 2018/1862. The instrument also defines 'dactyloscopic data' ('data on fingerprints and palm prints which due to their unique character and the reference points contained therein enable accurate and conclusive comparisons on a person's identity', Art. 3(13)), 'facial image' ('digital images of the face with sufficient image resolution and quality to be used in automated biometric matching', Art. 3(14)), and 'DNA profile' ('a letter or number code which represents a set of identification characteristics of the noncoding part of an analysed human DNA sample, namely the particular molecular structure at the various DNA locations (loci)', Art. 3(15)).

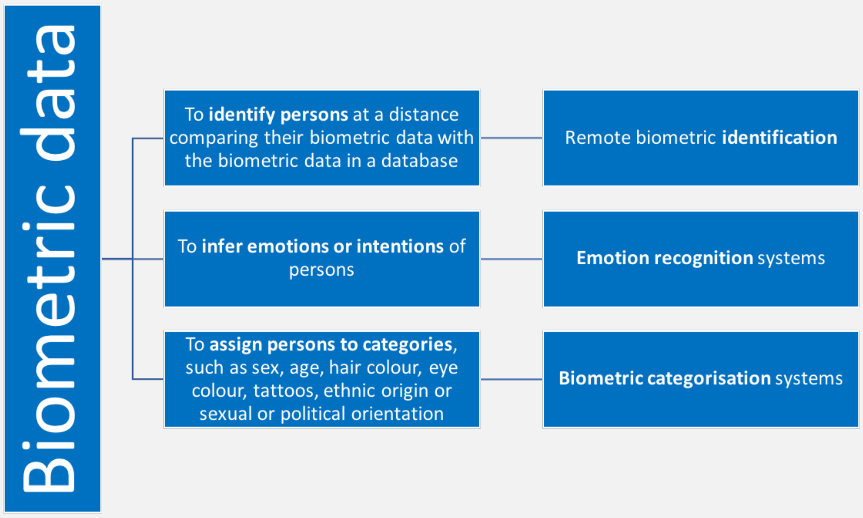
[8] Art. 4(11) of Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019, pp. 27–84. This Regulation also defines 'biometric template' (as 'a mathematical representation obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications', Art. 4(12)).

[9] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726, OJ L 135, 22.5.2019, pp. 1–26.

[10] Defined as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question' (Art. 4(13) GDPR; Art. 3(12) LED; Art. 3(17) EU DP Reg). Recital (34) of the GDPR further explains: 'Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained'.

Nevertheless, the use of these terms is not yet fully consolidated at EU level, and thus one of the objectives of the study is to unpack their meaning and possible limitations. All in all, it is possible to refer to the developments discussed in the study as 'biometrics-driven AI', or AI technologies developed around the use of biometrics understood in a broad sense – that is, not necessarily as biometrics aiming at identification. Another relevant term might be 'AI-enabled biometric technologies', if used to refer to AI technologies driven by AI which are capable of identifying, analysing and recognizing human traits.

Figure 1 - Types of AI systems defined by the processing of biometric data (in light of the proposed AI Act)



Biometric data

To **identify persons** at a distance comparing their biometric data with the biometric data in a database

Remote biometric **identification**

To **infer emotions or intentions** of persons

**Emotion recognition** systems

To **assign persons to categories**, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation

**Biometric categorisation** systems

As derived from the proposed Arts. 3(34-36) COM(2021) 206 final 42.

## 2.2. Methodology and use of resources

This study has been elaborated on the basis of desk-research, including traditional literature review. The selection of mobilised resources has been taken place on the basis of standard legal research criteria, giving special attention to applicable law, both primary and secondary law. For the identification and discussion of the challenges to human rights and ethical considerations, the focus has been placed on EU fundamental rights, and the relevant legal framework and case-law has been explored. In addition, special consideration has been given to the work of data protection supervisory authorities. For the analysis of policy developments, the output of the main relevant EU institutions has been considered. Although the focus of the study is the EU framework, due consideration has been given to international developments when relevant.

# 3. Synthesis of the research work and findings

This part of the study offers the main insights gathered from the research work. First, an overview of the current trends in biometrics and AI is provided, including technological considerations and information about notable uses, as well as specific information in relation to remote biometric identification, 'emotion recognition' and biometric categorisation. Second, the regulatory framework is presented, illustrating that the ongoing developments in the area of biometrics and AI do not occur in a legal vacuum, but amidst pre-existing legal provisions and overarching EU fundamental rights obligations. Third, are reviewed the current policy discussions, in particular in the EU and as embodied by the European Commission's proposal for a regulation on AI.

## 3.1. Biometric technologies and AI

Biometric data are increasingly used in many contexts. The fact that biometric data are, by definition, **enabling the unique identification** of individuals, is of particular value. It is the fact that they are 'unique' that makes them potentially more reliable than alphanumeric data for the purposes of identifying a person.[11] This is in any case the main reason why their processing has been progressively integrating EU policy and legal initiatives 'in order to assist in the reliable identification of the individuals' (Recital (20) of Regulation (EU) 2018/1862).

The following sub-sections further describe biometric technologies, present some key areas of use of biometrics in combination with AI, and finally discuss separately remote biometric identification, biometric categorisation and 'emotion recognition'.

### 3.1.1. Biometric technologies

Biometric technologies utilise various body characteristics, which can be called **sources of biometric data** or reference measures (Bygrave and Tosoni 212). The Article 29 Working Party argued that sources of biometric data shall not be considered biometric data themselves, but they can be used for the collection of personal data (Art29 WP193 4).

The sources of biometric data can relate to the **physical**, **physiological** or **behavioural characteristics** of a natural person. Technologies relying on the processing of physiological characteristics can include: fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odour detection, voice recognition, DNA pattern analysis, or sweat pore analysis (Art29 WP193 4). These are thus characteristics that could be described as **visual**, **auditory**, **olfactory** or **chemical**. Behavioural characteristics can include hand-written signature verification, gait analysis, or way of walking or moving (Art29 WP193 4).

**Behavioural biometric systems** started gathering much attention years ago mainly in the context of computer security, because although they might not by themselves be 'unique enough to provide reliable human identification, [...] have been shown to provide sufficiently high accuracy identity verification' (Yampolskiy and Govindaraju 2008 82).[12] Examples of behavioural biometrics include indeed human computer interaction (HCI)-based biometrics, which are concerned with metrics about humans' interaction with devices, such as way of using a keyboard or mouse, or their interaction with software (idem). Keystroke biometrics, for instance, uses 'the cadence of an individual's typing pattern for recognition', which has potential under some conditions but has a

[11] In this sense, see Recital (18) of Regulation (EU) 2019/817.

[12] Generally speaking, physiological biometric based authentication systems are believed to perform better than behavioural biometric based authentication systems (Ramu, Suthendran, and Arivoli 2019 10031).

limited level of accuracy due to factors such as distraction, fatigue, or emotions provoking variations in typing rhythm (Ramu, Suthendran, and Arivoli 2019 10031). **Mobile behavioural biometrics** focus on behavioural biometrics related to mobile and wearable devices, measuring for instance the touching of screens, or processing accelerometer-based and gyroscope-based data (Eglitis, Guest and Deravi 2020). Behavioural biometrics have also more recently attracted much attention in the field of banking and payment (Thales 2020).

For a characteristic or trait to be suitable for biometric applications, factors to be considered are that it should be **universal,** that is, in principle possessed by every relevant individual; **unique,** in the sense of sufficiently different across members of the population; **permanent,** or sufficiently invariant over time; and **measurable,** meaning it should be possible to be acquired, digitized and further processed to extract representative features (Pato and Millett 2010 34-35).

There exist multiple possible classifications of biometric systems. An often-used distinction opposes biometric technologies based on **unimodal** biometric systems, i.e., based on one single biometric trait, and **multimodal** modal systems, i.e., based on more than one trait. Multimodal biometric systems typically aim at mitigating or compensating some of the perceived limitations of unimodal biometric systems, for instance to limit the risk of spoofing, with the aim of making the systems more robust (Ross and Jain 2004; Sanjekar and Patil 2013).

A term often used in this field is '**soft biometrics'**. The term can have different meanings. 'Soft biometrics' has for instance been defined as 'biometric characteristics which are specific to an individual; however, not in themselves unique – subject age, e.g. or gender' (Fairhurst, Li and Da Costa-Abreu 2017 369), and there has been special interest from some researchers to work on the ability 'to predict soft biometric characteristics from conventional biometric data' (idem). The term is however also sometimes used to refer precisely to the systems that claim to be able to infer demographic characteristics, emotional states, and personality traits from bodily – but not necessarily biometric - data (Kak 2020 6).

The Article 29 Working Party, which provided guidance on the interpretation of EU data protection law before being replaced with the advent of the GDPR by the European Data Protection Board (EDPB), had defined what it designated as '**so-called soft biometrics'** as 'the use of very common traits not suitable to clearly distinguish or identify an individual but that allow enhancing the performance of other identification systems' (Art29 WP193 16).

Two important trends have actually been described in this area: first, there is literature on how to use soft biometric information to improve the performance of traditional biometric systems, and, second, there is work on how to predict 'soft biometrics' from traditional biometrics (Fairhurst, Li and Da Costa-Abreu 2017 370). Soft biometrics have themselves been divided into '**lower-level soft biometrics'**, dealing with prediction of demographic information typified by age and gender; and '**higher-level characteristics'**, about 'the prediction of what can be called the emotional or mental state of a subject' (idem).

It is not always straightforward to pinpoint the exact 'biometric' component of some technologies that are sometimes presented as related to or building on biometrics, unless this term is understood in a rather broad sense. For instance, some European Commission services have qualified as '**biometrics-enabled driver monitoring systems'** the systems developed to automatically detect and evaluate the level of awareness of drivers through detection of drowsiness and other distractions (European Commission 2018 4). It is unclear how levels of drowsiness could generally be speaking allow for uniquely identifying individuals. As already noted, the European Commission's proposed regulation on AI defines '**biometric data'** exactly as the GDPR, that is, as:

> 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique

> identification of that natural person, such as facial images or dactyloscopic data' (COM(2021) 206 final 42).

This legal definition can be qualified as **narrow** as, even though it potentially encompasses a broad spectrum of data related to possible physical, physiological and behavioural characteristics, such data will only qualify as biometric data if they allow or confirm the unique identification of an individual.

Broadly speaking, it is often stated that biometrics can be used for the purpose of verification, identification, or categorisation. **Biometric verification**, also known as authentication, concerns the (one-to-one) comparison between two sets of biometric data – for instance, two facial images – in order to determine whether they belong to the same person (FRA 2020(a) 6-7). **Biometric identification** refers to comparing a person's template with many other templates, to find out if that person's template image is part of the latter group; in relation to facial images, this is often referred to as 'automated facial recognition' (idem). **Biometric categorisation**, also referred to as segregation, may be described as a biometric technology used to extract information about an individual's characteristics in order to assign him or her to a certain category with predefined characteristics; in relation to facial images, this is sometimes referred to as 'face analysis' (FRA 2020(a) 6-8).

These notions might be technically and conceptually distinct, but nevertheless they can be **connected** in 'real life' practices. It is possible, for instance, to decide to first attempt to assign a person to a certain category in order to conveniently reduce the size of the group whose biometric data needs to be analysed for identification purposes.

In the context of this study it is important to note that here the term biometrics is not necessarily systematically used in the same sense as in EU data protection law – and thus in the same sense as in the proposed AIA, as the data processed might not allow per se for the identification of individuals, notwithstanding the fact that further processing might allow for such identification.

Other typologies of biometrics sometimes used distinguish between '**strong**' and '**weak**' biometrics – depending on their reliability for identifying individuals – and between '**generations**' of biometrics, on the basis of their historical emergence (Mordini, Tzovaras, and Ashton 2012 8-10).

Biometrics technologies can present important differences between them, as the behavioral and biological phenomena on which they are based have specific statistical properties, distinctiveness, and varying stabilities under different natural physiological conditions, in addition to triggering different environmental challenges (Pato and Millett 2010 4). The degree of universality, uniqueness, permanence and measurability varies between biometric techniques (Art29 WP193 3).

Progress in the field of biometrics technologies has been marked by the evolution of the algorithms used, as well as the evolution of hardware (eu-LISA 2015). Notable trends in the past years have included refining strategies for quick searches in biometric identification transactions, as the constant growth of databases to be searched represents a challenge for quick identification. It notably emerged that '[i]n situations where the person to be identified is present, the database can be trimmed based on gender, date of birth, nationality or other factors' (ibid. 33). In this context, the **categorisation** of individuals thus surfaced as a means to facilitate their **identification**.

The use of AI-enabled biometrics can lead to outcomes such as **false positives** and **false negatives**, a false positive being for instance the wrong match of a certain template with an individual (FRA 2020(a) 9)). The likeliness of a false positive is measured by the False Accept Rate (FAR) which quantifies the 'probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor' (Art29 WP193 6).[13] As the relevant algorithms are based on probabilities, when using these systems it is necessary to establish thresholds and rank-lists to determine how decisions about matches are taken (FRA 2020(a) 9-10). This can involve a 'trade-off' between foreseeable false positives and foreseeable false negatives (Art29 WP193 6), and in this regard it becomes important to assess if the rates diverge depending on some characteristics of the individuals – such as, for instance, their type of skin.

Studies of biometric technologies have often highlighted their limitations, most notably in terms of bias – with authors noting that some of the 'most egregious examples' of problems with these technologies 'occur reliably where gender, race, class, sexuality, and disability identities are constructed as other' (Magnet 2011 153).

Beyond the development of biometric technologies as such, an important ongoing development is the refinement of advanced data practices including biometric data but also its 'integration with big-data ecosystems which combine large datasets from multiple sources such as social media' (ICO 2021 5) or immigration data (ICO 2021 19).

The **exact demarcation between biometric technologies and other technologies** can be sometimes open to debate. In 2008, for instance, Karanja placed under the category of 'biometrics' – in addition to fingerprints, facial recognition, and iris recognition - the use of 'language testing as a form of identity control' by asylum and immigration authorities in Europe (Karanja 2008 340).

Nowadays, there a number of AI-driven, emerging technological solutions with potentially an important impact on fundamental rights that do not however necessarily fall under the category of biometric technology, although they might track individual's bodies, and sometimes track them in public spaces. This is the case for instance of systems deployed to **automatically detect individuals wearing face masks in public spaces** in the context of the Covid-19 pandemic, which can help illustrate ongoing trends and issues.

In March 2021, a French decree authorised the use of smart CCTV cameras to **measure the rate of population wearing face masks in public transport**.[14] The decree states that the collected images must be immediately transformed into anonymous data that can only be processed to determine a percentage of people wearing masks, and that the collection of any data allowing to classify people or to re-identify them is prohibited. The decree also exempts the pertinent personal data processing from basic data subject rights guaranteed under the GDPR – such as the right of access and rectification, and the right to object.[15]

In its assessment of the draft decree, the CNIL had pointed out that the systems being allowed by the instrument **do not have as an objective to process biometric data** (CNIL Délibération n° 2020-136 para. 8). It also noted that in the situation at stake it could be justified to limit the right to object,[16] but that generally speaking it is necessary to be cautious with the collection and systematic analysis of the images of individuals using public transport, and with the automated detection of some of their characteristics (ibid. 16). Such data processing, noted the CNIL, can indeed **generate**

[13] The likeliness of false negatives is measured by the False Reject Rate (FRR) which quantifies the probability that the system fails to match an individual to his/her own exisiting biometric template (Art29 WP193 6).

[14] Décret n° 2021-269 du 10 mars 2021 relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, JORF n°0060, 11 March 2021.

[15] Referring to Art. 23 GDPR.

[16] The exercise of the right to object in the described type of scenarios is sometimes challenging. The French company Datakalab, for instance, which develops computer vision products to monitor public spaces, states in its online data protection notice that the right to object can be exercised 'by nodding "no" to the device', more precisely with at least three movements of the head of more than 25 degrees (Datakalab 2021 10).

**a feeling of being under surveillance,** lead to habituation and banalisation, and ultimately result in increased surveillance (idem).

### 3.1.2. A variety of areas of use

The benefits and risks of using biometric technologies can vary depending on the area of use. Humanitarian organisations, for instance, increasingly adopt biometric technologies for reasons which include the technologies' potential for accurate individual identification, and for combating fraud and corruption – despite the fact that the use of biometrics in this context can trigger specific challenges (Kuner and Marelli (eds) 2020 129-130).[17]

The European Association for Biometrics (EAB) has stressed that biometrics 'have a strong impact on the **security** of European **borders** and other **governmental** and **commercial** applications', and devotes particular attention to EU data protection law compliance by supporting Privacy Enhancing Technology (EAB 2020 14).

Some of the areas in which the use of biometrics has gathered more attention over the years is **policing** (in both live contexts and in criminal investigations), but other areas that should also be mentioned are schools, corporate recruitment, supermarkets, airports and public transport in general (Kind 2021). At airports, facial recognition might be deployed on different grounds, including for commercial purposes.[18] In 2021 were launched for instance experiments with facial recognition for boarding planes at major French (Hue 2021) and Dutch airports.[19]

The Covid-19 outbreak is believed to have triggered an increased use of biometrics in areas such as **work surveillance** (Mascellino 2020).[20] The pandemic has also generated some novel situations such as a widespread use of online **proctoring**, sometimes relying on authentication and monitoring using facial recognition, which has resulted in a number of issues for students (see, for instance: Burt 2020). The wearing of face masks in public spaces has not stopped the remote identification of individuals. Already in May 2020, in this sense, the European Commission awarded a Seal of Excellence to a Spanish company developing facial recognition technologies allowing for the **identification of individuals wearing face masks** (Herta 2020).

Examples of potential future uses of biometrics that have gathered the interest of some actors are the possible use of live facial recognition for purposes such as age estimation at the entrance of age-restricted premises, for queue time monitoring and management in airports, and for photo matching at leisure attractions to allow purchasing photos through an app (ICO 2021 19).

The use of biometrics in **public spaces** triggers special concerns. 'Public spaces' may be understood in this context as generally including 'any physical space outside a domestic setting, whether publicly or privately owned', encompassing 'anywhere providing open access to the public, such as public squares, public buildings, transport interchanges or parks', as well as 'privately-owned premises such as shops, offices and leisure venues' (ICO 2021 12).

[17] Uses of biometrics in the aid context are extremely varied; see for instance, about a wearable digital necklace for infants aimed at reducing child mortality, including facial recognition of babies: Sandvik 2020. On this subject, see also: UNICEF 2019.

[18] Cf. for instance the Star Alliance Biometrics programme, which uses facial recognition at boarding gates, more information: https://www.lufthansa.com/be/en/information-on-data-protection. The CNIL has stated that certain uses of facial recognition for queue management at airport might be regarded as proportionate, as inappropriate queues could represent a security risk (CNIL 2020).

[19] See notably: https://www.schiphol.nl/en/page/facial-recognition-pilot-for-departing-travellers/.

[20] Mentioning examples of Dutch companies (a footwear chain and a department store) that had decided to impose – in 2019 – a compulsory fingerprint authorisation system for checkout staff: Das, De Jong and Kool 2020 98.

France has given much attention to the question of whether there is a need for **experimenting with facial recognition in public spaces**, after such experimentation was recommended in a governmental White Paper of 2020 (Ministère de l'intérieur 2020 263). The White Paper notably explicitly suggested that part of the experimentation should take place without the knowledge of the individuals affected, claiming that such secrecy could be based on public interest (ibid. 164).

The **Security Strategy** presented by the European Commission in 2020 stressed the importance of the protection of public spaces, referring to terrorist attacks that had targeted spaces such as places of worship and transport hubs (COM(2020) 605 final 9). In this regard, a footnote hinted that '[r]emote biometric identification systems deserve specific scrutiny' (idem). The European Commission also referred to its will to enhance public-private cooperation for the protection of public spaces, and to the launch of an **Urban Agenda** partnership on 'security in public spaces' in 2018 (ibid. 10).

**Security** a key driver of the development and deployment of biometric technologies. In 2017, the United Nations' Security Council adopted a Resolution which stated that 'Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters' (Resolution 2396 (2017) para. 15).

Many of the facial recognition initiatives that have seen the light in European territory are **local initiatives**, occurring at city level (Lequesne Roth 2021 31). Primarily concerned with transportation, these local developments have also been deployed in connection with cultural or sports events, punctually focusing on schools (ibid. 32). Sometimes, cities manifest interest in projects which might not involve facial recognition for identification purposes, but nevertheless are primarily concerned with the **massive monitoring and categorisation of pedestrians**, for instance in popular areas such as the city centre (on an initiative in Karlsruhe, cf. Marx 2020).

In Brussels, a number of actors including key mobility actors are supporting the Muntstroom project, a procurement programme for **people flow analytics** in the city centre, targeting major streets and public transport areas.[21] The project aims to collect data to be structured in accordance with what is described 'a set of metrics that are important to the understanding of public life', which would include categories such as age, gender and posture (Muntstroom PCP 2020 18), **automatically classifying pedestrians** for instance also depending on whether they are 'walking leisurely with intermittent stops', 'walking at an average human walking pace', or 'walking briskly and determined without looking anywhere but ahead' (ibid. 19).

The Impact Assessment accompanying the European Commission's proposal for the regulation on AI echoed the interest of Italy in the facial recognition system Sistema automatico di riconoscimento delle immagini (Sari),[22] its proliferation in train and bus stations in Madrid (Peinado 2019), but also the investigation by the Greek data protection authority about the use of facial recognition by the police in Greece (Homo Digitalis 2020) (SWD(2021) 84 final 18).

The processing of biometric data has been actively supported at EU level[23] in the context of EU-level large-scale IT systems in the **Area of Freedom, Security and Justice (AFSJ).** These systems, initially set up by the EU for asylum- and migration-management but increasingly also serving internal security, almost systematically rely on biometric data (FRA 2018). The EU Agency for Fundamental

[21] More information: https://www.stib-mivb.be/article-pro.html?l=en&_guid=90c280fa-8afa-3810-968f-eb0cea5e2307.

[22] On this case and others, see also: EDRi 2020(b) 20 and ff.

[23] For an overview of national laws of EU Member States on the processing of facial images, see notably: Ernst & Young Baltic AS 2020.

Rights has highlighted that the impact of these large-scale IT systems on fundamental rights remains largely unexplored territory (FRA 2018 19).

It is in this context that can be found the assertion that 'the use of biometrics is **necessary** as it is the most reliable method of identifying third-country nationals within the territory of the Member States' (Recital (25) of Regulation (EU) 2019/816).[24] Currently, the processing of **facial images** is foreseen in the context of all EU large-scale IT systems in this area, except for the European Travel Information and Authorisation System (ETIAS) (FRA 2020(1) 13). The majority of these systems encompass also the processing of other biometric identifiers, most notably **fingerprints**. This is for instance the case in the context of the oldest of these information systems, the Schengen Information System (SIS), which is regulated by multiple legal instruments,[25] as well as Eurodac and the Visa Information System (VIS). The VIS, which facilitates the exchange of data between Member States on applications for short-stay visas and on the decisions taken in relation thereto, for instance foresees the processing of fingerprints[26] and of photographs. Eurodac contains the fingerprints of asylum applicants and from persons apprehended in an irregular border crossing, operating since 2003.

In general, the processing of facial images in this context supports biometric verification in order to double check an individual's identity, in situations in which individuals are supposed to be in principle aware that the authorities are processing their facial image. Regulation (EU) 2018/1862, on the use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, left however the door open for uses of facial recognition yet to be determined. The regulation establishes indeed that facial images should initially be used **for identification purposes only in the context of regular border crossing points**. However, the instrument also confers on the European Commission, for an indeterminate period of time starting from December 2018, the power to adopt delegated acts concerning the determination of the circumstances in which **facial images may be used to identify persons, other than in the context of regular border crossing points** (Article 43(4) and 75(2) of Regulation (EU) 2018/1862).[27]

The upcoming **Entry/Exit System (EES)**[28] also deserves special mention. The EU Agency for the Operational Management of Large-Scale IT Systems in the AFSJ (eu-LISA) has observed that the Entry/Exit System (EES) 'incorporates a component for **automated biometric matching,** which will rely on machine learning techniques for biometric matching' (eu-LISA 2020 5).

[24] Discussing the fixing of identities as a driver for the use of biometrics: Martin and Whitley 2013.

[25] See notably Regulation (EU) 2018/1861 and Regulation (EU) 2018/1862, as well as Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, OJ L 312, 7.12.2018.

[26] Defined as 'the data relating to the five fingerprints of the index, middle finger, ring finger, little finger and the thumb from the right hand and, where present, from the left hand' (Art. 4(14) of the consolidated text of Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

[27] Equivalent provisions are to be found in Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L 312, 7.12.2018.

[28] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017.

The purpose of the EES is to record and store the date, time and place of entry and exit of third-country nationals, calculate the duration of their authorised stay, generate alerts to Member States when an authorised stay has expired, and record and store the date, time and place of refusal of entry. In this context, it will be possible for the immigration authorities of Member States to compare the **live facial image of a third-country national** with the facial image stored in the system for verification purposes (Article 26 of the EES Regulation), which shall in any case 'have sufficient image resolution and quality to be used in automated biometric matching' (Article 15(4) of the EES Regulation). In addition, the EES Regulation also foresees that in certain cases it will be possible for both border and immigration authorities to carry out searches in the system:

> 'with the fingerprint data or the fingerprint data combined with the facial image, **for the sole purpose of identifying any third-country national** who may have been registered previously in the EES under a different identity or who does not fulfil or no longer fulfils the conditions for entry to, or for stay on, the territory of the Member States' (Article 27 of the EES Regulation).

It is also important to mention the regulation on the **interoperability between EU information systems in the field of borders and visa**, Regulation (EU) 2019/817. This regulation provides for the creation of a shared biometric matching service ('shared BMS'), notably to be used in order to perform multiple-identity detection every time individual files (or applications or alerts) are created or updated in a large-scale IT system which foresees the use of biometrics (Article 27 of Regulation (EU) 2019/817).

The Interoperability policy initiative gave birth to the European Search Portal (ESP), a search portal allowing to submit queries to simultaneously query the EES, ETIAS, VIS, SIS, Eurodac, ECRIS-TCN, a newly created a Common Identity Repository (CIR), Europol data, and Interpol databases. The users of this portal will have the power to launch queries by submitting either alphanumeric or **biometric data** to the ESP.

The agency eu-LISA is responsible for the operational management of Eurodac, of the second generation Schengen Information System (SIS II), and of the Visa Information System (VIS), and leads the development of the EES, ETIAS, and ECRIS-TCN, as well as the realisation of the interoperability of these systems. In the context of their management and development, eu-LISA has awarded significant contracts to European companies active in the area of biometrics (Monroy 2020). In June 2020, IDEMIA and Sopra Steria announced they have entered into a framework contract with EU-Lisa for the delivery of the shared Biometric Matching System (sBMS) developed for the interoperability of systems, described as a system that will be '**one of the largest biometric systems in the world**, integrating a database of over 400 million third-country nationals with their fingerprints and facial images' (Havas Paris 2020).

Eu-LISA has not only a prominent role in the management of large-scale databases with biometric data, but also a documented keen interest in AI. In a report published in 2020, eu-LISA noted that 'the Agency can support the development and adoption of AI in the domain of borders, migration and security by, for example, supporting the necessary computational infrastructure for the development and testing of AI tools for the key stakeholders' (EU-Lisa 2020 5).[29]

### 3.1.3. Remote biometric identification

The expression '**remote biometric identification'** is nowadays being used by EU institutions primarily to discuss the regulation of certain uses of facial recognition. **Facial recognition** technology refers broadly speaking to the technology allowing for the automatic identification of an individual by matching two or more faces from digital images (FRA 2020(1) 2). Technically, facial

[29] The proliferation of biometric technologies in relation to borders is a phenomenon not limited to the EU; for a Canadian perspective on facial recognition and borders, for instance, see: Israel 2020.

recognition can be envisaged as a subcategory of the sphere of AI known as 'computer vision' (Wickert 2019 2), or a form of pattern recognition (Berle 2020 11). It takes as a starting point that 'facial images are probably the most common biometric characteristic used by humans to make a personal identification' (Datta, Datta and Banerjee 2015 4). Facial recognition technology should in any case never be expected to be 100% accurate and reliable (Wickert 2019 3), due to its probabilistic nature.

**Live facial recognition technology** is an expression often used to describe the practices consisting of comparing in **'real–time'** footage obtained from video cameras (CCTV) with facial images in databases (FRA 2020(1) 1).

In the proposed regulation on AI, the European Commission suggests regulating live facial recognition through the notion of remote biometric identification, further specified under the notion of '**real-time** remote biometric identification systems'. As noted, the proposal defines **remote biometric identification systems** as AI systems:

> 'for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified' (proposed Article 3(36) AIA).

Next, the proposal defines **'real-time' remote biometric identification system** as:

> 'a remote identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention' (proposed Article 3(37) AIA).

Three elements stand out in this definition: remote biometric identification systems serve the purpose of **identifying individuals at a distance**, comparing their biometric data with data **in a database**, and **without knowing** if the individual at stake is actually there or not. In other words, these are AI systems used for **searching for individuals on the basis of available biometric data** (e.g., a facial image).

European Commission's services[30] had in the past used the expression '**biometric mass surveillance'** to refer to '[r]emote biometric identification' as 'the use of technology for **identifying – out of a mass of people** – individuals through the use of unique biological characteristics, such as face, gait or voice, at a distance in publicly accessible spaces' in a summary of responses to a consultation on AI policy (EC DG CONECT 2020 11).

Remote biometrics are sometimes described as 'nonintrusive' (Datta, Datta and Banerjee 2015 xxiii), in the sense that biometric data such as facial templates can be collected without interfering physically with the individuals concerned. Remote biometric identification has in this sense been described as having a 'frictionless' nature by the EDPB and the EDPS (Joint Opinion 5/2021 11). This lack of obtrusion and friction represents as such a potential issue for the individuals, who might as a consequence not become aware of the fact that data about them is being processed, which makes the systems potentially particularly **intrusive** from a human rights and ethical perspective.

A number of controversies have accompanied the development of facial recognition technologies, for instance concerning the rights of the individuals whose images have been used to train the algorithms (Satisky 2019, Peng 2020).

[30] Directorate-General for Communications Networks, Content and Technology.

The UK's Information Commissioner has identified as most notable issues connected to the use of live facial recognition the governance of the systems, the automatic collection of biometric data at speed and scale without clear justification, a lack of choice and control for individuals, transparency and data subjects' rights, the effectiveness and the statistical accuracy of the systems, the potential for bias and discrimination, the governance of watchlists and escalation processes, the processing of children's and vulnerable adults' data, and the potential for wider, unanticipated impacts for individuals and their communities (ICO 2021 6).

Facial recognition can be used in a variety of contexts. It has particularly attracted the attention of **law enforcement**. In the US, police use of facial recognition is widespread (Spivak and Garvie 2020 87). It must be stressed that not all facial recognition systems fall under what is described as remote biometric identification. For instance, facial recognition can be used exclusively for authentication purposes, in a variety of contexts, by private or public authorities.[31]

Also, it is important to underline that the term facial recognition can sometimes be used with variable meanings, for instance as a broad term to encompass **face detection**, **facial analysis** or **facial recognition** in a narrow sense (for instance, to recognise the presence of a face). Some for instance classify face detection, **face classification** and face recognition under automated facial analysis (Buolamwini and Gebru 2018 2). Some of these practices might not involve the processing of biometric data, and, depending on the context, it could be that the data processing does not necessarily fall under the notion of personal data processing.

A whole range of practices not necessarily relying on biometrics have indeed emerged surrounding live facial recognition, in particular in the digital-out-of-home advertising sector (ICO 2021 17). Typically billboards will be fitted with cameras aiming not necessarily at capturing biometric templates, but rather at estimating characteristics such as age, gender, or ethnicity, or detecting brands (ICO 2021 19). Some commercial practices such as the deployment of 'smart billboards', which combine facial detection and ephemeral data processing, have triggered some hesitations among data protection law experts regarding how to guarantee that processing of personal data is legally recognised as such – in particular when those processing data claim that the individuals monitored cannot be 'identified'.[32]

For the purposes of determining the legal rules applicable to these systems, it is crucial to examine first whether the processing of data involves or not the processing of data allowing for the **identification of individuals**, that is, whether it will be regarded or not as personal data[33] processing, and, second, whether the data processed can be qualified as biometric data.

In 2017, for instance, the Italian data protection authority, the Garante per la Protezione dei Dati Personali, investigated the installation nearby the central station of Milan of 'digital signage' advertisement screens, which had been described as enabling facial recognition and tracking (Garante 2017). The Garante nevertheless concluded that the responsible company's devices did only very briefly process images of passers-by, and **not in order to obtain any template of their faces or to identify them** but to determine the presence of a human face in a specific area; to calculate the duration of such presence; to infer information such as gender, age range, and distance

[31] For example, in Morocco the use of facial recognition for authentication to benefit from welfare services is now permitted, with the approval of the competent data protection authority (CNDP 2020).

[32] On this issue, see notably: Earls Davis 2020. A pararell data protection issue concerns the use of CCTV cameras to protect billboards from attacks (cf. in this sense the judgment of VG Mainz, ECLI:DE:VGMAINZ:2020:0924.1K584.19.00).

[33] The GDPR defines personal data 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' (Art. 4(1) GDPR).

from the device; and to carry out statistical analysis to evaluate the level of enjoyment of the advertising messages. All in all, the authority concluded the devices carried out '**facial detection'** but not '**facial recognition'**, to the extent that they were unconcerned with the processing of biometric data, and thus data protection law applied, but only its general rules, not the ones on special categories of data (idem).

There seems to be some hesitation among some data protection authorities regarding how to apprehend biometric data processing, at least terminologically. In its reaction to the *White Paper on AI* of the European Commission, and discussing specifically remote biometric identification, the EDPS called for a moratorium on '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**' (EDPS 2020 2), as if remote biometric identification could encompass the processing of data other than biometric data, or behavioural signals could not biometric data.

In relation to facial recognition, a significant development in is the emergence of private companies that offer certain facial recognition services. Among them stands out **Clearview AI**, which attracted global controversy in 2020 for scrapping massive amounts of facial images, matched to names and other information, taken from the web without the individuals' consent, and using these photos and information to market surveillance tools addressed to private and public actors (Kak 2020 7). An investigation by Canadian authorities concluded the mass collection of images by Clearview AI, in what was described as an '**unreasonable** manner, via indiscriminate scraping of publicly accessible websites', and creation by Clearview AI of biometric facial recognition arrays was **inappropriate**, notably because the company used the images for purposes unrelated to their original publication, often to the detriment of the individual whose images are captured and create a risk of significant harm to those individuals, the vast majority of whom have never been and will never be implicated in a crime (Office of the Privacy Commissioner of Canada et al. 2021).

A Polish company named **PimEyes**, which describes itself online as offering 'face search engine reverse image search',[34] was later decried for offering a similar product, albeit even more problematically to any members of the public (Laufer and Mainek 2020). In May 2021, the data protection authority of Baden-Württemberg[35] opened an investigation concerning PimEyes (LFDI 2021).

### 3.1.4. Biometric categorisation

The proposed regulation on AI defines **biometric categorisation systems** as AI systems 'for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, **on the basis of their biometric data**' (proposed Article 3(35) AIA). A first key element of this definition is that it construes biometric categorisation systems as requiring the **processing of biometric data**, that is, of data defined as allowing for the unique identification of individuals, but such processing should not be carried out in order to uniquely identify them – instead, **to assign them to categories**.

A second key element of the definition is that the examples of categories mentioned, that is, 'sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation', **correspond partially to the categories of data recognised in EU data protection as special categories of data**, but not fully: some special categories of data recognised as such under EU data protection law are not mentioned in the definition, or only in different terms, while some categories presented here

[34] See: https://pimeyes.com/en. The exact location of the company is unclear, the website currently refers to an address in the Seychelles, but it has been pointed that until August 2020 a Warsaw address was used (Metz 2021).

[35] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit.

are not regarded as special categories of data under EU data protection law. It is thus unclear what is the exact rationale behind the selection of the mentioned categories.

In this sense, it should be recalled that the GDPR regards as processing of special categories of data the 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' (Art. 9(1) GDPR).

Under the proposed definition of biometric categorisation systems, a system assigning to an ethnic origin would be covered, while one assigning to a racial origin would not; a system assigning to a political orientation would be covered, while one assigning to religious or philosophical beliefs or trade union membership would not; a system assigning to a sexual orientation would be covered, but one assigning to a certain type of sex life would not. The logic of these choices is unclear.

Biometric categorisation is in any case also presented as applying when biometric data are used to assign to an age or sex, which **are not categories regarded as special categories of data** under EU data protection law, although certainly AI systems assigning individuals to such categories devote attention.

In relation to 'sex', it must be noted that the AI proposal here diverts from the currently most often used term of '**gender**'. There has been much critique of automated gender classification, also sometimes referred as **automated gender recognition** (Keyes 2018).[36] Buolamwini and Gebru (2018) highlighted that 'gender classification' features in facial analysis typically uses the binary labels of female and male, following a 'reductionist view of gender does not adequately capture the complexities of gender or address transgender identities' (ibid. 6).

Finally, some other categories mentioned in the proposed definition of biometric **categorisation** systems appear to be directly connected to a possible future **identification** of individuals: assigning to a certain hair colour, eye colour, or tattoos, might indeed constitute an intermediary step towards locating somebody, who could be searched more efficiently on the basis of such information.

The lack of manifest logic in the definition of biometric categorisation systems might be due to the fact that **there is currently no established definition** of this practice in Europe.

The Article 29 Working Party had pointed out in 2012 that '[d]ue to the recent technological developments it is now also possible to use biometric systems for categorisation/segregation purposes' (Art29 WP193 4). They described what they called '**biometric categorisation/segregation'** as 'the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action', noting that in these cases, 'it is not important to identify or verify the individual but to assign him/her automatically to a certain category' (Art29 WP193 6).

In this context, the Article 29 Working Party provided as an example of biometric categorisation/segregation an advertising display that 'may show different adverts depending on the individual that is looking at it based on the age or gender' (idem). Another example of categorisation offered by the Article 29 Working Party was the use of facial recognition systems 'to count demographics of visitors to an attraction' (Art29 WP193 22). These examples, however, bring

[36] Presenting it as a type of identity classification in automated facial analysis technology: Scheuerman, Paul and Brubaker 2019.

back the question of whether the attribution to a certain category is effectively based on biometric data, as the document implied, or not.

The Consultative Committee of the Convention 108 has more recently stated that:

> 'the use of facial recognition **for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health condition or social condition** should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination' (T-PD(2020)03rev4 5).

The statement appears to endorse that facial recognition technologies can allow to determine, for instance, the 'social condition' of individuals, although it is not clear how such attribution should take place, at least on the basis of facial recognition understood narrowly. What the statement seems to aim at highlighting is that certain uses of facial recognition, or connected to it, **go beyond the purpose of uniquely identifying individuals**, focusing instead of categorising them, which is nevertheless not deprived of risk – especially a risk of discrimination – and should thus be generally prohibited. The requirement that what should be prohibited is facial recognition exclusively aiming ('for the sole purpose') at **categorising** is in any case difficult to reconcile with the fact that it might apply only to biometric data, defined in reference to their **identification** potential.

In any case, the idea that certain information about individuals such as their **gender** can be inferred **from biometric data**, must be approached with extreme caution, as it typically either endorses a very broad notion of biometric data, or a problematic notion of gender identification, or both.

In this sense, it is worth knowing that the EDPS and the AEPD stated in a co-published document that '[d]epending on the biometric data collected, data can be derived from the subject such as race or gender (even from fingerprints)' (EDPS & AEPD 2020 1). The reference provided to back up this claim, however, refers to the **analysis of amino acids in finger marks found in crime scenes** (De Puit, Ismail and Xu 2014), the collection of which does not necessarily fall under what EU data protection law qualifies as processing of biometric data as a special category of data, if such processing is about measuring the presence of amino acids, as opposed to identifying individuals.

There is controversy about which information can exactly be legitimately attributed to individuals on the basis of biometric data processing. The EU Agency for Fundamental Rights has noted that '[c]haracteristics commonly predicted from facial images are sex, age and ethnic origin' (FRA (2020)(1) 8), while also commenting that researchers and companies have experimented with inferring other characteristics from facial images, such as sexual orientation (idem). While this might be true, the facial images at stake might not constitute biometric data.

A paper sometimes quoted to support the idea is that facial recognition allows to attribute **political orientation** to individuals is 'Facial recognition technology can expose political orientation from naturalistic facial images' (Kosinski 2021). The paper notably examines the predictability of political orientation exploring correlations between political orientation and 'a range of interpretable facial features including **head pose** (...); **emotional expression** (...); **eyewear** (...); and **facial hair**' (idem). As such, the paper is thus not directly concerned with inferring political orientation from biometric data, as the described data **do not constitute biometric data**, as a general rule.[37] Similarly, other researchers have been also exploring possible correlations between personality and facial images, but again not on the basis of the processing of biometric data (Kachur et al. 2020).

[37] For instance, eyewear may only be regarded as referring to somebody's physical characteristics if this notion is very broadly interpreted; also, for eyewear to be regarded as biometric data it should allow or confirm the unique identification of a natural person, but also constitute data processed through a 'specific technical processing'; mere information about 'the person with sunglasses', even if related to clearly to one specific individual in a specific context, will not constitute as such biometric data.

A dispatch published by the EDPS (EDPS 2021) mentions as an example of research on facial emotion recognition allowing for the '**detection of political attitudes**' that tried to measure 'spontaneous emotionally congruent facial responses' by means of electromyography (EMG) tracking of facial muscle activation in participants reading sentences describing politicians' emotional expressions (Fino et al. 2019). Equally, this would not generally fall under the definition of processing of biometric data in EU law, as such measurement can most probably not be used to identify a particular person.

A paper sometimes quoted to illustrate that **sexual orientation** could be **inferred from biometrics** is 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images' (Wang and Kosinski 2018). In this paper, the researchers processed images obtained from public profiles posted on a US dating website, leading them to findings such as '(a)verage landmark locations revealed that gay men had narrower jaws and longer noses, while lesbians had **larger jaws**', or that 'heterosexual men and lesbians tended to **wear baseball caps**' (idem). A replication study stressed that it is unclear to which extent the degree of predictability of sexual orientation from the type of images analysed might be influenced by biological features such as facial morphology, and how much by differences in presentation, grooming and lifestyle (Leuner 2019 52). In any case, this type of research was definitely not concerned with the possibility of inferring sexual orientation information **from biometric data**.

It is crucial to note that legal disputes around the possibility for public authorities to assert somebody's sexual orientation regardless of the individual's personal statement are not unknown in the EU, the most important examples emanating from the reliance on tests and expert views in the context of asylum applications.[38] In this context, it becomes particularly important to avoid backing up false claims according to which AI systems could accurately determine, on the basis of biometric data, the sexual orientation of individuals.

Research on detection of **ethnic origin** based on facial recognition has also sparked much controversy, in particular linked to research on 'ethnical group face recognition' encompassing the Chinese Uyghur (Van Noorden 2020).[39]

The impact assessment accompanying the proposal for a regulation on AI acknowledged that 'there are serious doubts as to the scientific nature and reliability' of both biometric categorisation and emotion recognition (SWD(2021) 84 final, Part 1/2 19).

Finally, it should be noted that categorisation systems can be based on visual information, but they might also be based on **audio information**. In May 2021, an international coalition of musicians and civil society organisations called Spotify to commit not to use a patent the company had obtained early this year regarding speech-recognition technology (18 Million Rising et al. 2021). The patent at stake, named 'Identification of taste attributes from an audio signal', notably aims at analysing speech to assign the speaker to categories such gender (based on speech frequency information)[40], age (based on information such as vocal tract length and pitch), or emotional state (based on prosodic information) (Hulaud 2021).

### 3.1.5. Emotion recognition

The AI regulation proposal defines **emotion recognition systems** as AI systems 'for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data' (proposed Article 3(34) AIA). Like in the previously discussed notions, those systems are defined as

[38] Cf. for instance: Poddar and Rajam 2018.

[39] For this type of research, see for instance: Cunrui et al. 2019.

[40] On these approaches, see notably: Ali, Islam and Hossain 2012.

operating on the basis of **biometric data**. Here the main difference is that instead of aiming at identifying somebody, or at assigning them to concrete specific categories, the purpose is to glean individuals' '**emotions or intentions'**. There can nevertheless be a thin line between inferring emotions and intentions, on the one hand, and attributing individuals to certain categories, on the other, for instance when AI systems aim at 'detecting' certain reactions in people in order to assign them to certain categories.

Emotion recognition has been described as a 'biometric technology' which is, however, not concerned with who people are – by identifying them or authenticating their identity – but rather with **how they feel** (Article 19 2021 13). Emotion recognition can be connected to a variety of technologies, but the most commented is what could be defined as **facial expression-based and multimodal emotion recognition** that includes face analysis (idem 15).

Emotion recognition relies on machine learning. The algorithms used for emotion recognition are often trained with data from databases in which individuals pose, representing manifestations of specific emotions.[41] It is sometimes amalgamated with 'facial expression analysis', understood as 'systems that attempt to automatically analyze and recognize facial motions and facial feature changes from visual information'.[42]

In addition to or instead of **faces** as such, could be analysed for the purposes of emotion recognition **body movements** or **voice tone**, for instance. Emotion recognition is indeed not necessarily connected to the visual reading of body expressions, but may also occur through sound. In 2012 the Article 29 Working Party noted that:

> '[i]n addition to using voice recognition as a biometric for identification, a relatively common use involves the identification of specific features within the voice pattern to categorise the speaker', giving as an example 'to analyse the responses of an individual throughout a telephone conversation to **identify stress patterns** and speech irregularities to highlight potential cases of fraud' (Art29 WP193 24).

The quote illustrates that distinguishing between inferred **emotions** and **intentions** is not always easy or relevant, as the AI system described would be concerned with identifying an emotional state (that is, stress) to the extent that it is conceived as a manifestation of an intention (that is, deception). '**Intention recognition'** technologies have historically grown closely connected to 'emotion recognition', notably building on the assumption that there exists a 'strong relation between emotional states and intentions', for instance because '[a]nxiety status can easily lead to an unpredictable action or a violent reaction' (Tistarelli and Grosso 2010 83).

Emotion recognition has been regarded as being particularly problematic for various reasons. First, it is highly contestable that it works as purported by its advocates: researchers have noted that despite the effort in connecting facial movements to emotion, there are no 'reliable 'fingerprints' for emotion categories', and no 'reliable facial movements to express these categories' (Feldman Barrett et al. 2019 49).

Second, emotion recognition is often in practice deployed in a way that eventually leads to **identifying**, **tracking**, and **classifying** individuals across a variety of sectors (Article 19 2021 16). A report on the deployment of emotion recognition in China recently highlighted **numerous problematic ongoing developments**, in contexts including research for and use in security settings (for 'early warning', closer monitoring after initial identification of a potential threat, and

[41] See, for instance, some of the databases listed here: https://face-rec.org/databases/.

[42] Stressing that such 'facial expression analysis' shall not be confused with 'emotion analysis in the computer vision domain', for which 'higher level knowledge is required': Tian, Kanade, and Cohn 2011.

interrogation), monitoring of drivers (also from outside of vehicles, for instance to detect drivers likely to commit highway fare evasion), and education (Article 19 2021).

The very grounds of emotion recognition have been criticised. The United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has observed that 'affect recognition', which 'seeks to infer a person's feelings, emotions or intentions from facial expressions', is '**based on highly questionable classification systems**' (United Nations Special Rapporteur 2019 5).

The European Data Protection Supervisor (EDPS) services have used the expression '**facial emotion recognition (FER)**' to refer to 'the technology that analyses facial expressions from both static images and videos in order to reveal information on one's emotional state' (EDPS 26 May 2021). Noting these technologies belong to the family of technologies often referred to as 'affective computing', they described FER as involving three distinct steps: a) face detection, b) facial expression detection, and c) expression classification to an emotional state (idem). In their view, FER 'can also **be combined with biometric identification'** (idem), which seems to suggest that they would not interpret FER as necessarily requiring the processing of processing of biometric data. However, in the same document FER is always described as a biometrics technology.

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) has taken some distance with the **credibility** of what it calls '**affect recognition'**, noting it could 'be carried out with facial recognition technologies to arguably detect personality traits, inner feelings, mental health or workers' engagement from face images' (T-PD(2020)03rev4 5). For the Consultative Committee, this type of affect recognition 'for instance, to hiring of staff, access to insurance, education may pose risks of great concern, both at the individual and societal levels and should be prohibited' (idem).

The EU Agency for Fundamental Rights has conceded that '[f]acial recognition technology can also be used to infer emotions, such as anger, fear or happiness, and to detect whether people are lying or telling the truth' (FRA (2020)(1) 8), referring to such technology as **a type of biometric categorisation**.

All **major US companies** currently offer emotion recognition services and products, for instance Google via Vision AI, or Amazon through the Amazon Rekognition API.[43] Apple bought a start-up operating in this area already in 2016 (Misener 2016). Microsoft is actively researching how to automatically detect 'affective responses from audience members during online presentations', analysing facial responses and head gestures of participants in Microsoft Teams online events (Hernandez et al. 2021).

The use of 'emotion recognition' is developing globally in a variety of settings. Emotion recognition systems which would have been used by police, nuclear power station operators, airport security and psychiatrists in Russia, China, Japan and South Korea, and deployed at an Olympic Games, FIFA World Cup, and G7 Summit (Wright 2021). There were reports about a police initiative in India to set up cameras to automatically 'detect distress on women's faces and alert officers', by detecting changes in facial expression, as a way to tackle sexual harassment and violence in public spaces (Ara 2021, TNN 2021).

[43] Noting that the product provides information on 'The emotions that appear to be expressed on the face, and the confidence level in the determination', and that 'The API is only making a determination of the physical appearance of a person's face. It is not a determination of the person's internal emotional state and should not be used in such a way' (https://docs.aws.amazon.com/rekognition/latest/dg/API_Emotion.html). Amazon further clarifies: 'For example, a person pretending to have a sad face might not be sad emotionally'.

A specific use of emotion recognition technologies is the use of AI for **lie detection.** The Article 29 Working Party had described as a type of behavioural characteristics which can be a source of biometric data '**patterns indicating some subconscious thinking like telling a lie'** (Art29 WP193 4). In this context, it should be noted that some Member States have their own rules on polygraphs.[44]

## 3.2. Overview of the regulatory framework

There is currently no European legislation exclusively on biometrics, as there is not, at this moment, European legislation on AI – although there is a legislative proposal on the table of the EU legislator. Regarding biometrics, the most directly relevant specific rules of EU law are to be found in EU data protection law. In addition, the whole existing EU fundamental rights architecture is fully applicable.

This section briefly describes such architecture and presents the relevant rules on biometrics and on automated decision-making to be found in EU data protection law. It also presents the most important case law in this area emanating from the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR). Overall, the section shows that ongoing developments are taking place amidst – and possibly also somehow *despite* – existing rights and principles, which might thus possibly need to be reinforced, clarified, or fine-tuned.

### 3.2.1. General fundamental rights framework

The European architecture for **fundamental rights** delineates the general framework for the use of biometrics and AI in the EU. It is marked by Article 2 and Article 6 of the Treaty of the European Union (TEU). Article 2 TEU states that 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 TEU notably establishes the legally binding force of the Charter of Fundamental Rights of the European Union (EU Charter).[45] In the EU Charter are recognised a number of rights very often perceived as being potentially negatively impacted by AI, such as the right to respect for private life,[46] the right to the protection of personal data,[47] and the right to non-discrimination.[48]

As a matter of fact, almost **all fundamental rights** recognised as EU fundamental rights in the EU Charter are potentially put at great risk by certain developments of AI. In this sense, for example, the tracking of individuals in public spaces can directly threaten the right to freedom of assembly and

[44] For instance, authorising polygraphs in Belgium: Arrêté Royal du 28 juin 2021 portant exécution de l'article 112duodecies, § 4, alinéa 3, et § 7, du Code d'instruction criminelle déterminant les informations minimales devant figurer dans le procès-verbal de consentement et portant établissement des exigences techniques auxquelles l'appareil avec lequel le test polygraphique est effectué, doit répondre, Numac : 2021041700.

[45] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

[46] Art. 7 EU Charter: '*Everyone has the right to respect for his or her private and family life, home and communications*'.

[47] Art. 8 EU Charter: '*1) Everyone has the right to the protection of personal data concerning him or her. 2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3) Compliance with these rules shall be subject to control by an independent authority*'.

[48] Art. 21 EU Charter: '*1) Any discrimination based on any ground such as 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 shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited*'.

of association.[49] Also, certain uses of biometric technologies could affect the right to a fair trial.[50] Importantly, some uses of AI systems can be regarded as a threat to **human dignity**, for instance because they aim at substituting human free will with a computer decision.[51]

The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[52] binds all EU Member States directly and is thus also relevant for the interpretation of the provisions of the EU Charter. To complete the EU fundamental rights architecture, the fundamental rights as guaranteed by the ECHR are also to be mentioned as they result from the constitutional traditions common to the Member States, which serve as a foundation of the general principles of EU law.

### 3.2.2. EU data protection law

Biometric data are currently explicitly regulated through general EU data protection law instruments such as the GDPR. In contrast, in the United States (US), some States have passed biometric privacy laws already since in 2017, the most notable example possibly being the Illinois' Biometric Information Privacy Act (BIPA).[53] The US has also witnessed interesting developments about protection from facial recognition in a consumer protection context, such as a settlement between a company and the Federal Trade Commission (FTC) which led to deleting facial images unlawfully processed by an app, but also 'any facial recognition models or algorithms developed' by the company with the contested photos and videos (FTC 2021).

It is important to note that the three major instruments of EU data protection law – the GDPR, the LED and the EU DP Regulation – have been adopted exclusively on the basis of Article 16 of the Treaty on the Functioning of the EU.[54] This provision has also been identified by the European Commission as one of the legal bases for the proposed regulation on AI, to the extent to which the proposal 'contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement' (proposed Recital 2 AIA) (COM(2021) 206 final 42).

[49] Art. 12 EU Charter: '*1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests. 2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.*'

[50] Art. 47 EU Charter: '*Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.*'

[51] In this sense, see for instance EDPB and EDPS, Joint Opinion 5/2021 12. Art. 1 EU Charter states: '*Human dignity is inviolable. It must be respected and protected.*'

[52] Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe Treaty Series 005, 1950.

[53] Which notably highlights that: '*The full ramifications of biometric technology are not fully known*' (Section 5(f)). Biometric Information Privacy Act 2008 (BIPA) 740 ILCS 14/1. This Act is the legal background of a major settlement that took place in 2020, involving the company Facebook and allegations about the use of facial recognition in connection with Instagram (Cox 2021).

[54] Art. 16 TFEU states that: '*1) Everyone has the right to the protection of personal data concerning them. 2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.*'

## On biometric data

The 1995 Data Protection Directive[55] did not refer explicitly to biometric data, even though its provisions had been interpreted as encompassing biometric data. It was with the adoption of the GDPR and the LED in 2016 that EU data protection law for the first time explicitly tackled the regulation of biometric data (Kindt 2020 63).

The GDPR indeed explicitly considers the processing of **biometric data for the purpose of uniquely identifying a natural person** as the processing of a **special category of personal data**, or 'sensitive data', which shall in principle be **prohibited**.[56]

The EDPB has stressed that for data to be regarded as biometric data under the GDPR, and taken into account the definition in Article 4(14) GDPR, three types of criteria must be considered: concerning the **nature of data** (data must relate to physical, physiological or behavioural characteristics of a natural person), concerning the **means and way of processing** (data must result from a specific technical processing) and concerning the **purpose of processing** (data must be used for the purpose of uniquely identifying a natural person) (EDPB, Opinion 3/2019 18). In this sense, the EDPB has noted that the video footage of an individual cannot in itself be considered processing of biometric data in the sense of Article 9 GDPR (idem), and that 'when the purpose of the processing is for example **to distinguish one category of people from another** but not **to uniquely identify anyone** the processing does not fall under Article 9' (ibid. 19).[57]

The GDPR details, in any case, a series of conditions under which, exceptionally, the processing of special categories of data such as biometric data can take place - under Article 9(2) GDPR. In addition, the GDPR establishes that 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health' (Article 9(4) GDPR).

The GDPR does not apply to all processing of personal data. When personal data are processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, by authorities competent for such purposes, the LED will apply instead. Under the LED, the processing of biometric data is **not formally prohibited**. It is allowed, even if 'only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

> (a) where authorised by Union or Member State law;
>
> (b) to protect the vital interests of the data subject or of another natural person;
>
> or (c) where such processing relates to data which are manifestly made public by the data subject' (Art. 10 LED).[58]

[55] 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, pp. 31–50.

[56] In this sense, Article 9(1) GDPR states: '*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*'.

[57] Although it is possible that biometric data processing occurs if the purpose of the processing of the video footage is for instance to detect a data subject re-entering an area or entering another area (EDPB, Opinion 3/2019 19).

[58] Is currently pending before the CJEU a request for a preliminary ruling on the possibilities for Member States to impose certain collection of biometric data (in reference concretely to a Bulgarian law providing, as a general rule, for the taking of photographs for the file, the taking of fingerprints, and the taking of samples in order to create a DNA profile for all persons who are charged with a premeditated criminal offence requiring public prosecution) (Case C-205/21).

When the processing of personal data is carried out by EU institutions and bodies, in principle the EU DP Regulation should apply. Under this regulation, like under the GDPR, the processing of biometric data is in principle **prohibited**, but exceptionally allowed.

The explicit reference to the fact that in order to be qualified as processing of a special category of data the processing of biometric data must be carried out for the purpose of uniquely identifying a natural personal must be underlined. This implies that the processing of biometric data for other purposes would **not qualify as processing of sensitive data under Article 9 GDPR**. In addition, it should be recalled that biometric data are defined in the GDPR as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, **which allow or confirm the unique identification** of that natural person' (Article 4(14) GDPR), which means that only data that do allow or can confirm the unique identification of somebody might be regarded as biometric data in the first place, under the GDPR. Additionally, already to constitute personal data, information must **relate to an identified or identifiable** natural person, and 'an identifiable natural person is one who can be identified, directly or indirectly' (Article 4(1) GDPR).

All in all, this means that the processing of biometric data constitutes processing of biometric data for the purposes of EU data protection law, and more specifically to be subject to the special rules on special categories of data, if the data allows or confirms the unique identification of a natural person, who is a person identified or identifiable, and the processing takes place **for the purpose of uniquely identifying that natural person.**

A similar approach can be found in Convention 108+ - the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[59] which was 'modernised' in 2018. Convention 108+ describes in its Article 6 as processing of special categories of data the processing of 'biometric data uniquely identifying a person'.

### On automated decision-making

EU data protection law foresees a number of provisions specifically aimed at protecting individuals facing automated decision-making, which are particularly relevant when considering the regulation of AI. The most commented of all is certainly Article 22 of the GDPR, establishing that individuals should have **the right not to be subject to a decision based solely on automated processing**, including profiling, **which produces legal effects** concerning them or similarly significantly affects them, unless such decision is necessary in the context of a contract, authorised by an EU or Member State law laying down suitable safeguards, or based on the data subject's explicit consent.

When such automated decisions are based on a contract or on the consent of the data subject, 'the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the **right to obtain human intervention** on the part of the controller, **to express his or her point of view** and **to contest the decision**' (Art. 22(3) GDPR).

Particularly important for this study is that Article 22(4) GDPR establishes that the described decisions 'shall **not be based on special categories of personal data**' referred to in **Article 9(1**), unless the individual has given explicit consent in accordance with Article 9(2)(a)[60] or if processing

[59] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, 28.01.1981 as amended by Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CM(2018)2-final, 18.05.2018.

[60] Art. 9(2)(a) GDPR: '*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject*'.

is necessary for reasons of substantial public interest in accordance with Article 9(2)(g)[61] and if **suitable safeguards** are in place.[62]

The real potential of Article 22 GDPR to effectively protect individuals in light of the uptake of AI has been contested on a series of grounds. Some relate to the limitation of scope of the provision, which only applies to decisions producing a legal – or similar – effect. It is also important to stress that, as previously mentioned, the GDPR does not apply in all circumstances, and provisions under the LED are not fully equivalent.[63] In other words, it has been argued that the 'normative radius of Art 22 GDPR is more limited than its heading (...) suggests' (Martini 2020 112).

## Insights from data protection authorities

Rules on the processing of special categories of data in EU data protection law are generally perceived as **particularly unclear** and currently generate a significant number of consultations submitted to data protection authorities (AEPD 2021 4).

Data protection supervisory authorities have not only published opinions, but also taken numerous initiatives as well as adopted decisions related to the processing of biometrics. In October 2020, the Global Privacy Assembly (GPA), which brings together data protection and privacy authorities from around the globe, adopted a resolution on facial recognition technology highlighting the **significant risks to privacy** that it can raise, and stressing the importance of strong data protection rules (GPA 2020).

In 2019, the French data protection authority – the Commission Nationale de l'Informatique et des Libertés (CNIL) – adopted a report in which it puts forward a series of recommendations, notably regarding possible **experimentation** with facial recognition in public spaces (CNIL 2019). The CNIL emphasised in this sense that experiments should in any case never aim at accustoming people to intrusive surveillance technologies, or making these technologies increasingly 'acceptable' by the population (ibid. 10).

Also in 2019, the Swedish supervisory authority fined a municipality for using facial recognition technology to monitor the attendance of students in school in the context of a pilot test (EDPB 22 August 2019).[64] The Spanish data protection authority, the AEPD, has emphasised that the current status of EU and Spanish legislation do not permit the use of facial recognition by private security companies, due to the lack of legal basis allowing for such biometric data processing (AEPD 2020). The AEPD has nevertheless mentioned that it could envisage the possibility that some of uses of facial recognition by private security companies would be permitted, if duly based on a needed law and accompanied by the pertinent safeguards – for instance, for the **protection of critical infrastructures** (AEPD 2020 31).

In March 2020, the Polish Personal Data Protection Office (UODO) fined a school for the processing of biometric data of **children** to regulate access to a school canteen (EDPB 5 March 2020). The biometric data of hundreds of children had been processed despite the fact that less invasive forms of identification were possible: collecting biometric data was regarded as constituting a significantly

[61] Art. 9(2)(g) GDPR: '*Processing is necessary for reasons of substantial public interest, on the basis of Union 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 the interests of the data subject*'.

[62] It is unclear to which extent the formulation of 'biometric data for the purpose of uniquely identifying a natural person' of Article 9(1) GDPR should be taken into account when applying Article 22(4), that is, whether what is prohibited as a general rule are automated decisions based on biometric data, or automated decisions based on biometric data which are processed for the purpose of uniquely identifying a natural person.

[63] For a detailed analysis, see: González Fuster 2020 83-87.

[64] Sometimes action is taken at other levels. The Belgian DPA, for instance, reported that in 2019 it contacted a school that was planning to use palm scans to check the payment of meals; the school eventually changed its plans (APD 2019 13).

disproportionate measure. The processing of biometric data was used to identify children and verify the payment of meal fees; children's parents had been given the possibility to not consent to such processing, but in that case the children were only allowed to enter the canteen once all the other pupils had entered. These rules were deemed by the data protection authority to introduce unequal treatment of the children and an unjustified differentiation, as they clearly favoured pupils going through biometric identification. Thus, relying on consent as legal basis for such processing was inappropriate.

The President of the Polish supervisory authority emphasised in the grounds of the decision that children require special protection of personal data. Moreover, in the present case, the processed data constituted the data of special categories. The biometric system identifies characteristics which are not subject to change, as in the case of dactyloscopic data. Due to the **unique** and **permanent** character of biometric data, which means that they cannot change over time, the biometric data should be used with special due care. Because biometric data are unique, their possible leakage **may result in a high risk** to the rights and freedoms of natural persons.

Another issue to which data protection authorities have been particularly attentive is the **tracking of individuals in public spaces** by different techniques, including most notably **Wi-Fi**. In April 2021, the Dutch data protection authority fined a municipality for illegal Wi-Fi tracking of individuals in the city centre (EDBP 29 April 2021). Equally in relation to the monitoring of **public spaces**, it has been reported in some Member States that complaints regarding the absence of due information about CCTV operating in public areas are very numerous (AEPD 2020 103).

Finally, generally speaking, in the realm of data protection law it has been highlighted that 'the proliferation of machine-learning and associated AI technologies (...) have the potential to **blur the lines between 'sensitive' and other personal data**, because they allow the drawing of inferences about sensitive attributes when seemingly innocuous data are combined with other data over the course of their life' (Clifford et al. 2020 20).

### 3.2.3. Fundamental rights case law

Analysing the case law of the Court of Justice of the EU (CJEU) on biometrics, a series of points stand out. In 2013, in **Schwarz v Stadt Bochum**,[65] the CJEU considered a request for a preliminary ruling concerning the validity of Article 1(2) of the Council regulation on standards for security features and biometrics in passports and travel documents.[66] Mr Schwartz had applied for a passport in a German city, but he refused to have his fingerprints taken, hence his application for a passport had been rejected.

In this judgment, the CJEU first found that fingerprints constitute personal data because 'they objectively contain **unique information** about individuals which allows those individuals to be identified with precision' (ibid. para 27). Since the taking and storing of fingerprints by the national authorities governed by Article 1(2) of Regulation No 2252/2004 is personal data processing, it constitutes a threat to the rights to respect for private life and the protection of personal data (ibid. paras 29 and 30).

With regard to the possible justification of the interference with such rights, the CJEU noted that consent could not have been the basis of the legal processing of the fingerprints. In general, EU citizens need to own a passport in order, for example, to travel to non-member countries and such a document must contain fingerprints pursuant to Article 1(2) of Regulation No 2252/2004 (ibid. para 32). Hence, 'citizens of the Union wishing to make such journeys are not free to object to the

[65] *Schwarz v Stadt Bochum* (2013) CJEU C-291/12 ECLI:EU:C:2013:670.

[66] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004.

processing of their fingerprints', meaning that persons applying for passports cannot be deemed to have consented to that processing (idem).

Regarding the proportionality of the interference with fundamental rights, the CJEU found that the appropriateness of the used measure of storing fingerprints for attaining the aim of preventing the fraudulent use of passport is not automatically rendered futile by the fact that the used technology is not wholly reliable (ibid. para 43). Hence, a significant reduction of the likelihood of the preventing fraudulent use of passports was sufficient for the CJEU to find that the measure was appropriate (idem). Regarding the fact that fingerprints were collected in addition to a facial image, the CJUE noted that 'the combination of two operations designed to identify persons may not a priori be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation' (ibid. para 49). Hence, the fact alone of collecting both fingerprints and a facial image at the same time was not enough to give rise to greater interference with the mentioned rights (ibid. para 50).

Regarding the risk of the use of fingerprints for purposes other than those provided for by Regulation No 2252/2004, the CJEU noted the particular role of fingerprints in the field of identifying persons in general and that 'the identification techniques of comparing fingerprints taken in a particular place with those stored in a database make it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly' (ibid. para 59). However, the fact that the regulation does not provide for any other form or method of storing the fingerprints, other than in the passport itself, cannot be automatically understood as providing a legal basis for the centralised storage of data for purposes other than previewed by the regulation (ibid. para 61).

The CJEU was asked to return to the last point in a more recent case **Willems et al. v Burgemeester van Den Haag**,[67] where it ruled on the obligation to provide digital fingerprints for the purposes of passport application under the amended Regulation No 2252/2004's Article 4(3). The collected biometric data was stored not only on the storage medium integrated into the passport or identity cards, but also on a decentralised database. Eventually, local authority databases were to be combined into a centralised database. The CJEU was asked to decide on whether Member States must guarantee that biometric data collected and stored under Regulation No 2252/2004 will not be collected, processed or used for purposes other than the issuing of passports or other travel documents.

In this context, the CJEU recalled that 'the use and storage of biometric data for the purposes specified in Article 4(3) of that regulation are compatible with the requirements of Articles 7 and 8 of the Charter' (ibid. para 46). However, all other uses and storage of the data are not governed by Regulation No 2252/2004, because the regulation is without prejudice to any other use or storage of these data in accordance with national legislation of Member States, and does not provide a legal basis for setting up or maintaining databases for storage of those data in Member States (ibid. para 47). Hence, Regulation No 2252/2004 does not oblige a Member State to introduce legislative guarantees that biometric data will not be used or stored for other purposes (ibid. para 48).

Since Regulation No 2252/2004 does not apply to such other purposes, the CJEU found that the EU Charter was not applicable, hence no compatibility assessment with its Articles 7 and 8 thereof was performed (ibid. para 50). However, this is without prejudice to compatibility assessments under national law and under the ECHR (ibid. para 51).

Turning to the case law of the European Court of Human Rights (ECtHR), important points, especially related with fingerprints, should be noted. In **S. and Marper v. the United Kingdom**,[68] the ECtHR

[67] *Willems et al. v Burgemeester van Den Haag*, (2015) CJEU Joined Cases C-446/12 and C-449/12 ECLI:EU:C:2015:238.

[68] *S. and Marper v. the United Kingdom* (2008) ECtHR nos. 30562/04 and 30566/04 ECLI:CE:ECHR:2008:1204JUD003056204.

ruled on a case concerning two non-convicted individuals who wanted to have their records, including fingerprints, cellular samples and DNA profiles, removed the criminal identification database of the UK.

With regard to the nature of fingerprints, the ECtHR noted that 'all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals' (ibid. para 68). Recognizing that fingerprints do not contain as much information as cellular samples or DNA profiles, the ECtHR found that 'fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances' rendering them 'capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant' (ibid. paras 78 and 84). In this context, the ECtHR ruled that already the sole 'retention of fingerprints constitutes an interference with the right to respect for private life' (ibid. para 86).

In the context of necessity analysis, the ECtHR underlined that the state legislature must ensure that there are **specific guarantees** that the processing of such data will be effectively protected from misuse and abuse (ibid. para 103). In this context, the need for safeguards is greater if **automatic processing** is deployed, not least when such data is used **for police purposes** (idem). Hence, such collected data must be relevant and not excessive in relation to the purposes of storage, it must be preserved for identification for no longer than is required by these purposes, and it must be efficiently protected from misuse and abuse (idem).

The ECtHR ruled that it constitutes a violation of Article 8 of the ECHR to store for unlimited periods of time the mentioned types of information related to non-convicted people in a nationwide database processed by automated means for criminal-identification purposes (ibid. paras 77 and 86). The ECtHR found that such '**blanket and indiscriminate'** retention of fingerprints, cellular samples, and DNA profiles does not 'strike a fair balance between the competing public and private interests' (ibid. para 125). Such retention was thus judged a 'disproportionate interference' with the right to respect for private life and regarded as not necessary in a democratic society (ibid.). Crucially, the ECtHR drew particular concern of the risk of stigmatization which stems from the fact that persons who have not been convicted are treated in the same way as convicted persons (ibid. para 122).

Additionally with regard to fingerprints, the ECtHR in **M.K. v. France**[69] considered the case of a person whose fingerprints were retained in a database held by French authorities; the fingerprints had been taken in the context of investigations into alleged book theft, none of which ended in convictions.

The ECtHR here found that such retention interfered with the applicant's right to respect for private life. It ruled that retention of fingerprints solely for the reason of preventing future identity theft would in practice be tantamount to justifying the storage of information on the entire population, which would most definitely be excessive or irrelevant (ibid. para 40). With regard to the exercise of the rights of individuals, the ECtHR ruled that the deletion requests are not safeguards if they are theoretical and illusory rather than practical and effective (ibid. para 44). As such, the Court ruled that:

> 'while the retention of information stored in the file is limited in time, it nevertheless extends to twenty-five years. Having regard to its previous finding that the chances of deletion requests succeeding are at best hypothetical, a twenty-five-year time-limit is in practice tantamount to

[69] *M.K. v. France* (2013) ECtHR no. 19522/09 ECLI:CE:ECHR:2013:0418JUD001952209.

> indefinite retention, or at least, as the applicant contends, a standard period rather than a maximum one' (ibid. para 45).

In **Gaughran v. the United Kingdom**,[70] the ECtHR considered the indefinite retention of personal data (DNA profile, fingerprints and photograph) but this time concerning a person who had been convicted.

The ECtHR stressed that states have a narrow margin of appreciation when setting retention limits for the biometric data of convicted persons (ibid. para 84). However, it also noted that it is not only the retention period that is conclusive in assessing it the state overstepped its margin of appreciation, but also whether the state 'takes into account the seriousness of the offending and the need to retain the data, and the safeguards available to the individual' (ibid. para 88).

In practice, retention of convicts' biometric data must be modulated with reference to the seriousness of their offence and with regard to any continuing need to retain such data indefinitely (ibid. para 94). Hence, if a state chooses to put in place a regime of indefinite retention, it has to ensure certain safeguards that are present and effective, such as the possibility to apply to have data deleted (ibid. paras 88 and 94). Whether further retention is no longer necessary must be assessed 'in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and the person's current personality' (ibid. para 94).

Importantly from the perspective of biometric technologies, the ECtHR reiterated the significance of continuously improving technological capacities in the analysis of the interference with Article 8 ECHR. It noted that the domestic UK courts had made their assessment, in particular relating to the retention of the applicant's photograph, 'on the basis that it was held on a local database and could not be searched against other photographs' (ibid. para 86).

However, this conclusion has been 'superseded by **technological developments'** since, although the applicant's photograph had been held on a local database which did not have **facial recognition** or **facial mapping software**, these photographs could be uploaded on a national database which does have such software (ibid. paras 69 and 86). Hence, the state needs to analyze its compliance with Article 8 ECHR where the powers vested in the state are obscure, creating a risk of arbitrariness where the technology available is continually becoming more sophisticated (ibid. para 86).

Furthermore, although not concerning biometrics, several important judgments of ECtHR point to the limits of monitoring individuals in public spaces.

In **P.G. and J.H. v. the United Kingdom**,[71] the ECtHR considered the case of voice surveillance at a police station. In the context of the existence of an interference with private life, the ECtHR observed that Article 8 ECHR also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world (ibid. para 56). Hence, there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life' (idem.). The ECtHR noted that there is:

> 'a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through

[70] *Gaughran v. the United Kingdom* (2020) ECtHR no. 45245/15 ECLI:CE:ECHR:2020:0213JUD004524515.

[71] *P.G. and J.H. v. the United Kingdom* (2001) ECtHR no. 44787/98 ECLI:CE:ECHR:2001:0925JUD004478798.

> closed-circuit television) is of a similar character. **Private life considerations may arise**, however, **once any systematic or permanent record comes into existence** of such material from the public domain' (ibid. para 57).

Whether the way the information is gathered is intrusive or covert has no bearing on the fact that such information falls within the scope of Article 8 ECHR (idem recalling Rotaru v. Romania paras 43-44).[72]

In **Peck v. the United Kingdom**,[73] the ECtHR built on its reasoning in P.G. and J.H. v. the United Kingdom when ruling on a disclosure of CCTV footage by local authorities which resulted in publication and broadcasting of the applicant's identifiable image.

The ECtHR did not decide on whether the collection of data through the CCTV-camera monitoring of applicant's movements and the creation of a permanent record thereof in itself amounted to an interference with applicant's private life, because the applicant did not introduce a complaint in that regard. Yet, the ECtHR provided some noteworthy remarks regarding the monitoring of individuals in public places.

The ECtHR found that the monitoring of the actions of an individual in a public place by the use of photographic equipment, which does not record the visual data, does not per se give rise to an interference with the individual's private life (ibid. para 59 recalling Pierre Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium)[74]. Conversely, there might be interference with individuals' private life **if the recording of the data is of a systematic or permanent nature** (ibid. para 59).

More recently in **López Ribalda and Others v. Spain**,[75] the ECtHR ruled on covert use of video surveillance of workers, in a judgment including some general points regarding monitoring of individuals that should be taken into account.

At the onset, the ECtHR built on its previous case law, as described above, to point out that 'a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers' (ibid. para 89). Individuals' right to the protection of their image is 'one of the essential components of personal development and presupposes the right to control the use of that image' (idem.). As such, the right to control such use includes the right to refuse publication of their image, as well as the right to object to the recording, conservation and reproduction of the image by another person (idem.).

The ECtHR observed that, while the relevant international and European standards:

> 'do not seem to require the prior consent of individuals who are placed under video-surveillance or, more generally, who have their personal data collected', it is in principle necessary '**to inform** the individuals concerned, clearly and prior to implementation, of the existence and conditions of such data collection, even if only in a general manner' (ibid. para 131).

It noted that the requirement of transparency and the ensuing right to information are fundamental in nature (idem.). At the same time, the ECtHR noted that 'the provision of information to the individual being monitored and its extent constitute just one of the **criteria to be taken into account** in order **to assess the proportionality of a measure** of this kind in a given case' (idem.). If such information is not provided, other safeguards are all the more important (idem.).

[72] *Rotaru v. Romania* (2000) ECtHR no. 28341/95 ECLI:CE:ECHR:2000:0504JUD002834195.

[73] *Peck v. The United Kingdom* (2003) ECtHR no. 44647/98 ECLI:CE:ECHR:2003:0128JUD004464798.

[74] *Pierre Herbecq and the Association 'Ligue des droits de l'homme' v. Belgium* (1998) ECtHR nos. 32200/96 and 32201/96 ECLI:CE:ECHR:1998:0114DEC003220096.

[75] *López Ribalda and Others v. Spain* (2019) ECtHR nos. 1874/13 and 8567/13 ECLI:CE:ECHR:2019:1017JUD000187413.

Crucially, the ECtHR rejected a general proposition that:

> 'the slightest suspicion of misappropriation or any other wrongdoing on the part of employees might justify the installation of covert video-surveillance by the employer, the existence of reasonable suspicion that serious misconduct has been committed and the extent of the losses identified in the present case may appear to constitute weighty justification' (ibid. para 134).

It is also worth noting that there is an emerging case law on the procedures to be followed when examining, using, storing and destroying data intercepted via surveillance. In **Liberty and Others v. The United Kingdom**,[76] the ECtHR considered the interception by authorities, on the basis of a warrant, of external communications of civil liberties' organizations.

The crux of the case was the fact the legality of **a filtering process**, whereby communications between the United Kingdom (UK) and an external source, captured under a warrant, were sorted and accessed pursuant to secret selection criteria (ibid. para 13). The process included five stages, one of which was deploying an automated filtering system, operating under human control, which selected intercepted communications containing specific search terms or combinations thereof (ibid. para 43). The only protection afforded to those whose communications were intercepted was that the Secretary of State 'had to 'make such arrangements as he considers necessary for the purpose of securing that ... so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person' unless specific conditions were met (ibid. para 44). Yet, the precise nature of these 'arrangements' was not made known to the public and there was no procedure to permit an individual to confirm that the 'arrangements' had been followed (idem.).

After finding that the existence of such surveillance powers constituted an interference with the Article 8 ECHR rights of the applicants, the ECtHR found that an annual distribution of a report by a Secretary of State did not contribute towards the accessibility and clarity of the scheme, since the 'arrangements' were not revealed (ibid. paras 32 and 67). In this context, the Court recalled that 'the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is **open to public scrutiny and knowledge**' (ibid. para 67). Consequently, the ECtHR found that the domestic law at the relevant time failed to 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' (ibid. para 69). In particular, such domestic law failed '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' (idem.). Hence, the ECtHR ruled that the interference with the applicants' rights under Article 8 ECHR was not in accordance with the law (idem.).

## 3.3. Impact on fundamental rights

Much has been written on the impact on fundamental rights of the processing of biometric data, of AI in general, and of AI enabled by biometrics more particularly – especially of facial recognition.[77] As mentioned above, potentially all EU fundamental rights enshrined in the EU Charter of Fundamental Rights are potentially affected by ongoing and foreseeable developments in this area.

In this sense, despite the existence of the described architecture of fundamental rights protection in the EU, and secondary law such as data protection law, the European Commission in its Impact Assessment accompanying the proposal for a regulation on AI assessed that 'current EU law does

[76] *Liberty and Others v. The United Kingdom* (2008) ECtHR no. 58243/00 ECLI:CE:ECHR:2008:0701JUD005824300.

[77] See, for instance: Nesterova, 2020.

not effectively ensure protection for safety and **fundamental rights risks specific to AI systems**' (SWD(2021) 84 final Part 1/2 35).

Biometrics and AI potentially allow for the broad surveillance of individuals, the potential impact of which is not limited to one or more specific fundamental rights, but can affect democracy itself. This has notably been emphasised by the Committee of Ministers of the Council of Europe, observing that digital tracking and surveillance technologies can have a detrimental **chilling effect** on citizen participation in social, cultural and political life (Committee of Ministers of the Council of Europe 2013).

Biometric data were explicitly included in the list of data the processing of which deserves special protection under data protection law precisely because such processing can have particularly serious consequences for individuals and society. Biometric data being **irrevocable**, certain data breaches might imply that an individual is no longer able to effectively rely on such data, and unable to modify it.

AI systems using biometrics are increasingly used in social welfare administration, where decisions **significantly impact** individuals' lives (CAHAI(2020)23 10). The Article 29 Working Party warned in 2012 that biometric identification systems used on a large scale 'produce serious side effects'. Concretely, they noted in reference to facial recognition that 'a widespread use would **terminate anonymity in public spaces** and allow consistent tracking of individuals' (Art. 29 WP193 9).

AI systems relying on biometrics such as remote biometric identification enable the tracking of individuals at an unprecedented scale. The **pervasive tracking of individuals in public spaces** can seriously negatively impact the rights to freedom of expression, and to freedom of assembly and association. These systems can interfere with the population's daily lives and normal movements, but also alter the way in which certain individuals and groups are able to exercise **social** and **political protest**.

The risks to the rights of freedom of expression, assembly and association are particularly visible in the case of live facial recognition.[78] Using these technologies in public spaces might interfere with the way a person expresses their opinions, by compromising their anonymity (FRA 2020(a) 29). The resulting chilling effect might result in individuals changing their behaviour because they know they are being watched (idem). Similarly, the deployment of facial recognition technologies during peaceful assemblies might discourage individuals from attending them, limiting the potential of participatory democracy (idem). Depending on how live facial recognition is used, and if used by law enforcement authorities, it could interfere with the right to liberty.

The United Nations (UN) High Commissioner for Human Rights has explicitly warned of the effect of the increasing use of facial recognition on **peaceful protests.** A 2020 report noted that assemblies traditionally have allowed participants a certain level of protection against being singled out or identified, and that this 'protection was already considerably weakened by many States that routinely made audiovisual recordings of assembly participants' ((UN) High Commissioner for Human Rights 2020 para. 34).

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) has highlighted that the use of live facial recognition technologies in uncontrolled environments bares **a particular intrusiveness upon the right to privacy and the dignity of individuals**, coupled with a special risk of adverse impact on other human rights and fundamental freedoms (T-PD(2020)03rev4 5). The Consultative Committee described the notion of '**uncontrolled environment'** as covering 'places freely accessible to

[78] In this sense, for instance: Bergamini 2020 para. 26.

individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools' (idem).

A survey conducted in Brazil documented a **very high concern** (95.2%) among **trans individuals** regarding the possibility that facial recognition technologies lead to their **stigmatisation** (Silva and Varon 33). This confirms other available insights. Throughout 2020, the Ada Lovelace Institute established in the UK a Citizens' Biometrics Council to deliberate on the use of biometric technologies (Ada Lovelace Institute 2021). The deliberations notably showed that 'Council members were particularly concerned to hear about unethical research using facial recognition and other biometrics to attempt to identify people according to their sexuality or target them because of their gender' (ibid. 33).

In its LGBTIQ Equality Strategy for the period 2020-2025, the European Commission observed that 'one of the emerging challenges in the field of facial recognition AI systems is the identification of trans faces, especially during transition period', referring to the then upcoming legislative proposal on AI as an opportunity to 'address bias and unjustified discrimination inherent in high-risk AI systems, including biometric systems' (COM(2020) 698 final 8).

The use of facial recognition for law enforcement purposes has additional serious implications, among other reasons due to the accuracy limitations of the technologies and the fact that **inaccuracies disproportionately affect certain population groups**.

The risk of **discrimination** has been widely discussed in the literature in the last few years. Racial, gender-based, and intersectional forms of discrimination in biometric technologies such as facial recognition have been profusely demonstrated in research (Article 19 2021 40). Problems are however not only limited to technologies' inaccuracies across the skin tone and gender map, as they can also be connected to **cultural differences** in expressions of emotion (Article 19 2021 40).

Discrimination can be due to a variety of different factors, as well as to a combination of them. Factors include problems related to **training data**, problems related to the **design** of the algorithms, problems related to the **learning** of the system while functioning, or to an **inappropriate use**. The limited **diversity of workforce** in AI can also have a negative impact at different stages of development and deployment. The biases might be incorporated in the algorithm itself, or when individuals decide what action to take following a biometric match (FRA 2020(a) 27). Bias in AI systems is generally regarded as possibly originating also in bias in data scientists' **methods**, in the object of their investigation, in their data sources (e.g., selection bias) or in the person responsible for the analysis (Mantelero 2019 24).

The **quality** of training data is critical for effectiveness and accuracy of biometric technologies. For instance, in the specific case of facial recognition, accuracy is not only dependent on the amount of training data (the facial images processed), but also on their quality (FRA 2020(a) 27). Quality can be compromised when, for instance, the reflection of light affects the quality of facial images of fair-skinned persons, or when too little light affects the quality of dark-skinned persons (idem). Maintaining quality requires that training data is representative in that it adequately reflects different groups of people. However, the contemporary reality is that training data often over-represents white men, resulting in erroneous results for the under-represented groups of people, and to the disadvantage (idem). The issues identified expose a risk that some groups of people (e.g., women and dark-skinned individuals in general) are more often false positives, exacerbating the risk of **discrimination**.

The work by Buolamwini and Gebru (2018) evaluated the performance of automated gender classification systems to find that in the researched systems classifiers performed better on male faces than on female faces, and better on lighter faces than on darker faces, the worst performance being on darker female faces (ibid. 8). Later research has found empirical evidence of the **existence**

**of demographic differentials** in many contemporary face recognition algorithms, with false positive differentials being much larger than those related to false negatives (Grother, Ngan and Hanaoka 2019). The US National Institute of Standards and Technology (NIST) in the US performs face recognition vendor tests (FRVT) to evaluate the performance of facial recognition systems, including related to bias.

The impact of automated facial recognition is currently particularly visible in the US, where it has been more extensively used. In this context, in addition to technology performing differently depending on the type of skin of individuals, meaning that the risks of facial recognition police use, notably in terms of inaccuracy, are not equal for all (Spivak and Garvie 2020 88), it has been highlighted that certain communities are known to be **disproportionately enrolled in facial recognition databases**, and generally disproportionately targeted by surveillance (Spivak and Garvie 2020 88).

Publicised cases of wrongful arrest of black people **misidentified** by police facial recognition, as well as several studies, indicate that many facial recognition algorithms are most accurate for white men, but less accurate for other persons. The widespread use of facial recognition for law enforcement has indeed been connected to a number of wrongful arrests, in particular of black men (Anderson 2020, Hill 2020(a), Hill 2020(b)). In the US there was also controversy in light of reports of **retroactive use of facial recognition** applied to footage of participants to demonstrations connected to the Black Live Matters movement (Vincent 2020).

In the UK, the Court of Appeal ruled that South Wales Police's use of automated facial recognition was **unlawful**, in response to a case brought by a civil liberties campaigner, Ed Bridges, and Liberty.[79] The Court observed in the judgment that '[f]acial biometrics bear some similarity to fingerprints because both can be captured without the need for any form of intimate sampling and both concern a part of the body that is generally visible to the public', but it also noted the existence of a 'significant difference', as automated facial recognition technology 'enables facial biometrics to be procured without requiring the cooperation or knowledge of the subject or the use of force, and can be obtained **on a mass scale'** (para. 23).

Generally speaking, existing data protection safeguards that might in principle apply in the context of the deployment of remote biometric identification systems might in practice not be applied or effective, notably due to the **recurrent power imbalance** between the data controllers deciding to deploy the systems and the data subjects.[80]

In any situations where freedom or personal security are at stake, the impact of biometrics-enabled AI can be particularly serious. This is thus also the case in the **judicial context.** As underlined in a report for the Committee on Equality and Non-Discrimination of the Council of Europe's Parliamentary Assembly, certain flaws in a the criminal justice system can have 'far-reaching human rights consequences' (Lacroix 2020 12).

Discriminatory effects are not always merely secondary to the deployment of AI systems. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stressed already in 2019 that credible reporting suggests that the government of China, 'using a combination of facial recognition technology and surveillance cameras throughout the country', tracks **Uighurs** based on their appearance and keeps records of their comings and goings for search and review (UN Special Rapporteur 2019 5) (see also Human Rights Watch 2020).[81]

[79] UK, Court of Appeal, *R (Bridges) v. CC South Wales*, EWCA Civ 1058, 11 August 2020.

[80] Referring to such power imbalance: Penner and Chiusi 2020 25.

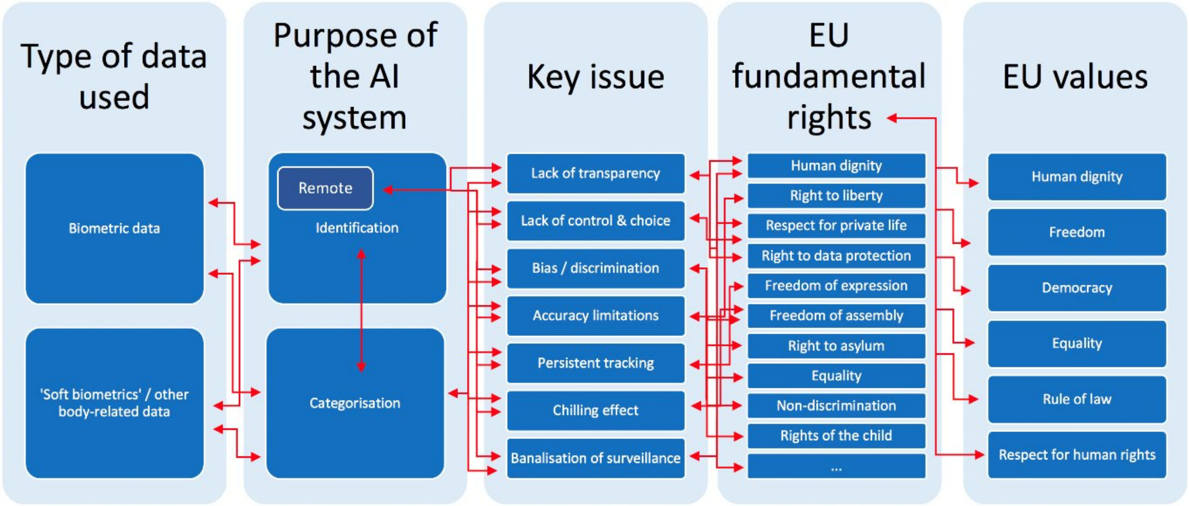
[81] Concerns have also been raised regarding the inappropriate use of facial recognition by law enforcement authorities for tracking protesters in other countries, such as, for instance, Uganda (Kafeero 2020).

A study of how **emotion recognition technologies** are spreading in China alerts about the fact that, even when identification as such is not the prime end, there are serious implications in terms of **surveillance**. Indeed, their deployment is connected to a concentration of state and industry power resulting 'in constant, intrusive, and arbitrary qualitative judgements to assess individuals' (Article 19 2021 36). In addition, it is worth noting that the very claims that emotion recognition technology can infer people's 'true' inner states has in itself significant implications for freedom of expression, as it gives way to significant **chilling effects** (Article 19 2021 37). When used in the context of interrogation, the use of emotion recognition can run counter to the right against **self-incrimination** contemplated in international human rights law, which includes the right to silence (Article 19 2021 38).

Finally, a mention needs to be made of the **rights of children**. The commented ECtHR's Marper judgment of the ECtHR (2008) emphasised the risks connected to the storage of biometric data of children. The EU Agency of Fundamental Rights has been particularly vocal about the risks associated to collecting and storing biometric data of children in the context of migration, asylum and border management control, observing that such data is often made available to law enforcement authorities for law enforcement purposes (FRA 2017 32).[82]

For a representation of some key interdependencies between the processing of biometric data – in a large sense, identification and categorisation systems, and fundamental rights, see Figure 2.

Figure 2 - Identification and categorisation, EU fundamental rights and values



## 3.4. Regulatory trends and current policy debates

The potential impact of AI on fundamental rights and ethical principles has triggered many reactions at policy level, in parallel with judicial developments and calls from the civil society. Generally speaking, at policy level the current trend is a shift from an emphasis on the need to elaborate ethical guidelines and principles towards work on **legal instruments** and **legislative proposals**. This is, however, not a systematic development, and some calls stressing the importance of ethical principles simultaneously also stress the importance of appropriate legal frameworks.[83]

[82] See also, on fundamental rights concerns regarding the biometric data of children processed by EU large-scale databases: Fondazione Giacomo Brodolini 2019 43.

[83] In this sense, for instance, the Global Privacy Assembly (GPA) in its 2020 Resolution on Facial Recognition Technology reiterated the importance of 'An ethical approach to the use of biometric data', but also of 'Legal frameworks that are fit for purpose in regulating evolving technologies such as facial recognition technology' (GPA 2020 3).

The Guidelines on Facial Recognition of the Consultative Committee of Convention 108 incorporate some references to the need of an **ethical framework** especially for the use of facial recognition technologies in certain sectors (T-PD(2020)03rev4 15). According to the Guidelines, '[t]his could take the form of independent ethics advisory boards that could be consulted before and during lengthier deployments, carry out audits and publish the results of their research to complement or endorse an entity's accountability' (idem). The Guidelines see a potential for '**committees of experts** from different fields of expertise' to discuss the most difficult cases in order **to avoid human rights abuses** and connect to this topic the role of whistle-blowers (idem).

In the literature, there has been much discussion about how to improve the regulation of AI, notably in terms of **fairness**, **transparency** and **accountability**. These notions are deeply intertwined, as transparency is instrumental not only for instance in order to allow for the exercise of data subject rights, but also to facilitate the detection of bias and discrimination, and thus support fairness.

Some researchers have in this sense advocated that in order to 'support meaningful **accountability**', automated decision-making processes 'should be designed and developed to be reviewable' (Cobbe, Lee and Singh 2021 4). In this context, **reviewability** is understood as involving:

> 'technical and organisational record-keeping and logging mechanisms that expose the contextually appropriate information needed to assess algorithmic systems, their context, and their outputs for legal compliance, whether they are functioning within expected or desired parameters, or for any other form of assessment relevant to various accountability relationships' (idem).

As possible ways to tackle bias, have also been discussed, in addition to the involvement of committees of experts from a range of fields, participatory forms of risk assessment (Mantelero 2019 25). The recommendations stemming from the Ada Lovelace Institute's UK Citizens' Biometrics Council deliberations note that 'the **representation of a diverse range of perspectives** needs to be included in not just the development of biometric technologies, but in the standards, governance and oversight relating to them', and that 'for those communities most at risk from the harms these technologies may pose, standards and oversight are not enough if they are not backed by law' (Ada Lovelace Institute 2021 38).

### 3.4.1. Overview of global discussions

Important developments have occurred in the United States (US), where civil society has notably called US President Joe Biden to act in order to stop the spread of facial recognition (Freedom House 2021). In 2020, major US companies made public announcements about stopping or pausing the selling of some of their facial recognition products for law enforcement purposes, calling for a regulation of its use (Heilweil 2020).

In the US, civil society concerns over to growing concern over the use of police facial recognition have led to legislators introducing and passing facial recognition bans, moratoria, and regulatory bills (Spivak and Garvie 2020 88). **Moratoria** might be sub-classified into time-bound moratoria, pausing facial recognition use for a set amount of time; and directive moratoria, pausing it and requiring legislative action to supersede the pause (idem).[84] The Facial Recognition and Biometric Technology Moratorium Act of 2020[85] introduced in the US Senate has as objective to prohibit

[84] Moratoria have also been called for in other parts of the world. For instance, the Australian Human Rights Commission has stated that: '*Australia's federal, state and territory governments should introduce a moratorium on the use of facial recognition and other biometric technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement*' (Australian Human Rights Commission 2021, Recommendation 20).

[85] Facial Recognition and Biometric Technology Moratorium Act of 2020, S.4084, 25.06.2020.

federal use of certain biometric technologies until Congress explicitly allows their use with certain limitations.

**Regulatory bills** seeking to place restrictions on facial recognition's use have also been introduced, for instance proposing a **court order requirement** for law enforcement to run some of all facial recognition searches (Spivak and Garvie 2020 93). **Bans** have seen the light, in particular implemented by local municipal authorities, and concentrated in towns and cities in California and Massachusetts (Spivak and Garvie 2020 89).

In March 2020, the **Washington** state legislature passed a public sector facial recognition privacy bill, placing controls on the public sector use of facial recognition technology in the State and to take effect in July 2021 (Halpert 2020). The bill[86] sets forth requirements for the use of facial recognition services by State and local government agencies, including accountability reporting,[87] annual reporting, operational testing, independent testing, training, and human review.[88] Accountability reports must notably include clear and understandable statements with *inter alia*:

> 'a description of **any potential impacts of the facial recognition service on civil rights and liberties**, including potential impacts to privacy and potential disparate impacts on marginalized communities, and the specific steps the agency will take to mitigate the potential impacts and prevent unauthorized use of the facial recognition service' (Section 3(2)(g)).

Such accountability reports must, prior to finalisation, **be public** to allow for a public review and comment period (Section 3(3)(a)). The agency aiming at using facial recognition services must additionally hold at least three **community consultation meetings** (Section 3(3)(b)), and it is obliged to take into account their input and the input from the public consultation ((Section 3(3)(c)).

The bill generally determines the obligations of users of facial recognition systems, and one of the obligations of such users is to demand from the facial recognition service provider to make available an application programming interface or other technical capability 'to enable legitimate, independent, and reasonable tests of those facial recognition services for **accuracy and unfair performance differences across distinct subpopulations**' (Section 6(1)(a)). The subpopulations which must be taken into account are those 'defined by visually detectable characteristics such as: (i) Race, skin tone, ethnicity, gender, age, or disability status; or (ii) other protected characteristics that are objectively determinable or self-identified by the individuals portrayed in the testing dataset' (idem).

The bill prohibits state and local agencies from using a facial recognition service for ongoing surveillance, unless specified conditions are met, and either a court order is obtained, or the agency reasonably determines that exigent circumstances exist and an appropriate court order is obtained as soon as reasonably practicable. The bill categorically **prohibit**s State and local agencies from applying a facial recognition service **based on certain protected characteristics**,[89] as well as creating a record describing any individual's exercise of certain constitutional rights. It also specifies disclosure and reporting requirements, in addition to creating a legislative task force on facial recognition. The task force shall include, among others, decision-makers, representatives of law

[86] Engrossed Substitute Senate Bill, SB 6280, passed by the Senate on 12 March 2020.

[87] Prior to developing, procuring, or using a facial recognition service, a state or local government agency must produce an accountability report for that service (Section 3(2)).

[88] Human review is exclusively foreseen when a facial recognition service is used to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals (Section 4).

[89] *'A state or local government agency may not apply a facial recognition service to any individual based on their religious, political, or social views or activities, participation in a particular noncriminal organization or lawful event, or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender identity, sexual orientation, or other characteristic protected by law'* (Section 11(2)).

enforcement agencies, industry representatives and academics, '[e]ight representatives from advocacy organizations that represent individuals or protected classes of **communities historically impacted by surveillance technologies**' (Section 10(1)(a)(iii)).[90]

The Washington bill is based on the idea that '[u]nconstrained use of facial recognition services by state and local government agencies poses **broad social ramifications** that should be considered and addressed', with rules 'prohibiting uses that threaten our democratic freedoms and put our civil liberties at risk' (Section 1(1)). At the same time, the bill also notes that 'state and local government agencies may use facial recognition services to locate or identify missing persons, and identify deceased persons, including missing or murdered indigenous women, (...) and other possible crime victims, for the purposes of keeping the public safe' (Section 1(2)), and thus its use should not be fully prohibited.

The bill defines 'facial recognition service' as:

> 'technology that analyzes facial features and is used by a state or local government agency for the identification, verification, or persistent tracking of individuals in still or video images' (Section 2(3)(a)).

This definition is thus **broader** than definitions of remote biometric identification axed on the processing of data for identification purposes,[91] which is the approach currently embodied in the AI regulation proposed by the European Commission. This is even more evident when taking into account the definition of '**persistent tracking'** put forward in the bill:

> ' 'Persistent tracking' means the use of a facial recognition service by a state or local government agency **to track the movements of an individual on a persistent basis without identification or verification** of that individual. Such tracking becomes persistent as soon as:
>
> (a) The facial template that permits the tracking is maintained for more than forty-eight hours after first enrolling that template; or
>
> (b) Data created by the facial recognition service is linked to any other data such that the individual who has been tracked is identified or identifiable.' (Section 2(10)).

Another salient feature of the Washington bill is that it regulates '**ongoing surveillance**' of individuals defined as 'using a facial recognition service to track the physical movements of a specified individual through one or more public places over time, whether in real time or **through application of a facial recognition service to historical records**' (Section 2(9)). This means that the definition does not cover exclusively 'real-time' or 'almost real-time' facial recognition, but applies also to data stored over time.

### 3.4.2. Council of Europe

The Council of Europe has put in place an Ad hoc Committee on Artificial Intelligence (CAHAI). In September 2019, the Committee of Ministers of the Council of Europe mandated the CAHAI to examine, on the basis of broad multi-stakeholder consultations, the feasibility and potential elements of **a legal framework** for the development, design and application of AI, based on Council of Europe standards in the field of human rights, democracy and the rule of law (CAHAI(2020)23 2).

A feasibility study published by the CAHAI in December 2020 notably asserts that biometric data can be used, beyond identification or authentication purposes, 'to profile or categorise individuals

[90] '*Including, but not limited to, African American, Latino American, Native American, Pacific Islander American, and Asian American communities, religious minorities, protest and activist groups, and other vulnerable communities*' (idem).

[91] This has a direct impact on the scope of the bill’s definition of ‘facial template’, defined as '*the machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service*' (Section 2(4)).

for various purposes and in different contexts', while noting in a footnote that '**no sound scientific evidence** exists corroborating that a person's inner emotions or mental state can be accurately "read" from a person's face or other biometric data' (CAHAI 2020 8).

On 28 January 2021, the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) published its **Guidelines on Facial Recognition** (T-PD(2020)03rev4). The Guidelines describe a set of reference measures for governments, facial recognition developers, manufacturers, service providers and entities using facial recognition technologies to apply to ensure that they do not adversely affect the **human dignity**, **human rights** and **fundamental freedoms** of any person, including the **right to protection of personal data** (ibid. 3).

The Guidelines notably state that the use of live facial recognition technologies in 'uncontrolled environments', 'should be **subject to a democratic debate** on its use and the possibility of a moratorium pending complete analysis' (ibid. 5). The Committee declares that 'biometric data processing by facial recognition technologies for identification purposes (...) should be **restricted, in general, to law enforcement purposes**' (ibid. 6). It also considers that '**[p]rivate entities shall not deploy facial recognition technologies in uncontrolled environments** such as shopping malls, especially to identify persons of interest, for marketing purposes or for private security purposes' (ibid. 7).

The Guidelines on Facial Recognition of the Consultative Committee of Convention 108 support the use by legislators and decision-makers of different mechanisms to ensure the **accountability** of the developers, manufacturers, service providers or entities using these technologies, of which an essential element would be the 'setting up of independent and qualified **certification mechanism** [sic] for facial recognition and data protection to demonstrate full compliance of the processing operations carried out' (ibid. 8).

### 3.4.3. EU recent developments

In January 2021, the European Commission registered a **European Citizens' Initiative** entitled 'Civil society initiative for a ban on biometric mass surveillance practices', calling on 'the European Commission to strictly regulate the use of biometric technologies in order to avoid undue interference with fundamental rights', and, 'in particular, to prohibit, in law and in practice, indiscriminate or arbitrarily-targeted uses of biometrics which can lead to unlawful mass surveillance'.[92] The initiative is connected to an EU-wide campaign called 'Reclaim Your Face' with which a group of NGOs demand the EU to ban facial recognition in public spaces.

In May 2020 the European Digital Rights initiative (EDRi) had already issued a public call 'to permanently stop all biometric processing in public and publicly-accessible spaces, wherever it has the effect or potential effect to establish mass surveillance' (EDRi 2020(a)). In June 2021, an international group of civil society representatives and academics signed a letter calling 'for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance' (Access Now et al. 2021). The NGO Access Now, in conjunction with the 'Reclaim Your Face' campaign and All Out, also launched a campaign calling for a ban of the **automated recognition of the gender and sexual orientation**, arguing that such technologies are not only scientifically flawed, but also put lives at risk.[93]

In February 2020, the European Commission had published its White Paper on AI, 'A European approach to excellence and trust' (COM(2020) 65 final), which was followed by a public consultation.

[92] More information: https://europa.eu/citizens-initiative/initiatives/details/2021/000001_en.

[93] More information: https://act.accessnow.org/page/79916/action/1.

The ensuing public consultation offered some insights on public **concerns related to remote biometric identification**. As reported by the European Commission, 28% of respondents expressed their support for **a general ban of remote biometric identification in public spaces**; 29% asked for **specific EU guidelines or legislation** before such systems may be used in publicly accessible spaces; 20% wished to see **more requirements** or conditions for remote biometric identification, and only 6% argued that the current situation is adequate (EC DG CONECT 2020 11).

In 2019 it had already started to become clear that the European Commission was committed to proposing legislation for an EU approach on the implications of AI (Von der Leyen 2019 13). By then the Expert Group on Liability and New Technologies called for new rules on liability (Expert Group on Liability and New Technologies - New Technologies Formation 2019), while the High-level expert group on AI (AI HLEG) worked on guidelines for AI systems to be 'trustworthy'. The AI HLEG, set up in 2018, eventually published its influential Ethics Guidelines for Trustworthy AI (2019), among other documents.[94]

It must be noted that the moves towards a regulation of AI in the EU have taken place in parallel to decisions aiming at **supporting the development of AI**, notably through investment and support of research. Research co-funded by the AI has included controversial research such as the iBorderCtrl project, encompassing automated deception detection.[95] Another example of project known to cause some concerns (eu-LISA 2020 18) is the Automatic Sentiment Analysis in the Wild (SEWA) project,[96] connected to the development of a predictive framework for '**continuous-time prediction of dimensional affect or behavior** (e.g., valence/arousal, interest, conflict)'.[97]

### 3.4.4. Towards a regulation on AI

The European Commission published its proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI (COM(2021) 206 final) on 21 April 2021.[98] It is based on Articles 16 and 114 of the TFEU, on personal data protection and the internal market, respectively.[99] Article 16 of the TFEU is the relevant legal basis 'in as far' are concerned rules on restrictions of the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement (COM(2021) 206 final 6) and only to such extent (Recital (2) of the proposed AIA).

It has been nevertheless described as putting forward a certification system primarily inspired in product safety regimes (Matus and Veale 2021).

The proposed AI regulation **prohibits the use of some AI systems** (listed in the proposed Article 5), and qualifies other as '**high-risk**', detailing the rules applicable to such 'high-risk' systems. Some high-risk systems are to be classified as such because of their connection with safety issues (under

[94] Can also be mentioned its Assessment List for Trustworthy AI (ALTAI), which does not explicitly mention biometrics but includes a couple of references to the processing of special categories of data, to be taken into account under the ‘privacy and data governance’ requirement (AI HLEG 2020 12-13).

[95] More information: https://www.iborderctrl.eu/. For an analysis, see notably: Penner 2019 36-38; Sánchez-Monedero and Dencik 2020.

[96] More information: https://www.sewaproject.eu/.

[97] More information: https://ibug.doc.ic.ac.uk/resources/continuous-time-prediction-behavior-affect/.

[98] This constitutes a first step in a broader movement to be followed by a proposal on liability issues by the end of 2021 or beginning of 2022 (SWD(2021) 84 final. Part 1/2 9).

[99] According to the Impact Assessment accompanying the proposal for the Regulation on AI, Art. 16 TFEU had to be used as a legal basis because '*this Regulation contains certain specific rules, unrelated to the functioning of the internal market, restricting the use of AI systems for ‘real-time’ remote biometric identification by the law enforcement authorities of the Member States, which necessarily limits the processing of biometric data by those authorities*' (SWD(2021) 84 final Part 1/2 31).

the proposed Article 6(a)). Others shall be regarded as high-risk because they are listed in the proposed Annex III to the regulation.

## High risk systems

Annex III lists the areas that allow to determine which systems are to be regarded as 'high risk' for the purposes of the proposed AI regulation, and under each area one or more types of AI systems qualifying as high risk are mentioned. The first identified area is **biometric identification and categorisation of natural persons.** Under this heading (heading 1), only a concrete group of AI systems are mentioned, however: 'AI systems intended to be used for the '**real-time**' and '**post' remote biometric identification** of natural persons'. There is, however, **no reference to biometric categorisation** being recognised as 'high risk', despite the reference on the heading's title.

According to the Impact Assessment accompanying the proposal for the regulation on AI, allowing certain uses of remote biometric identification while considering them high risk 'because they pose significant risks to fundamental rights and freedoms of individuals or whole groups thereof' would be '**overall consistent** with the EP [European Parliament] position in its resolution on the ethics of AI that the use and gathering of biometric data by private entities for remote identification purposes in public areas, such as biometric or facial recognition, would not be allowed' (SWD(2021) 84 final Part 1/2 45).

Other areas mentioned as involving the qualification of an AI system as high risk are management and operation of **critical infrastructure**, **educational** and **vocational training**; **employment**, workers management and access to self-employment; access to and enjoyment of **essential private services** and **public services** and **benefits**; **law enforcement**; **migration**, **asylum** and **border control management**; **administration of justice** and **democratic processes**.

Potentially, in any of these areas it is possible to imagine there might exist AI systems that involve the processing of **biometric data**, for instance consisting in facial recognition or so-called emotion recognition. There are in addition some references in some sub-headings to AI systems that appear to be directly related to either categorisation or emotion recognition.

Under heading 4, '**Employment**, workers management and access to self-employment', there is a reference to:

- '(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, **evaluating candidates** in the course of interviews or tests.'
- '(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.'

Under heading 5, 'Access to and enjoyment of **essential private services** and **public services and benefits**', there is a reference to:

> '(a) AI systems intended to be used by public authorities or on behalf of public authorities **to evaluate the eligibility of natural persons for public assistance benefits and services**, as well as to grant, reduce, revoke, or reclaim such benefits and services.'

Under heading 6, on **'Law enforcement'**, are mentioned:

> '(b) AI systems intended to be used by law enforcement authorities as **polygraphs and similar tools** or **to detect the emotional state** of a natural person'. This could relate to 'emotion recognition.'

> '(e) AI systems intended to be used by law enforcement authorities for **predicting the occurrence or reoccurrence of an actual or potential criminal offence** based on profiling of

> natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or **assessing personality traits and characteristics** or past criminal behaviour of natural persons or groups.'
>
> '(f) AI systems intended to be used by law enforcement authorities **for profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences.'
>
> '(g) AI systems intended to be used for **crime analytics** regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.'

Under heading 7, on '**Migration**, **asylum** and **border control** management', stand out:

> '(a) AI systems intended to be used by competent public authorities as **polygraphs and similar tools** or to **detect the emotional state** of a natural person;'
>
> 'd) AI systems **intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility** of the natural persons applying for a status.'

Under heading 8, on 'Administration of **justice** and **democratic processes'**, are mentioned:

> '(a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.'

The proposal foresees that Annex III might be amended by the European Commission via delegated acts (proposed Article 7(1) AIA). The European Commission would be able to **add new categories of systems to be considered 'high-risk'** as long as they are intended to be used in one of the areas already listed in Annex III, and if:

> 'the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, **equivalent to or greater** than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III' (proposed Article 7(1)(b)).

In practice, this means that, in relation to fundamental rights,[100] in the future might only be added to the list of high-risk systems those that the European Commission considers as having an **adverse impact on fundamental rights equivalent to or greater** than those already listed. This immediately triggers the question on how such an adverse impact could be **measured** and **compared**.

In this sense, the proposal clarifies that when making such an assessment, the European Commission shall take into account **a series of criteria**, listed in the proposed Article 7(2):

> '(a) the intended purpose of the AI system;
>
> (b) the extent to which an AI system has been used or is likely to be used;
>
> (c) the extent to which the use of an AI system has already caused harm to the health and safety or **adverse impact on the fundamental rights** or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;
>
> (d) the potential extent of such harm or such adverse impact, in particular in terms of its **intensity** and its ability to **affect a plurality of persons**;

[100] In light of the focus of this study, references to safety harms are not directly discussed here.

> (e) the extent to which potentially harmed or adversely impacted persons are **dependent** on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;
>
> (f) the extent to which potentially harmed or adversely impacted persons are in a **vulnerable position** in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;
>
> (g) the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;
>
> (h) the extent to which existing Union legislation provides for:
>
> (i) effective measures of **redress** in relation to the risks posed by an AI system, with the exclusion of claims for damages;
>
> (ii) effective **measures to prevent or substantially minimise those risks**.'

It is not completely clear **what such 'taking into account' of all these criteria is expected to imply** in practice. For instance, in relation to the criterion related to 'the extent to which an AI system has been used' (proposed Article 7(2)(b) AIA), it could be interpreted that if a system has already been used to some extent, it was because it did not have an adverse impact, but this might also not be the case.

The proposed Article 7(2)(c) AIA refers to the need to take into account already materialised adverse impact on fundamental rights, as well as signification concerns in relation to such materialisation, but only to the extent these have been 'demonstrated by reports or documented allegations submitted to national competent authorities', without specifying how or by whom, or at which moment the European Commission would be legally obliged to take into account such submitted evidence.

AI systems qualifying as **high risk systems** shall in any case, in line with the proposal, **comply with the requirements listed in its Chapter 2**, which concern: a risk management system (proposed Article 9 AIA), rules on data training, validation and testing (proposed Article 10 AIA), technical documentation (proposed Article 11 AIA), record keeping (proposed Article 12 AIA), transparency and provision of information to users (proposed Article 13 AIA), human oversight (proposed Article 14 AIA), and on accuracy, robustness and cybersecurity (proposed Article 15 AIA).

The required **risk management system** is described in the proposed Article 9 AIA, which notes that it 'shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating', necessarily include testing prior to the placing on the market or the putting into service, and notably comprise four steps:

> '(a) identification and analysis of the **known and foreseeable risks** associated with each high-risk AI system;
>
> (b) estimation and evaluation of the **risks that may emerge** when the high-risk AI system is used **in accordance with its intended purpose** and **under conditions of reasonably foreseeable misuse**;
>
> (c) evaluation of **other possibly arising risks** based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;
>
> (d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs' (proposed Article 9(2) AIA).

The proposed Article 10 AIA details the data-related requirements applicable to high-risk systems which make use of techniques involving the training of models with data, under the heading **data**

**and data governance**. These are particularly relevant from a fundamental rights perspective insofar as they directly concern issues related to risk of bias. In line with the proposed text, and specifically the proposed Article 10 AIA, for the mentioned systems the training, validation and testing data sets shall:

- 'be subject to appropriate data governance and management practices', inter alia concerning '**examination in view of possible biases'**, as well as 'the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed';
- 'be relevant, representative, free of errors and complete', and 'have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used'; and
- 'take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high- risk AI system is intended to be used'.

The same provision foresees that exceptionally and to the extent that 'it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems', the providers of such systems may process special categories of personal data, subject to appropriate safeguards (proposed Article 10(5)(g) AIA). There are no specific safeguards detailed in this context.

Chapter 3 of the proposed regulation describes among others the **obligations of providers** of high-risk AI systems. Providers are responsible for ensuring that their high-risk AI systems are compliant with the requirements set out in Chapter 2, but have also other obligations, such as **affixing a CE marking** to their high-risk AI systems to indicate the conformity with the regulation (proposed Article 16 AIA). They must also **put a quality management system** in place (proposed Article 17 AIA), draw up the **technical documentation** (proposed Article 18 AIA), ensure that their systems undergo the relevant **conformity assessment procedure** (proposed Article 19 AIA),[101] keep the automatically generated **logs** (proposed Article 20 AIA), **take appropriate corrective measures** when they consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with the regulation (proposed Article 21 AIA), comply with a duty of information if the system presents **a risk within the meaning of the proposed Article 65(1)** of the proposed AIA (proposed Article 22 AIA), and, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity (proposed Article 23 AIA).

The **obligations of users**[102] of high-risk systems are described in the proposed Article 29 AIA, and they include using the systems in accordance with the accompanying instructions, ensuring that input data is relevant in view of the intended purpose, and monitoring the operation of the system on the basis of the instructions of use. When the users have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting **a risk within the meaning of the proposed Article 65(1),** or if they when they have identified any serious incident or any malfunctioning within the meaning of the proposed Article 62, they shall inform the provider or distributor and suspend the use of the system.

[101] Special rules regarding this conformity assessment procedure apply to '*AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons*' (cf. proposed Art. 43(1) AIA).

[102] In the proposed AIA, 'users' are defined as '*any natural or legal person, public authority, agency or other body using an AI system under its territory, except where the AI system is used in the course of a personal non-professional activity*' (proposed Art. 3(4) AIA).

According to the Impact Assessment accompanying the proposal for the regulation on AI, it is possible to impose further obligations on users 'because users are already bound by the **fundamental rights legislation in place**' (SWD(2021) 84 final Part 1/2 57).

Title VIII of the proposed regulation on AI describes measures for post-market monitoring, information sharing and market surveillance. Particularly relevant is the proposed Article 62, on the '**reporting of serious incidents and of malfunctioning'**, which establishes that providers of high-risk AI systems placed on the EU market 'shall report any serious incident or any malfunctioning of those systems **which constitutes a breach of obligations under Union law intended to protect fundamental rights** to the market surveillance authorities of the Member States where that incident or breach occurred'. The notified market surveillance authority shall inform the competent national public authorities or bodies.

The proposed Article 65 describes the procedure in place for **AI systems regarded as presenting a risk** at national level insofar as risk to the health or safety or to the protection of fundamental rights of persons are concerned, if the risk, as established by Regulation (EU) 2019/1020, is of 'a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned'.[103] Where the market surveillance authority of a Member State has sufficient reasons to consider that an AI system presents such a risk, 'they shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation'; if risks to the protection of fundamental rights are present, the market surveillance authority shall also inform the relevant national public authorities or bodies. A special procedure is set up for the cases in which a market surveillance authority would consider that non-compliance is not restricted to its national territory, involving informing the European Commission and the other Member States (proposed Article 65(3), and Article 66 AIA).

The evaluation carried out by the national market surveillance might result in determining that although the AI system is in compliance with the regulation, '*it **presents a risk** to the health or safety of persons**, to the compliance with obligations under Union or national law intended to*** **protect fundamental rights** or to other aspects of public interest protection' (proposed Article 67(1) AIA). In such a case, the market authority it shall require the relevant operator 'to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk' (idem). The European Commission and other Member States shall be informed about these corrective measures, with the former being able to adopt a final decision on whether they are appropriate measures, according to the proposed draft (proposed Article 67(5) AIA).

The existence of these measures is important, as experts have stressed that it is very difficult for developers and providers of AI systems to fully ascertain 'the real-world impacts of any given AI application prospectively', noting it 'is hard enough to predict what human rights impacts a relatively anodyne product will have when it is released into the marketplace, hence the challenge of assessing the human rights impacts of AI systems before they are deployed is all the more considerable' (Raso et al. 54).[104]

[103] See Art. 3(19) of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011, OJ L 169, 25.6.2019, p. 1–44.

[104] The authors evoke in this sense the controversy around reports that the US government used facial recognition technology supplied by Microsoft in implementing a policy of separating the children of unlawful migrants from their parents, to which the company reacted expressing dismay (Shu 2019).

## Real-time remote biometric identification for law enforcement in public spaces

The AI regulation proposed by the European Commission foresees, as a general principle, 'the **prohibition of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement'** (proposed Article 1(d) AIA).[105] Nevertheless, such real-time remote biometric identification systems **can be used** 'as far as such use is strictly necessary for one of the following objectives:

> '(i) the targeted search for specific potential victims of crime, including missing children;
>
> (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
>
> (iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State' (proposed Article 1(d)(i-iii) AIA).

To understand the scope of the proposed rules on real-time remote biometric identification systems, a series of definitions in the proposal are pertinent, in addition to the definition of remote biometric identification system already commented. First, **'real-time'** remote biometric identification systems are defined as meaning 'a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay', which 'comprises not only instant identification, but also limited short delays in order to avoid circumvention' (proposed Article 3(37) AIA). Real-time remote biometric identification systems are opposed to 'post' remote biometric identification systems, which are the systems other than real-time (idem).

Second, a '**publicly accessible space'** is defined as 'any physical place accessible to the public, regardless of whether certain conditions for access may apply' (proposed Article 3(39) AIA). Third, '**law enforcement'** is defined in the proposal as 'activities carried out by law enforcement authorities 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' (proposed Article 1(40) AIA).

All these elements are important, as what the proposed regulation prohibits in principle – but allows under certain conditions - are **real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement**. In contrast, all other AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons, for the purposes of law enforcement or not, are regulated as high-risk AI systems (Annex III, point 1(a)).

The foreseen conditions allowing for the use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement include the mentioned requirement of **strict necessity** for one of the specific mentioned objectives, but also **additional requirements**.

[105] This prohibition notably derives from the fact that other options are described in the Impact Assessment accompanying the proposal for the Regulation on AI as insufficient. In this sense, the document notes that '*not to impose any further restrictions on the use of remote biometric identification in publicly accessible places and apply only the requirements for Trustworthy AI*' was a policy choice that was '*discarded as it would not effectively address the high risks to fundamental rights posed by these systems and the current potential for their arbitrary abuse witho without an effective oversight mechanism and limitations on the permitted use*' (SWD(2021) 84 final Part 1/2 46).

The proposal states that their use 'shall take into account the following elements:

> (a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;
>
> (b) the **consequences of the use of the system for the rights and freedoms of all** persons concerned, in particular the seriousness, probability and scale of those consequences' (COM(2021) 206 final 44).

The text does not specify **what is expected exactly from this 'taking into account' of the mentioned elements.** They are potentially to be taken into account when deciding of the strict necessity of the use of the mentioned systems. They represent what could be described as an invitation to **balance**, on the one hand, the risks in terms of harm connected to the possible non-use of the system, and, on the other, the risks for fundamental rights and freedoms connected to the possible use of the system.

The use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement must in any case 'comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the **temporal**, **geographic** and **personal limitations'** (proposed Article 5(2) AIA). This requirement refers to the need for accompanying safeguards but also to the need to limit the use of these systems to what is strictly necessary, notably by preventing unlimited and indiscriminate uses of real-time remote biometric identification in public spaces for law enforcement purposes.

The proposed Article 5(3) AIA puts forward that each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces 'shall be **subject to a prior authorisation granted by a judicial authority** or **by an independent administrative authority** of the Member State in which the use is to take place', issued upon a reasoned request and in accordance with rules of national law as referred to in the proposed Article 5(4) AIA.

Despite such general requirement of prior judicial authorisation, however, 'in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use' (proposed Article 5(3) AIA). The proposal does not specify what happens if the use already took place, and judicial authorisation is eventually denied.

The proposed Article 5(4) AIA states that it is up to Member States to decide to provide – or not - for the possibility **to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement**, always within the limits and under the conditions specified above. The text clarifies that when doing so Member State shall lay down in their national law 'the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to' the mentioned judicial authorisations, and that the national rules shall also specify in respect of which of the objectives listed, including in respect of which criminal offences, the competent authorities may be authorised to use those systems for the purpose of law enforcement (proposed Article 5(4) AIA).

Regarding 'post' remote biometric identification, which would fall in principle under 'high-risk' activity (proposed Article 6 (2) AIA), a requirement that any identification resulting from the system must be verified and confirmed by two natural persons (proposed Article 14) before any decision is taken would apply (Kind 2021).

According to the Impact Assessment accompanying the proposal for the regulation on AI, it was notably some Member States including France, Finland, the Czech Republic and Denmark that submitted that the use of remote biometric identification systems in public spaces **might be justified** in certain cases, for important public security reasons under strict legal conditions and safeguards, in response to the European Commission's consultation on its White Paper on AI (SWD(2021) 84 final Part 1/2 18).

## Transparency obligations and their limitations

The proposed AI regulation foresees special **transparency obligations** for providers of certain AI systems. In this sense, providers shall ensure 'that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use' (proposed Article 52(1) AIA). Thus, such transparency obligations apply to **providers of any AI systems intended to interact with natural persons**. Exceptionally, these obligations 'shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence' (idem).

In addition, the proposed regulation establishes that that **the users of emotion recognition systems** and **biometric categorisation systems** 'shall inform of the operation of the system the natural persons exposed thereto' (proposed Article 52(2) AIA).[106] Thus, these transparency obligations apply to users (as opposed to providers), but only to users of emotion recognition systems and of biometric categorisation systems. These obligations do not apply to 'AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences' (idem).

It has been noted that police use of **biometric categorisation for purposes other than identification** does not even appear to be classified as a high-risk use of biometrics, as biometric identification and categorisation systems only fall into the high-risk category when they are used for 'biometric identification' (Kind 2021).

## Exclusion of AI systems in EU large scale databases

The proposed regulation on AI is generally to apply, according to the proposal of the European Commission, to the high-risk AI systems that have been placed on the market or put into service before the date of application of this regulation 'only if, from that date, those systems are subject to significant changes in their design or intended purpose' (proposed Article 83(2) AIA).

Nevertheless, the proposal states that **the regulation shall not apply at all** – that is, none of its provisions would apply - to the AI systems which are part of the large-scale IT systems established by the legal acts listed in its Annex IX that have been placed on the market or put into service within the first year of application of the regulation (proposed Article 83(1) AIA). The legal acts listed in Annex IX refer to the Schengen Information System (SIS), the Visa Information System (VIS), Eurodac, the Entry/Exit System, the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System on third-country nationals and stateless persons (ECRIS-TCN), and their Interoperability.

**Only exceptionally**, if the replacement or amendment of the legal acts establishing these large-scale IT systems leads to a significant change in the design or intended purpose of the AI system or AI systems concerned, the regulation would apply to such AI systems. Nevertheless, the proposal states that the regulation's requirements 'shall **be taken into account**, **where applicable**, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts' (idem).

All the mentioned IT systems are managed or to be **managed by eu-LISA**, an agency that has openly endorsed a great interest in AI. A 2020 report of the Agency, for instance, notably suggested that AI could be used introduced in ETIAS **to assist the humans who have to review manually decisions**

[106] There is also a provision for users of ‘deep fakes’ (proposed Article 52(3) AIA).

**labelled as such by the system,** claiming that such 'system could support case officers responsible for evaluating applications with additional risk assessment based on the data stored in the relevant systems and the historical data on the individual submitting the application' (eu-LISA 2020 30). The idea could potentially fundamentally undermine the safeguards against automated decision-making foreseen for ETIAS, as precisely the '**human in the loop'** is supposed to bring in a manual consideration of the decision, not an additional automated decision.

## On impact assessments

The need for impact assessments is often put forward when discussing the regulation of AI, also in relation to biometrics. In the proposed regulation on AI can be identified several instances in which it might be appropriate to integrate insights from some type of impact assessments. It is the case, for instance, of the obligation imposed on the European Commission to take into account the adverse impact on the fundamental rights of AI systems to be potentially added to the list of high-risk systems.

Some have suggested that all agencies wishing to deploy facial recognition should be obliged to carry out a formal **algorithmic impact assessment**, which would be '[m]odelled after impact-assessment frameworks for human rights, environmental protection and data protection', and '**guarantee public input**' (Crawford 2019).[107] The EU Agency for Fundamental Rights put forward its own list of selected elements that in its view could be incorporated into fundamental rights impact assessments carried out before using any AI-driven systems (FRA 2020(c) 96 and ff.).

The Guidelines on Facial Recognition of the Consultative Committee of Convention 108 stress that '[e]ntities using facial recognition technologies have to **carry out impact assessments** before the processing as the use of these technologies involves biometric data processing and presents high risks to the fundamental rights of data subjects' (T-PD(2020)03rev4 14). The Consultative Committee nevertheless refers to such impact assessments as **data protection impact assessments**, which appears to imply they are not as such a specific type of impact assessment. What is worthwhile noting is that the Guidelines state that '[a]fter completion of this assessment, entities should publish it to receive views from the public on the potential deployment of facial recognition technologies' (idem). This can be regarded as a positive step for integrating the views of the public, although it could be questioned whether it would be preferable to integrate such views not after the completion of the impact assessment, but rather while carrying it out.

The impact assessment accompanying the proposal for a regulation on AI explicitly mentions that it would be possible to require insofar as for high-risk AI systems with fundamental rights implications are concerned '**fundamental rights impact assessments** / **algorithmic impact assessments** as implemented in Canada and the U.S. and recommended by some stakeholders, the Council of Europe or the Europe and the Fundamental Rights Agency' (SWD(2021) 84 final Part 1/2 58-59). Nevertheless, the document points out that this possibility was this was:

> '**discarded**, because users of high-risk AI systems would normally be obliged to do a **Data Protection Impact Assessment (DPIA)** that already aims to protect a range of fundamental rights of natural persons and which could be interpreted broadly, so new regulatory obligation was considered unnecessary' (ibid. 59).

Indeed, it is possible that a certain assessment of AI systems involving biometrics might have to occur before their use in the context of **data protection impact assessments** (**DPIAs**) – that is, an assessment of impact as regulated by EU data protection law.[108] The GDPR foresees that '[w]here a

[107] Also concluding that *'[p]olicymakers should ensure that biometric programmes undergo thorough and transparent civil rights assessment prior to implementation'*: EC Directorate-General for Research and Innovation 2020 146.

[108] Data protection impact assessments are also currently required outside of the UE. In this context, the ICO has provided detailed guidance on 'Expectations on data protection impact assessments for live facial recognition in public places',

type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an **assessment of the impact** of the envisaged processing operations on the protection of personal data'.[109] A DPIA shall 'in particular', as detailed in Article 35(3) GDPR, be required in the case of:

> '(a) a **systematic and extensive evaluation of personal aspects relating to natural persons** which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) **processing on a large scale of special categories of data** referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
>
> (c) a **systematic monitoring of a publicly accessible area on a large scale**.'

These three requirements are potentially pertinent in relation to AI systems involving biometrics, in particular those deployed in public spaces. The requirement of Article 35(3)(a) GDPR will apply if the system involves 'a systematic and extensive evaluation of personal aspects (...) based on automated processing', as long as such system produces legal effects or similarly affects individuals; Article 35(3)(b) GDPR will apply if the processing of biometric data takes place 'on a large scale'; and Article 35(3)(c) GDPR concerns the large scale and systematic monitoring of publicly accessible areas.

Under Article 35(4) GDPR, national supervisory authorities shall establish lists of the kind of processing operations that are in all cases subject to the requirement of a DPIA, and they must communicate such lists to the European Data Protection Board (EDPB).[110]

An important source of knowledge on the relation between DPIAs and biometrics-driven AI are the opinions of the EDPB on the draft lists submitted to it by national supervisory authorities regarding the processing operations which are to be subject to the requirement of a DPIA under Article 35(4) GDPR. In compliance with Article 64(1) GDPR, the EDPB must issue an opinion where a supervisory authority (SA) intends to adopt such a list of processing operations, in view of creating a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the EU, despite the fact that the GDPR does not impose a single, EU-wide list.

which can be read as partially overlaping with some requirements foreseen under the proposed Regulation on AI (ICO 56).

[109] Data protection impact assessments are also foreseen under the LED, which notes that *'[w]here a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data'*, and that the assessment *'shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned'* (Art. 27 LED). See also Art. 39 of the EU DP Regulation.

[110] Art. 35(4) GDPR states: '*The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.*'

The analysis of such opinions allows to identify the following points:

- According to the EDPB – and despite prior pointers in a different sense,[111] the processing of biometric data is **not necessarily likely to represent a high risk** per se.[112] Thus, the processing of biometric data for the purpose of uniquely identifying a natural person requires a DPIA to be carried out only when it is done in conjunction with at least one other criterion, without prejudice to Art. 35(3) GDPR (Gellert 2018 503). It is however appropriate for supervisory authorities to state that when such processing takes place 'in conjunction with one other criterion', a DPIA must be carried out (EDPB, Opinion 26/2018 6).

- Equally, 'processing activities that consist of or include regular and systematic monitoring of publicly accessible areas are **not necessarily likely to represent a high risk**', although, in conjunction with at least one other criterion, such processing is likely to present a high risk and requires a DPIA to be carried out (EDPB, Opinion 26/2018 6). Such one other qualifying criterion should not be however that the data are stored (idem).

- In a similar vein, the EDPB opposed the view that personal data processing 'using **new or innovative technology'** should immediately trigger the need to carry out a DPIA, noting that this should only be the case when such processing is done in conjunction of at least one other criterion (EDPB, Opinion 21/2018 8).

[111] In 2017, the Art. 29 Working Party had stated that 'the processing of any type of biometric data (…) could (…) be considered as relevant for the development of a list pursuant to article 35(4)' (Art. 29 WP, WP 248 rev.01 12).

[112] See, in this sense, for instance: EDPB, Opinions 9/2018 and 26/2018.

# 4. Policy options

In light of the analysis carried out and the described findings, the following policy options are put forward. They do not exclude, but complement each other.

## Policy option 1. Better delimiting the regulation of biometrics

There exists no general definition of biometrics or biometric data in EU law. The proposal for a regulation on AI published by the European Commission reproduces the **definition of biometric data** emanating from EU data protection law.

This definition of biometric data supports a rather **narrow approach to biometric data**, qualifying as such only the personal data that allow or confirm the **unique identification** of a person through a specific technical processing. The definition is also not particularly clear (Jasserand-Breeman 2019 163), as there are for instance **uncertainties** as to what such specific technical processing means, or how the data's ability to allow or confirm the unique identification of a person differs – if it does – from the requirement of processing such data 'for the purpose of uniquely identifying a natural person', which accompanies the reference to biometric data in the provisions about the processing of special categories of data.

The rather narrow nature of EU data protection law's view contrasts with the broader understanding of biometrics encountered in much of the literature and in some policy documents. Generally speaking, there is a concern with **AI systems that rely on the processing of data related to the body**, data that might not necessarily always fall under the current definition of biometric data.

As a consequence, and to the extent that the current definition of biometric data in EU data protection law would be merely reproduced in other, upcoming legal instruments, certain practices, albeit presenting serious risks for fundamental rights, might not be adequately regulated – for instance if the proposed AI regulation is adopted with the current definitions of biometric categorisation and emotion recognition, the scope of which is conditioned to the processing of biometric data, and the meaning of which is thus **indirectly circumscribed by the described narrow and not fully clear definition of biometric data**.

The **ambiguities surrounding the very notion of biometric data** are perceptible in the call of the EDPB and the EDPS, in their Joint Opinion on the proposed regulation of AI, to ban certain uses of AI 'for **an automated recognition of human features** in publicly accessible spaces' (Joint Opinion 5/2021 11) The EDPB and the EDPS call indeed 'for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals' (ibid.), a formulation in which transpire numerous terminological uncertainties. The sentence for instance appears to imply that 'biometric' and 'behavioural signals' would be something different, despite the fact that EU data protection law defines biometric data as encompassing data about the behavioural characteristics of natural persons. Also, the call refers to generally banning the recognition of **human features**, but still only provides examples that could be regarded as clearly potentially falling under biometric data.

Using in the future AI regulation the same definition of biometric data as in existing EU data protection law instruments has certainly the advantage of potentially facilitating **consistency**. If the definition in the European Commission's proposal is not revised, at least further clarity should be urgently provided, for instance through unambiguous guidance from the EDPB on how to interpret the definition and how to apply it to the most controversial and recurrent AI scenarios. In this context, in July 2021 the EDPB published a final version of its *Guidelines on virtual voice assistants*, in which is stated that '**voice data is inherently biometric personal data**' (Guidelines 02/2021 13). It is very unclear what 'inherently biometric personal data' mean, and whether voice is the only type of such data, or which biometric data would be biometric data but not 'inherently biometric personal data'.

In addition, special care has to be given to the implications of referring to the notion of biometric data in other legal definitions.

## Policy option 2: Improve the future qualification of AI systems as high-risk

The procedure foreseen in the proposed AI regulation **to add types of AI systems to the list of AI systems regarded as 'high risk'** gives a prominent role to the European Commission, without detailing with sufficient clarity how such a procedure will unfold, how to initiate it or request its launch, or how long it could take. Furthermore, the foreseen procedure rests on an ultimately subjective appreciation of whether the AI systems to be added to the list can have an **equivalent or greater adverse impact on fundamental rights** compared to the adverse impact initially included in the list.

In their Joint Opinion on the proposed regulation on AI, the EDPB and the EDPS have stressed that already the proposal on the table appears to miss – and may problematically fail – to qualify as high-risk some systems which involve significant risks, and that in any case the relevant 'annexes will need to be regularly updated to ensure that their scope is appropriate' (Joint Opinion 5/2021 9).

In order to prevent the irreparable materialisation of an adverse impact on fundamental rights, it is crucial to design a robust and open system for the inclusion of new categories of AI systems in the list of high-risk systems. In particular, compared to the procedures in place for reacting when a user perceives a significant problem with a system already falling under a high-risk category, the procedure to add new types of systems to the list of high-risk AI systems is particularly weak.

It appears thus necessary to foresee a **faster**, **clearer** and **accessible path** to qualify additional AI systems as high-risk systems.

Additional transparency requirements on the use of AI systems would facilitate the monitoring of the risk of relevant adverse impact. Moreover, **civil society organisations** could be given a role to raise the alarm of major risks, especially insofar as the affected persons would potentially be in vulnerable positions, and might not be able to easily document and communicate harms by themselves.

## Policy option 3: Explicitly ban certain uses of live facial recognition

The proposed AI regulation fails to effectively prohibit real-time remote biometric identification in public spaces for law enforcement purposes, even if it uses words that hint in such a direction. What it provides for is actually **a framework to allow for the widespread use of such AI systems**, in a manner that mirrors for instance the prohibition in the GDPR of the processing of special categories of data, processing that is nevertheless permitted under certain conditions.

This approach does not effectively prevent **the serious adverse impact that can stem from the deployment in Europe of an infrastructure allowing for the recurrent** – even if recurrently short-term – **authorisation of remote biometric identification in public spaces for law enforcement purposes**.

In particular, the **persistent tracking of individuals in public spaces by means of remote biometric identification**, be it or not for law enforcement purposes, must be explicitly and unambiguously prohibited, as it has major consequences for fundamental rights and democracy as such.

## Policy option 4: Regulate 'post' remote biometric identification as the 'live' version

In relation to remote biometric identification, the proposed AI regulation fails to properly address the risks connected to the **retroactive identification** with facial recognition of individuals whose images have been recorded while they were in public spaces. Indeed, the proposed regulation does not even formally prohibit the **'post' remote biometric identification of natural persons**, which is deemed as falling under the high-risk category of AI systems, and thus potentially subject to certification.

In practice, the **risk of persistent tracking and its associated adverse impact on fundamental rights and democracy** are, however, at least equivalent. As the images potentially available for 'post' remote biometric identification of natural persons are actually more numerous than those available at any point in time for real-time identification, they should also **make it possible to draw a much more complete picture of the activities of any individual**, thus representing a major interference with their fundamental rights.

The weakness of the distinction between 'real-time' and 'post' might be best apprehended thinking about access for law enforcement purposes to retained data in the context of the retention of data processed by communication providers under data retention laws. Although it is undisputed that real-time surveillance of communications constitutes an interference with fundamental rights that requires in principle, as a safeguard, a specific authorisation, **the same applies to access to data that have been stored.**[113]

'Post' remote biometric identification of natural persons recorded while in public spaces should be accompanied by the same safeguards as the 'real-time' equivalent if permitted. Any permitted use for law enforcement 'post' remote biometric identification of natural persons recorded while in public spaces should be made dependent on a prior review carried out by a **court** or by an **independent administrative body** whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued. This would be in line with the European Parliament's call to generally subject to judicial review the use of facial recognition by public authorities (P9_TA(2020)0275 § 65).

The EDPB and the EDPS have noted that it is problematic to submit to particularly less stringent rules remote biometric identification systems in which the comparison of data and the identification all occur with 'a significant delay', observing that 'a mass identification system is able to identify thousands of individuals in only a few hours', and that 'the intrusiveness of the processing does not always depend on the identification being done in real-time or not', as 'post' remote biometric identification 'in the context of a political protest is likely to have a significant chilling effect on the exercise of the fundamental rights and freedoms, such as freedom of assembly and association and more in general the founding principles of democracy' (Joint Opinion 5/2021 11). They have described the approach of regulating differently such 'post' remote biometric identification as **flawed** (ibid.).

## Policy option 5: Safeguards for real-time remote biometric identification

The proposed AI regulation leaves in the hands of Member States to define, by law, the exact conditions for the use of in principle prohibited but actually permitted real-time remote biometric identification in public spaces for law enforcement purposes. The proposed Article 5(2) AIA notes

[113] Cf. for instance *Digital Rights Ireland Ltd*. (2014) CJEU Joined Cases C-293/12 and C-594/12ECLI:EU:C:2014:238.

indeed that the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement 'shall comply with **necessary and proportionate safeguards and conditions** in relation to the use, in particular as regards the temporal, geographic and personal limitations', but fails to specify such necessary and proportionate safeguards. The only detailed condition is the need for **prior authorisation** granted by a judicial authority or by an independent administrative authority (proposed Article 5(3) AIA).

The EDPB and the EDPS Joint Opinion on the proposed regulation on AI underlines that the 'use of AI in the area of police and law enforcement requires **area-specific, precise, foreseeable and proportionate rules** that need to consider the interests of the persons concerned and the effects on the functioning of a democratic society' (Joint Opinion 5/2021 9).

The Washington bill passed in 2020[114], which, just like the proposed regulation, 'prohibits' certain uses of facial recognition while allowing them under certain conditions, is more specific in relation to the substantial safeguards foreseen for such permitted uses than the proposal now on the table of the EU legislator.

Experience has shown that, when the EU legislator adopts legislation that establishes limitations of fundamental rights while referring to necessary safeguards to be adopted later at national level, **serious problems can emerge**. A similar lack of specified safeguards led to the invalidation of the Data Retention Directive[115]. More recently, the European Commission noted that some Member States have used the freedom provided to them by the GDPR (in its Article 23) to restrict data subject rights in ways that do not adequately meet the conditions and safeguards required (SWD(2020) 115 final).

The EDPS has in the past consistently called for 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, so that an informed and democratic debate can take place and **until the moment when the EU and Member States have all the appropriate safeguards**' (EDPS 2020 2). That is, the EDPS calls for a moratorium giving time for a democratic debate, but also to identify appropriate safeguards. As it stands, the proposed AI regulation cannot be deemed to guarantee appropriate safeguards.

Substantive safeguards for the prohibited but exceptionally permitted uses of real-time remote biometric identification, if any, must be specified in the future AIA itself, as opposed to being left to the discretion of the Member States.

## Policy option 6: Ban AI systems assigning to categories that constitute sensitive data based on biometric data

The proposed AI regulation provides a definition of 'biometric categorisation system' which is not only **unclear** but also **conceptually problematic**, most notably to the extent that it seems to endorse that it is possible – scientifically, ethically, legally – to use AI systems to assign natural persons to a sexual orientation or to a political orientation. In doing so, the proposal opens the door to the possible national certification in the EU of systems with potentially extremely dangerous impact. The definition should be thus revised to remove the existing ambiguity in this sense.

If a reference to the use of similar AI systems persists in future versions of the proposal, it should be phrased clearly as a **prohibition**. This is also the message from the EDPB and the EDPS, who have explicitly recommended 'a **ban,** for both public authorities and private entities, **on AI systems**

[114] SB 6280.

[115] *Digital Rights Ireland Ltd*. (2014) CJEU Joined Cases C-293/12 and C-594/12 ECLI:EU:C:2014:238.

**categorizing individuals from biometrics** (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other **grounds for discrimination prohibited** under Article 21 of the Charter' (Joint Opinion 5/2021 12).

The question of the definition of biometric data is crucial to properly assess the potential impact of such a ban on current and future problematic practices. It should be thus assessed whether certain AI systems categorising individuals should be prohibited **regardless of whether they categorise on the basis of biometric data**.

## Policy option 7: Clarify the regulation of 'emotion recognition'

The status of 'emotion recognition' in the proposal for a regulation on AI is **not entirely clear**. The definition of emotion recognition, as in the proposed Article 3(34) AIA, seems to imply that emotions and intentions of individuals can be inferred **from biometric data**. This would only make sense – provided that what is meant is that certain emotions and intentions will be attributed, regardless of whether the individual *de facto* experienced or had them – if biometric data are understood in a broad sense, not limited to data allowing for the unique identification of individuals.

In addition, the list of high-risk systems in Annex III includes various references to **systems used 'to detect the emotional state of a natural person'**, without clarifying if these would correspond to what is defined as 'emotion recognition' systems or would potentially be something else or a broader notion, possibly applying also in the absence of biometric data processing.

The EDPB and the EDPS have explicitly recommended that the future regulation on AI should ban 'AI systems whose scientific validity is not proven or which are in direct conflict with essential values of the EU (e.g., **polygraph** (...))' (Joint Opinion 5/2021 12). They have also stated that they 'consider that the use of AI to infer emotions of a natural person is highly undesirable and should **be prohibited**, except for certain well-specified use-cases, namely for health or research purposes' (Joint Opinion 5/2021 12). This statement appears to refer to any use of AI to infer emotions, not limited to biometric data.

## Policy option 8: Increase transparency towards individuals

Generally speaking, the proposed AI regulation privileges imposing obligations on **actors other than the users of AI systems**, who are only subject to a limited number of provisions. For example, in relation to bias detection, it is for the providers of AI systems to take in advance the necessary measures on data governance, anticipating also risks associated with uses yet to be determined.

The use of **extremely high-risk systems** in particular should be conditioned on **additional obligations imposed on users towards individuals**, notably in terms of transparency both prior to the use and during the use. Individuals should indeed be able to access the relevant information, also on data governance, and this will only be possible if they are informed by the users of the AI systems specifically of the systems being used and applied to them.

In their Joint Opinion on the proposed regulation on AI, the EDPB and the EDPS have identified as a major blind spot in the proposal the **absence of references to the individuals affected** by AI systems, '[w]hether they are end-users, simply data subjects or other persons concerned by the AI system' (Joint Opinion 5/2021 8). The EDPB and the EDPS notably call for the proposal to explicitly address the **rights and remedies available to individuals** subject to AI systems (ibid. 9). They have also brought to the fore that, from the perspective of EU data protection law, the 'problem regarding the way to properly inform individuals about' the processing of data for remote biometric identification 'is still unsolved', as is still unsolved 'the effective and timely exercise of the rights of individuals' (ibid. 11). Rights and remedies are especially important when AI systems involve biometric data, and even more where remote processing affects the level of individuals' awareness.

The UK's ICO investigations into the use of live facial recognition in public places revealed numerous problems in terms of signage displayed, communications to the public, and information available in privacy notices (ICO 2021 20). Transparency is thus a key challenge in this area, and it is of the greatest importance because a **lack of transparency directly affects the individuals' ability to exercise their data protection rights** (idem).

The Impact Assessment accompanying the proposal for a regulation on AI conceded that, whenever AI is at stake, '[i]f breaches of fundamental rights do happen, these can also be very difficult to detect and prove, especially when the system is not transparent' (SWD(2021) 84 final Part 1/2 16).

Whereas the proposed Article 52 AIA establishes that '[u]sers of an emotion recognition system or a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto', it also declares that such 'obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences'. This limitation of **transparency**, applying specifically to systems that might be attributing individuals to categories constituting special categories of data, shall only be envisaged if compensated by other means that would render the use of such systems **transparent enough to be accountable**.

## Policy option 9: No special exemptions for EU large-scale databases

The use of biometrics and AI in EU large-scale IT systems raises special risks for fundamental rights. The fact that the proposal for a regulation of AI of the European Commission deliberately pushes away from its scope of application certain upcoming AI systems to be used in the context of the Schengen Information System (SIS), the Visa Information System (VIS), Eurodac, the Entry/Exit System, the European Travel Information and Authorisation System (ETIAS), the European Criminal Records Information System on third-country nationals and stateless persons (ECRIS-TCN), and their Interoperability, is **of great concern**.

Although it is true that the mentioned large-scale IT systems are not completely excluded from the scope of the regulation, the proposed Article 83(1) AIA would leave out of its scope in an indefinite manner any AI system they would use, if the AI system was put on the market at any moment during the first year of application of the proposed regulation. This can have as indirect effect **to incentivise a major advent in the market of potentially high-risk systems** that will nonetheless manage to evade the need to comply with the regulation, later **to be used in systems that process massive quantities of sensitive data of individuals often in a vulnerable position**. This must thus be avoided.

The EDPB and the EDPS have noted that, generally speaking, taking into account that the entry into application of the regulation is envisaged for two years after its entry into force, **it does not appear** '**appropriate** to exempt AI systems already placed on the market for an even longer period of time' (Joint Opinion 5/2021 13).

The mentioned information systems, most of which are already established and some of which are about to be launched in the AFSJ, almost entirely concern only non-EU citizens. Over the years, some have stressed that this fact could explain that in their context 'the use of dubious, untested technologies is taking place with so little public interest and scrutiny' (Jones 2020 35). The **routine registration of the biometric data of third country nationals** in these EU information systems has progressively configured what has been described as 'a system of mass surveillance' (Vavoula 2020).

In a 2020 Resolution, the European Parliament noted that there needs to be an 'extensive and **rigorous public scrutiny and the highest possible level of transparency** both with regard to the risk assessment of individual applications, as well as a general overview of the use of AI, robotics and related technologies in the area of law enforcement and **border control**' (EP P9_TA(2020)0275 para. 71). It is thus essential that large-scale IT systems in the AFSJ comply with the highest standards of EU law.

# 5. References

18 Million Rising et al. Letter to the CEO and Co-founder of Spotify. 4 May 2021.

Access Now et al. Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance. 07 June 2021.

Ada Lovelace Institute. *The Citizens' Biometrics Council: Recommendations and findings of a public deliberation on biometrics technology, policy and governance*. March 2021.

Agencia Española de Protección de Datos (AEPD). Informe jurídico N/REF: 010308/2019. 28 May 2020.

--- Memoria 2020. April 2021.

Ali MS, Islam MS and Hossain MA. 'Gender recognition system using speech signal'. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*. 2(1). 2012. pp. 1-9.

Anderson E. 'Controversial Detroit facial recognition got him arrested for a crime he didn't commit'. *Detroit Free Press*. 20 July 2020.

Ara I. 'Lucknow Police to Use AI Cameras to Track Women's Distress, Activists Slam Privacy Invasion'. *The Wire*. 22 January 2021.

Article 19. *Emotional Entanglement: China's emotion recognition market and its implications for human rights*. 2021.

Article 29 Working Party. Opinion 3/2012 on developments in biometric technologies. WP193. 23 April 2012.

--- Opinion 02/2012 on Facial Recognition in Online and Mobile Services. WP192. 22 March 2012.

--- 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.

Australian Human Rights Commission. *Human Rights and Technology Final Report*. 2021.

Autorité de protection des données (APD). Rapport annuel 2019. 2020.

Bergamini D. *Need for democratic governance of artificial intelligence*. Report for the Parliamentary Assembly of the Council of Europe. Doc. 15150. 24 September 2020.

Berle I. *Face Recognition Technology: Compulsory Visibility and its Impact on Privacy and the Confidentiality of Personal Identifiable Images*. Springer, 2020.

Buolamwini J and T Gebru. 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification'. *Proceedings of Machine Learning Research. Conference on Fairness, Accountability, and Transparency*. 81. 2018. pp. 1–15.

Burt C. 'Concerns about biometric online proctoring expressed by students in Australia, U.S. and Canada'. *Biometric Update*. 3 July 2020.

Bygrave LA and L Tosoni, 'Article 4(14). Biometric Data' in C Kuner, LA Bygrave and C Docksey (eds). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press; 2020. 207-216.

CAHAI. Feasibility study. CAHAI(2020)23. Council of Europe, Strasbourg. 17 December 2020.

Clifford, D et al. 'Artificial Intelligence and Sensitive Inferences: New Challenges for Data Protection Laws' in M Findlay et al. (eds). *Regulatory Insights on Artificial Intelligence: Research for Policy*. Edward Elgar, 2021 / ANU College of Law Research Paper No. 21.1.

Cobbe J, MS Ah Lee and J Singh. Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems. ACM Conference on Fairness, Accountability, and Transparency (FAccT '21), March 1–10, 2021, Virtual Event, Canada. ACM, New York, NY, USA.

Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). Délibération n°D-126-EUS/2020du 29/07/2020 relative à la définition de l'usage des technologies de reconnaissance faciale par les établissements de prévoyance sociale pour la preuve de vie des allocataires.

Commission Nationale de l'Informatique et des Libertés (CNIL). *Reconnaissance faciale : pour un débat à la hauteur des enjeux*. 15 Novembre 2019.

--- *Reconnaissance faciale dans les aéroports : quels enjeux et quels grands principes à respecter ?* 9 October 2020.

--- Délibération n° 2020-136 du 17 décembre 2020 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports (demande d'avis n°20019694). 17 December 2020.

Committee of Ministers of the Council of Europe. Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies. Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies.

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Guidelines on Facial Recognition. Directorate General of Human Rights and Rule of Law. T-PD(2020)03rev4.

Cox K. 'Facebook will pay more than $300 each to 1.6M Illinois users in settlement'. Arstechnica. 15 January 2021. https://arstechnica.com/tech-policy/2021/01/illinois-facebook-users-to-get-more-than-300-each-in-privacy-settlement/

Crawford K. 'Halt the use of facial-recognition technology until it is regulated'. *Nature World View*. 27 August 2019.

Cunrui, W et al. 'Facial feature discovery for ethnicity recognition'. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. 9.2. 2019.

Das, D, R de Jong and L Kool. *Valued at work. Limits to digital monitoring at the workplace using data, algorithms and AI*. Rathenau Instituut. 2020.

Datakalab. Privacy policy, updated 15 March 2021.

Datta, AK, M Datta, and PK Banerjee. *Face detection and recognition: theory and practice.* CRC Press, 2015.

De Puit M, M Ismail and X Xu. 'LCMS Analysis of Fingerprints, the Amino Acid Profile of 20 Donors'. *Journal of Forensic Sciences*. 59(2). 2014. pp. 364-370.

Earls Davis PA. 'Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR'. *European Data Protection Law (EDPL)* 6 (3). 2020. pp. 365-377.

Eglitis, T, R Guest, and F Deravi. 'Data behind mobile behavioural biometrics–a survey'. *IET Biometrics* 9(6) 2020. pp. 224-237.

Ernst & Young Baltic AS. *Towards the European Level Exchange of Facial Images: Legal Analysis for TELEFI project*. Towards the European Level Exchange of Facial Images (TELEFI). 7 February 2020.

European Association for Biometrics (EAB). *Misunderstandings in Misunderstandings on Biometrics A Position Paper*. August 2020.

European Commission (EC). *Digital Transformation Monitor: Biometrics technologies: A key enabler for future digital services.* January 2018.

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

--- Commission Staff Working Document accompanying the Communication from the Commission 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. SWD(2020) 115 final. Brussels, 24 June 2020.

--- *Communication on the EU Security Union Strategy*, COM(2020) 605 final, 24 July 2020.

--- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Union of Equality: LGBTIQ Equality Strategy 2020-2025. COM(2020) 698 final. Brussels, 12 November 2020.

--- Public consultation on the AI White Paper: Final report. DG CONECT. November 2020.

--- Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts. COM(2021) 206 final. Brussels, 21 April 2021.

--- Commission Staff Working Document: Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union legislative acts. SWD(2021) 84 final. Part 1/2. Brussels, 21 April 2021.

European Commission (EC) Directorate-General for Research and Innovation. Gendered Innovations 2: How inclusive analysis contributes to research and innovation. July 2020.

European Data Protection Board (EDPB). Opinion 9/2018 on the draft list of the competent supervisory authority of France regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), adopted on 25th September 2018.

-- Opinion 21/2018 on the draft list of the competent supervisory authority of Slovakia regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), adopted on 25th September 2018.

--- Opinion 26/2018 on the draft list of the competent supervisory authority of Luxembourg regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), adopted on 4 December 2018.

--- Facial recognition in school renders Sweden's first GDPR fine. EDPB website news. 22 August 2019. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_sv

--- Guidelines 3/2019 on processing of personal data through video devices, adopted on 29 January 2020.

--- Fine for processing students' fingerprints imposed on a school. EDPB website news. 5 March 2020. https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

-- Dutch DPA fines municipality for Wi-Fi tracking. EDPB website news. 29 April 2021. https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en

--- Guidelines 02/2021 on virtual voice assistants, Version2.0, adopted on 7 July 2021.

European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 June 2021.

European Data Protection Supervisor (EDPS). Opinion 4/2020 on the European Commission's White Paper on Artificial Intelligence –A European approach to excellence and trust. 29 June 2020.

--- TechDispatch #1/2021 - Facial Emotion Recognition. 26 May 2021.

European Data Protection Supervisor (EDPS) and Agencia Española de Protección de Datos (AEPD). *14 misunderstandings with regard to biometric identification and authentication.* 24 June 2020.

European Digital Rights initiative (EDRi), Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States. 13 May 2020. 2020(a).

--- Use cases: Impermissable [sic] AI and fundamental rights breaches. 2020(b).

European Parliament. *Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*. P9_TA(2020)0275.

European Union Agency for Fundamental Rights (FRA). Opinion 2/2017: The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS). Vienna, 30 June 2017.

--- Under watchful eyes: Biometrics, EU IT systems and fundamental rights. 2018.

--- Facial recognition technology: Fundamental rights considerations in the context of law enforcement. FRA Focus. 2020. 2020(a).

--- Fundamental rights report. 2020. 2020(b).

--- Getting the future right: Artificial Intelligence and fundamental rights. 2020(c).

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). *Biometrics in Large-Scale IT: Recent trends, current performance capabilities, recommendations for the near future*. 30 April 2015.

--- *Artificial Intelligence in the Operational Management of Large-scale IT Systems. Perspectives for EU-LISA*: Research and Technology Monitoring Report. July 2020.

Expert Group on Liability and New Technologies – New Technologies Formation. Liability for artificial intelligence and other emerging digital technologies. Luxembourg. 2019.

Fairhurst M, C Li, M Da Costa-Abreu. Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data. IET Biom., 6(6), 2017. pp. 369-378.

Federal Trade Commission (FTC). California Company Settles FTC Allegations It Deceived Consumers about use of Facial Recognition in Photo Storage App. January 2021. https://www.ftc.gov/news-events/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers

Feldman Barrett et al. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. Psychological Science in the Public Interest 2019. 20(1) 1-68.

Fino E et al. 'Unfolding political attitudes through the face: facial expressions when reading emotion language of left- and right-wing political leaders'. *Scientific Reports*. 9. 15689. 2019.

Fondazione Giacomo Brodolini (FGB). *Fundamental rights review of EU data collection instruments and programmes: Final report*. 2019.

Freedom House. Coalition Letter Requests Federal Moratorium on the Use of Facial Recognition Technology. 16 February 2021. https://freedomhouse.org/article/coalition-letter-requests-federal-moratorium-use-facial-recognition-technology

Garante per la Protezione dei Dati Personali (Garante). Installazione di apparati promozionali del tipo 'digital signage' (definiti anche Totem) presso una stazione ferroviaria. 21 December 2017 [7496252].

Gellert R. EDPB opinion on the draft lists of competent supervisory authorities regarding the processing operations subject to DPIAs. European Data Protection Law (EDPL) Review. 2018. 4. 500-504.

Global Privacy Assembly (GPA). Resolution on Facial Recognition Technology. October 2020.

González Fuster G. Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, Directorate-General for Internal Policies PE 656.295 July 2020.

Grother P, M Ngan and K Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280. December 2019.

Haeck P. 'Ex-Google boss slams transparency rules in Europe's AI bill'. *Politico*. 31 May 2021.

Halpert J. 'In Washington State's landmark facial recognition law, public sector practices come under scrutiny and regulation'. *DLA Piper. Data Protection, Privacy and Security Alert*. 22 April 2020.

Havas Paris. 'IDEMIA and Sopra Steria Chosen by eu-LISA to Build the New Shared Biometric Matching System (sBMS) for Border Protection of the Schengen Area'. *Business Wire*. 3 June 2020.

Heilweil R. 'Big tech companies back away from selling facial recognition to police. That's progress'. *Vox - Recode*. 11 June 2020.

Hernandez J et al. Affective Spotlight: Facilitating the Communication of Affective Responses from Audience Members during Online Presentations. CHI. May 2021. https://www.microsoft.com/en-us/research/publication/affectivespotlight-facilitating-the-communication-of-affective-responses-from-audience-members-during-online-presentations/

Herta. *Herta awarded with the highly competitive 'COVID-19 Response Seal of Excellence' from the European Commission*. 26 May 2020. https://hertasecurity.com/news/herta-awarded-with-the-highly-competitive-covid-19-response-seal-of-excellence-from-the-european-commission/

High Level Expert Group for Artificial Intelligence (AI HLEG). *Ethics Guidelines for Trustworthy AI*. 2019.

--- *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment*. 17 July 2020.

Hill K. Wrongfully Accused by an Algorithm, NY Times. 24 June 24 2020 (2020a).

--- Another Arrest and Jail Time Due to a Bad Facial Recognition Match, NY Times. 29 December 2020 (2020b).

Homo Digitalis. The Greek DPA investigates the Greek Police. 31 August 2020. https://www.homodigitalis.gr/en/posts/7684

Hue B. 'Comment fonctionne la reconnaissance faciale testée à l'aéroport d'Orly'. *RTL*. 27 March 2021.

Hulaud, Stéphane. 'Identification of taste attributes from an audio signal'. US Patent 10,891,948. 12 January 2021.

Human Rights Watch. 'China: Big Data Program Targets Xinjiang's Muslims'. 9 December 2020. https://www.hrw.org/news/2020/12/09/china-big-data-program-targets-xinjiangs-muslims

Information Commissioner's Office (ICO). The use of live facial recognition technology in public places. 18 June 2021.

Israel T. *Facial recognition at a crossroads: Transformation at our borders and beyond*. Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC). September 2020.

Jasserand-Breeman, C. *Reprocessing of biometric data for law enforcement purposes: Individuals' safeguards caught at the Interface between the GDPR and the 'Police' Directive?* University of Groningen. 2019.

Jones C. *Automated suspicion: The EU's new travel surveillance initiatives*. Statewatch. June 2020.

Kachur et al. 'Assessing the Big Five personality traits using real-life static facial images'. *Scientific Reports*. 10, 8487. 2020.

Kafeero S. 'Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests'. *Quartz Africa*. 27 November 2020.

Kak A. Introduction, in A Kak (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute, 1 September 2020, pp. 6-15.

Karanja SK. *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation*. Martinus Nijhoff Publishers. 2008.

Keyes O. 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition'. *Proceedings of the ACM on Human-Computer Interaction*. 2I. November 2018. pp. 1–22.

Kind C. 'Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics'. *Ada Lovelace Institute Blog*. 30 April 2021.

Kindt E. 'A First Attempt at Regulating Biometric Data in the European Union'. in A Kak (ed.). *Regulating Biometrics: Global Approaches and Urgent Questions.* AI Now Institute, 1 September 2020, pp. 62-69.

Kosinski M. 'Facial recognition technology can expose political orientation from naturalistic facial images'. *Scientific Reports*. 11, 100. 2021.

Kuner C and M Marelli (eds). *Handbook on data protection in humanitarian action.* Brussels Privacy Hub (BPH) and International Committee of the Red Cross (ICRC). 2020.

Lacroix C. Preventing discrimination caused by the use of artificial intelligence. Parliamentary Assembly of the Council of Europe. Doc. 1515129 September 2020.

Laufer D and S Mainek. 'A Polish Company is Abolishing our Anonymity'. *NetzPolitik*. 10 July 2020.

Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LFDI). Gesichtserkennung: LfDI eröffnet Verfahren gegen Unternehmen PimEyes. 26 May 2021. https://www.baden-wuerttemberg.datenschutz.de/gesichtserkennung-lfdi-eroeffnet-verfahren-gegen-unternehmen-pimeyes/

Lee-Morrison L. *Portraits of Automated Facial Recognition on Machinic Ways of Seeing the Face*. Transcript. 2019.

Lequesne Roth C. *New Surveillance Technologies in Public Spaces: Challenges and Perspectives for European Law at the Example of Facial Recognition*. Partnership Security in Public Spaces, Urban Agenda for the EU. April 2021.

Leuner, J. 'A Replication Study: Machine Learning Models are Capable of Predicting Sexual Orientation from Facial Images'. arXiv preprint: arXiv:1902.10739. 2019.

Magnet, SA. *When biometrics fail: Gender, Race, and the Technology of Identity*. Duke University Press. 2011.

Mantelero A. Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies, accompanying the Guidelines on artificial intelligence and data protection adopted by the Committee of the Convention for the Protection of Individuals with regards to Processing of Personal Data (Convention 108) on 25 January 2019.

Martin AK and EA Whitley. 'Fixing identity? Biometrics and the Tensions of Material Practices'. *Media, Culture & Society*. 35(1). 2013, pp. 52–60.

Martini, M. 'Regulating Algorithms: How to demystify the alchemy of code?'. In M Ebers and S Navas (eds). *Algorithms and Law*. 2020, pp. 100-135.

Marx M. 'New win against biometric mass surveillance in Germany'. EDRi, https://edri.org/our-work/new-win-against-biometric-mass-surveillance-in-germany/ 2021.

Mascellino A. 'Union warns against biometric monitoring of employees amid increase in remote work'. *Biometric Update*. 30 October 2020.

Matus K and M Veale. Certification Systems for Machine Learning: Lessons from Sustainability. 2 June 2021.SocArXiv: doi:10.1111/rego.12417.

Ministère de l'intérieur. *Livre blanc de la sécurité intérieure*. 2020.

Misener D. 'Apple buys Emotient emotion detection company'. *CBC News*. 16 January 2016.

Monroy M. Project Interoperability: EU to pay 300 million EUR for face and fingerprint recognition. 5 June 2020. https://digit.site36.net/2020/06/05/project-interoperability-eu-to-pay-300-million-eur-for-face-and-fingerprint-recognition/

Mordini E, D Tzovaras, and H Ashton. 'Introduction'. In E Mordini and D Tzovaras (eds). *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, 2012. pp. 11-19.

Muntstroom PCP, Brussels Capital Region Pre-Commercial Procurement (PCP) regarding R&D of end-to-end solutions for monitoring multi-faceted people flow. *Market consultation document -Annex 1: Scope of the project*.2020.

Nesterova, I. 'Mass data gathering and surveillance: the fight against facial recognition technology in the globalized world'. *SHS Web of Conferences*. Vol. 74. EDP Sciences, 2020.

Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, Joint investigation of Clearview AI, Inc., 2 February 2021.

Pato JN and LI Millett (eds). *Biometric Recognition: Challenges and Opportunities.* The National Academic Press. 2010.

Peinado F. 'Las cámaras que leen la cara se extienden por Madrid'. *El País*. 29 November 2019.

Peng K. 'Facial recognition datasets are being widely used despite being taken down due to ethical concerns. Here's how'. *Freedom to Tinker.* Princeton's Center for Information Technology Policy. 21 October 2020.

Penner K. European Union. in Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations. 2019. pp. 17-38.

Penner K and F Chiusi. European Union in Automating Society Report 2020. AlgorithmWatch and Bertelsmann Stiftung October 2020. pp. 14-31.

Poddar M and S Rajam. 'Proof of Sexual Orientation – A Precondition for Asylum?' *Cambridge International Law Journal Posts.* 2018.

Privacy International. Briefing: Biometrics: Friend or foe of privacy? 2017.

Ramu, T, K Suthendran, and T Arivoli. 'Machine learning based soft biometrics for enhanced keystroke recognition system'. *Multimedia Tools and Applications*. 2019. pp. 10029–10045.

Raso, F, H Hilligoss, V Krishnamurthy, C Bavitz and K Levin. Artificial Intelligence & Human Rights: Opportunities & Risks. Berkman Klein Center for Internet & Society Research Publication. 2018.

Ross A and AK Jain. Multimodal Biometrics: an overview. *12th European Signal Processing Conference*, 1221-1224. IEEE. 2004.

Sánchez-Monedero J and L Dencik. 'The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl'. *Information, Communication & Society*. 3 August 2020.

Sandvik, KB. 'Wearables for something good: Aid, dataveillance and the production of children's digital bodies'. *Information, Communication & Society* 23(14). 2020. pp. 2014-2029.

Sanjekar PS and JB Patil. 'An overview of multimodal biometrics'. *Signal & Image Processing*. 2013. 4(1), pp. 57-64.

Satisky J. 'Duke study recorded thousands of students' faces. Now they're being used all over the world'. *The Chronicle*. 12 June 2019.

Scheuerman MK, Paul JM, Brubaker JR. How computers see gender: An evaluation of gender classification in commercial facial analysis services. Proceedings of the ACM on Human-Computer Interaction. 2019 Nov 7;3(CSCW). pp. 1-33.

Spivak J and C Garvie. A Taxonomy of Legislative Approaches to Face Recognition in the United States, in A Kak (ed.). Regulating Biometrics: Global Approaches and Urgent Questions. AI Now Institute, 1 September 2020, pp. 86-95.

Shu C. Microsoft Says It Is 'Dismayed' by the Forced Separation of Migrant Families at the Border. TechCrunch, 19 June 2018. http://social.techcrunch. com/2018/06/18/microsoft-says-it-is-dismayed-by-the-forced-separation-of-migrant-families-at-the-border

Silva MR and J Varon. Reconhecimento facial no setor público e identidades trans. Coding Rights, 2021.

Thales. *Behavioral biometrics and biometrics in payment cards: Beyond the PIN and password.* https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/inspired/behavioral-biometrics. 2020.

Tian, Y, T Kanade, and JF Cohn. 'Facial expression recognition'. In SZ Li and K Jain (eds). *Handbook of Face Recognition* (Second edition). Springer, 2011. pp. 487-519.

Tistarelli M and E Grosso. 'Human face analysis: from identity to emotion and intention recognition'. In *Third International Conference on Ethics and Policy of Biometrics and International Data Sharing*, ICEB 2010 Hong Kong, January 4-5, 2010. Revised Selected Papers. Springer, 2010. pp. 76-88.

TNN. 'Lucknow: Smart cams to read expressions of women in distress'. *Times of India*. 21 January 2021.

UNICEF. *Faces, Fingerprints & Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs*. July 2019.

United Nations (UN) High Commissioner for Human Rights. *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests.* A/HRC/44/24. 24 June 2020.

United Nations (UN) Security Council. Resolution 2396 (2017), adopted by the Security Council at its 8148th meeting, on 21 December 2017.

United Nations (UN) Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Surveillance and human rights. A/HRC/41/35. 28 May 2019.

Van Noorden R. 'The ethical questions that haunt facial-recognition research'. *Nature. News feature.* 18 November 2020.

Vavoula N. 'The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection'. *European Law Review*. 3. 2020, pp. 348-372.

Vincent J. 'NYPD used facial recognition to track down Black Lives Matter activist'. *The Verge*. 18 August 2020.

Von der Leyen U. *A Union that strives for more: My agenda for Europe*. Brussels. 2019.

Wang, Y and M Kosinski. 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images'. *Journal of Personality and Social Psychology*. 114(2). 2018.

Wickert F. *Technical aspects. in S Azria and F Wickert. Facial Recognition: Current Situation and Challenges*. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Strasbourg. 13 November 2019. T-PD(2019)05rev, pp. 2-11.

Wright J. 'Suspect AI: Vibraimage, Emotion Recognition Technology and Algorithmic Opacity'. *Science, Technology and Society*. 2021.

Yampolskiy, RV and V Govindaraju. 'Behavioural biometrics: a survey and classification'. *International Journal of Biometrics*. 1(1). 2008. pp. 81-113.

QA-01-21-551-EN-N

As the use of biometrics becomes commonplace in the era of artificial intelligence (AI), this study aims to identify the impact on fundamental rights of current and upcoming developments, and to put forward relevant policy options at European Union (EU) level.

Taking as a starting point the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on AI, presented by the European Commission in April 2021, the study reviews key controversies surrounding what the proposal addresses through the notions of 'remote biometric identification' (which most notably includes live facial recognition), 'biometric categorisation' and so-called 'emotion recognition'.

Identifying gaps in the proposed approaches to all these issues, the study puts them in the context of broader regulatory discussions. More generally, the study stresses that the scope of the current legal approach to biometric data in EU law, centred on the use of such data for identification purposes, leaves out numerous current and expected developments that are not centred on the identification of individuals, but nevertheless have a serious impact on their fundamental rights and democracy.

This is a publication of the Scientific Foresight Unit (STOA)
EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

ISBN 978-92-846-8818-0 | doi: 10.2861/384495 | QA-01-21-551-EN-N