STUDY

Requested by the JURI and PETI committees

European Parliament

Biometric Recognition and Behavioural Detection

Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces

Policy Department for Citizens' Rights and Constitutional Affairs EN
Directorate-General for Internal Policies
PE 696.968 -August 2021

Biometric Recognition and Behavioural Detection

Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI and PETI Committees, analyses the use of biometric techniques from an ethical and legal perspective. Biometric techniques raise a number of specific ethical issues, as an individual cannot easily change biometric features, and as these techniques tend to intrude into the human body and ultimately the human self. Further issues are more generally associated with large-scale surveillance, algorithmic decision making, or profiling. The study analyses different types of biometric techniques and draws conclusions for EU legislation.

This document was requested by the European Parliament's Committee on Legal Affairs and Petitions Committee.

AUTHORS
Christiane WENDEHORST, University of Vienna, Austria
Yannic DULLER, University of Vienna, Austria

The authors wish to thank Matthias KLONNER, University of Vienna, for background support.

ADMINISTRATOR RESPONSIBLE
Mariusz MACIEJEWSKI

EDITORIAL ASSISTANT
Christina KATSARA

LINGUISTIC VERSIONS
Original: EN

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

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

Manuscript completed in August 2021

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

DISCLAIMER AND COPYRIGHT

CONTENTS

LIST OF ABBREVIATIONS 5

LIST OF BOXES WITH ILLUSTRATIONS 7

LIST OF FIGURES 7

LIST OF TABLES 7

EXECUTIVE SUMMARY 8

1. CURRENT AND POTENTIAL FUTURE DEVELOPMENTS OF BIOMETRIC TECHNIQUESE 12

1.1. Biometric technologies 12

1.1.1. Strong, weak and soft biometrics 12

1.1.2. First and second generation biometric technologies 13

1.1.3. Future trends and technologies 15

1.2. Identification, categorisation, and detection 20

1.3. Scope of this Study 21

2. OVERVIEW OF LEGISLATION AND CASE LAW 23

2.1. Legislation 23

2.1.1. International law 23

2.1.2. EU law 25

2.1.3. Proposals by the European Commission 30

2.1.4. National law 32

2.2. Case Law 35

2.2.1. European Court of Human Rights (ECtHR) 35

2.2.2. Court of Justice of the European Union (CJEU) 37

2.2.3. National courts/data protection authorities 38

3. ETHICAL ASPECTS OF BIOMETRIC IDENTIFICATION 42

3.1. Characteristic steps involved in biometric identification 42

3.2. Ethical issues raised by enrolment 43

3.2.1. 'Datafication' of humans, power and human dignity 44

3.2.2. Potential for harm 45

3.3. Ethical issues raised by application in public spaces 47

3.3.1. Large-scale surveillance 47

3.3.2. Stigmatisation and discrimination 50

4. ETHICAL ASPECTS OF BIOMETRIC CATEGORISATION 52

4.1. Characteristic steps involved in biometric categorisation 52

4.2. Ethical issues raised 53

5. THE ETHICAL ASPECTS OF BIOMETRIC DETECTION 56

5.1. Characteristic steps involved in biometric detection 56

5.2. Ethical issues raised 57

6. CONCLUSIONS WITH REGARD TO THE PROPOSAL FOR AN ARTIFICIAL INTELLIGENCE ACT 60

6.1. General approach of the AIA Proposal 61

6.1.1. Biometric techniques and the risk-based approach 61

6.1.2. Interplay of the AIA Proposal with other EU legislation 63

6.2. Recommendations with regard to definitions 66

6.2.1. Biometric data and biometrics-based data 66

6.2.2. Real-time and post remote biometric identification 68

6.2.3. Emotion recognition and biometric categorisation 69

6.2.4. Biometric inferences 70

6.3. Recommendations with regard to Title II 71

6.3.1. Differentiating between *per se*-prohibitions and restrictions 71

6.3.2. Adding total surveillance and infringements on mental privacy and integrity as prohibited AI practices 71

6.3.3. Allowing for flexible adaptation of the list of prohibited AI practices 72

6.3.4. Clarifying the relationship with prohibitions following from other laws 73

6.4. Recommendations with regard to biometric identification 74

6.4.1. Limitations on scope of the existing proposal 74

6.4.2. A new regulatory approach 77

6.4.3. Clarifications with regard to data collection and storage 79

6.5. Recommendations with regard to emotion recognition and biometric categorisation 80

6.5.1. Emotion recognition and biometric categorisation as restricted AI practices 80

6.5.2. How to design the restrictions? 80

6.6. Recommendations with regard to decisions taken 82

6.6.1. Mirroring and adapting the rule in Article 14(5) 82

6.6.2. Use as legal evidence 82

6.7. Recommendations with regard to biometric inferences 83

6.8. Recommendations with regard to consent management 86

REFERENCES 88

ANNEX: PROPOSED WORDING OF TITLE II AND TITLE IIA 94

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AFIS	Automated Fingerprint Identification System
Art(s)	Article(s)
BCI	Brain-Computer-Interface
BDSG	Bundesdatenschutzgesetz - German Federal Data Protection Act
BIPA	Illinois Biometric Information Privacy Act
BVerfG	Bundesverfassungsgericht - German Constitutional Court
BVerwG	Bundesverwaltungsgericht – German Federal Administrative Court
CCPA	California Consumer Privacy Act
CCTV	Closed-Circuit Television
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DNA	Deoxyribonucleic acid
DSA	Digital Services Act
DSG	Datenschutzgesetz - Austrian Data Protection Act
EC	European Commission
ECG	Electrocardiography
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
Ed(s)	Editor(s)
Edn	Edition

EEG	Electroencephalography
EES	Entry-Exit-System
e.g.	exempli gratia (for example)
EGE	European Group on Ethics in Science and New Technologies
etc.	et cetera (and so on)
EU	European Union
EUDPR	European Union Data Protection Regulation – Regulation (EU) 2018/1725
GDPR	General Data Protection Regulation – Regulation (EU) 2016/679
i.e.	id est (that is)
IoT	Internet of Things
LED	Law Enforcement Directive – Directive (EU) 2016/680
OGH	Oberster Gerichtshof - Austrian Supreme Court of Justice
OJ	Official Journal of the European Union
Para(s)	Paragraph(s)
PIPL	Personal Information Protection Law of the People's Republic of China
SIS	Schengen Information System
SPG	Sicherheitspolizeigesetz- Federal Security Police Act
TEU	Treaty of the European Union (TEU)
TTDSG	German Act on Data Protection and Privacy in Telecommunications and Telemedia
UDHR	Universal Declaration of Human Rights
UK-DPA	Data Protection Act of the United Kingdom
UN	United Nations

LIST OF BOXES WITH ILLUSTRATIONS

Illustration 1: Differentiating biometrics-based data and other personal data 67
Illustration 2: Differentiating 'real-time' and 'post' remote identification 69
Illustration 3: Relationship between 'biometric categorisation' and 'biometric inferences' 70
Illustration 4: Undesirable remote biometric identification beyond law enforcement 76
Illustration 5: Remote biometric identification in grey zones around law enforcement 77
Illustration 6: Data collection and storage in the context of biometric identification 79
Illustration 7: Justification of emotion recognition or biometric categorisation 81
Illustration 8: Emotion recognition or biometric categorisation used as legal evidence 82
Illustration 9: Personality profiles created with the help of a video game 84
Illustration 10: Biometric inferences drawn with regard to third parties 85

LIST OF FIGURES

Figure 1: Authentication/identification, categorisation, and detection 21
Figure 2: Steps involved in biometric identification 43
Figure 3: Steps involved in biometric categorisation 53
Figure 4: Steps involved in biometric detection 57
Figure 5: Risk-based approach of the AIA Proposal 62
Figure 6: Biometric techniques under the risk levels of the AIA Proposal 63

LIST OF TABLES

Table 1: Admissibility of biometric techniques (based on simplified assumptions) 64
Table 2: Limitations on scope with regard to identification measures 74

EXECUTIVE SUMMARY

Background

Biometric identification together with biometric categorisation, behavioural detection, emotion recognition, brain-computer-interfaces (BCIs), and similar techniques are being used to an increasing extent by public and private bodies. They serve a broad variety of purposes, ranging from healthcare to law enforcement and border control to warfare, and are deployed in public as well as in private spaces.

The term 'biometric techniques' should be understood as including any technology or operation that

- relies on specific technical processing of data relating to physical, physiological or behavioural aspects of the human body (including when in motion);
- for purposes such as authentication or identification of human individuals, categorisation of human individuals according to permanent or long-term characteristics (including with a view to predicting future behaviour), or detection of temporary or permanent conditions of a human individual (such as fear, fatigue, or illness, or a particular intent).

Beyond traditional biometric techniques such as fingerprint or facial recognition, biometric techniques clearly include, e.g., analysis of keystroke or mouse dynamics, gesture dynamics, signature dynamics, as well as voice and gait features. By way of contrast, the term is normally not understood as including behaviour that can be controlled by the human will to a higher extent, such as shopping behaviour, browsing history or the content of communication. As far as such behaviour is analysed to infer conditions of a genetic, physical, physiological, behavioural, psychological or emotional nature characterising a particular individual, it may, however, be justified to include them in the notion of biometric techniques in a broader sense.

Major trends are the increasing use of 'weak' and 'soft' biometrics alongside 'strong' biometrics, focussing on a variety of patterns of a more behavioural kind, and the development towards multimodal biometrics. Together with enhanced sensor and computing capabilities as well as enhanced connectivity, this paves the way for mass roll-out of biometric technologies in a broad variety of sectors and for a broad variety of purposes, far beyond law enforcement and border control, turning biometric technologies into something like universal technologies.

Latest technological advances include improved sensors, enabling the capture of entirely new types of bio-signals, such as heart beats and brain waves via EEG or ECG, and the development of brain-computing-interfaces (BCI). BCIs measure neuro activity and translate brain activity into machine-readable input. These new technologies are potentially highly intrusive, allowing for the detection of thoughts or intent and possibly also for influencing operations of the human brain.

The Proposal for an Artificial Intelligence Act (AIA) of 21 April 2021 addresses such techniques in various ways, as do other instruments, both existing and in the pipeline. However, the question arises whether existing and proposed legislation adequately addresses ethical and fundamental rights issues raised.

Aim

This study analyses the ethical and legal aspects raised by biometric techniques. In particular, it provides

- a suggestion for a comprehensive definition of 'biometric techniques' and for grouping them into authentication/identification, categorisation and detection techniques;

- a stock-taking of related legal instruments, case-law and literature;
- a thorough ethical and legal assessment of the implications raised;
- recommendations on a possible legislative framework for responsible use of biometric techniques.

Key findings

Biometric identification of humans

The main ethical issue raised specifically by biometric identification is related to the enrolment phase, i.e. the creation and storage of a unique template that identifies a particular person. The enrolment phase and the deployment phase may overlap where templates are refined during deployment, e.g. through supervised learning in the field. Creating unique templates means transforming unique physical features of a human being into digital data, leading to a 'datafication' of humans. Since the features that uniquely identify a person are part of a person's body, their collection and use interfere with a human's personal autonomy and dignity. Once this template is created and stored, anyone who comes into possession of it in the future has the power to trace and recognise that individual anywhere in the world and potentially for any purpose. There is no way for the individual to escape it as an individual cannot normally change 'strong' biometric identifiers. Considering also data security concerns, collecting and storing biometric templates has a significant potential for harm.

Apart from this, ethical issues raised by the use of biometric identification methods in public spaces do not so much relate specifically to biometrics, but to large-scale surveillance of individuals as such (i.e., they are similar to issues raised by, for example, large-scale surveillance using mobile device signals), or otherwise to the purposes for which the technology is used, and how it is used. The dimension of ethical issues raised depends, in particular, on

- the concrete purpose of identification;
- the place, manner or dimension of identification;
- the transparency of the identification measures taking place;
- the reactions (e.g. arrest) triggered by a high matching score;
- the evidentiary force ascribed to a high matching score and possibilities of the individual to demonstrate error or identity fraud; and
- any storage and further processing of matching data (e.g. for the creation of mobility profiles).

Issues of discrimination or stigmatisation arise mostly as a result of deficiencies in one or several of the aspects mentioned (e.g. where, despite diminished accuracy of the system with particular ethnic groups, unjustified assumptions are made).

Biometric categorisation of humans

The main ethical issues raised by the biometric categorisation of human individuals (e.g. allocation to risk groups within an airport security system, assessment of job applicants) are related to the development and concrete use of categorisation systems. In particular, ethical issues arise in relation to the definition of categories, the associated assumptions and the conclusions or reactions triggered by the system, leading to risks such as discrimination, stigmatisation, and the drawing of inappropriate inferences. Further risks include manipulation and exploitation of group-specific vulnerabilities. Ethical issues may be related to, in particular,

- the concrete purpose, context and conditions of categorisation;

- the degree of sensitivity of data collected and of inferences drawn;
- the accuracy of the system, the appropriateness of inferences drawn, and any control mechanisms, including human oversight;
- the gravity (including potential irreversibility) of consequences triggered by the system;
- the awareness of the individual of the categorisation and the possibility of the individual to challenge the output; and
- any storage and further processing of data for profiling purposes.

It follows that the fundamental rights risks to be addressed in this context are primarily associated with standardised profiling and/or scoring as a means to achieve a given end in a given social context. The fact that categorisation includes biometrics (e.g. that a person's age is inferred from wrinkles in their face rather than from their shopping history) adds some ethical relevance, as an individual cannot easily change most biometric traits (e.g. wrinkles), but it is hardly ever the decisive factor (as compared, e.g., with age-specific targeting that might follow categorisation). Biometric inferences, i.e. inferences drawn with regard to permanent or long-term physical, physiological or behavioural characteristics, may in general be ethically even more relevant than the use of biometric techniques as such.

Biometric detection of human conditions

The main ethical issues raised by the biometric detection of human conditions (e.g. intention to commit a crime, fear, fatigue or illness) follow from its potentially intrusive nature, often analysing very intimate traits, some of them beyond the individual's consciousness. In addition, previously unknown conditions, when revealed to the individual, may cause stress or anxiety.

Most ethical issues raised by the use of biometric detection do not relate specifically to the fact that biometric data are used for inferring a condition, but to detection of that condition as such (i.e., they are largely identical to issues raised by, for example, detection on the basis of a shopping or browsing history), and to the way the information about this condition is used (e.g. for manipulation and exploitation of detected vulnerabilities). Again, the fact that an individual has little control over their physical, physiological or behavioural signals, many of which will be subconscious, may give their use to detect conditions a special ethical dimension.

Fundamental rights risks posed by biometric detection techniques are very similar to those posed by biometric categorisation. However, within the field of biometric detection systems, it is systems detecting human emotions, thoughts and intentions that deserve particular attention from an ethical and regulatory perspective, potentially calling for a new set of 'neuro-rights' (such as the right to mental privacy and mental integrity).

Key recommendations

The recent Proposal for an AIA goes in the right direction but still fails to address ethical concerns in a consistent manner, in particular due to various restrictions in the scope of provisions. The study proposes to include in the Proposal a new Title IIa that is devoted to restricted AI practices, including biometric techniques and inferences, ensuring responsible use of these techniques without stifling innovation and growth.

The Study suggests that, in particular, the amendments to the Proposal as listed below should be considered by the European Parliament.

The definitions in Article 3 should be amended:

- The definitions of 'emotion recognition system' and 'biometric categorisation system' should be detached from the concept of 'biometric data' as defined in the GDPR and rather based on a new definition of 'biometrics-based data';
- The definitions of 'remote' and 'real-time' with regard to biometric identification should be slightly modified.
- An additional definition for 'biometric inferences' should be introduced;

Title II on prohibited AI practices should be amended:

- The current Article 5(1)(d) and (2) to (4) on real-time remote biometric identification should be removed from Article 5 and transferred to a new Title IIa on 'restricted AI practices';
- The list of prohibited AI practices in Article 5(1) should be enriched, at least, by a prohibition of total or comprehensive surveillance of natural persons in their private or work life and of infringements of mental privacy and integrity (further extensions being beyond the scope of this Study);
- The Commission should have the possibility to adapt the list of prohibited AI practices periodically, potentially under the supervision of the European Parliament;
- There should be a clarification that prohibitions following from other laws (such as data protection or consumer protection law) remain unaffected.

A new Title IIa on 'restricted AI applications' should be inserted:

- The new Title IIa should deal with 'real-time' remote biometric identification (or even with other forms of real-time remote identification) in a more comprehensive way, without limitation to law enforcement purposes;
- It should also include a provision on other biometric identification systems, emotion recognition systems and biometric categorisation systems, limiting the admissibility of such systems and integrating the transparency obligation which is currently in Article 52(2);
- Title IIa should likewise include a new provision on decisions based on biometric techniques;
- Title IIa might possibly also include provisions that put substantive limits to the drawing of biometric inferences and provide for automated consent management.

Annex III point 1 should be extended so as to cover emotion recognition systems in (at least) the same way as biometric categorisation systems.

1. CURRENT AND POTENTIAL FUTURE DEVELOPMENTS OF BIOMETRIC TECHNIQUES

KEY FINDINGS

'Biometric techniques' should be understood as including any technology or operation that

- relies on specific technical processing of data relating to physical, physiological or behavioural aspects of the human body (including when in motion);
- for purposes of
  - authentication/identification of human individuals;
  - categorisation of human individuals according to permanent or long-term characteristics (including with a view to predicting future behaviour); or
  - detection of temporary or permanent conditions of a human individual (such as fear, fatigue, or illness).

Biometric techniques clearly include, e.g., analysis of keystroke or mouse dynamics, gesture dynamics, signature dynamics, as well as voice and gait features. However, the term is normally not understood as including behaviour that can be controlled by the human will to a higher extent, such as shopping behaviour, browsing history or the content of communication. As far as such behaviour is analysed to infer conditions of a genetic, physical, physiological, behavioural, psychological or emotional nature it may, however, be justified to include them in this Study.

Major trends are the increasing use of 'weak' and 'soft' biometrics alongside 'strong' biometrics, focussing on a variety of patterns of a more behavioural kind, and the development towards multimodal biometrics. Together with enhanced sensor and computing capabilities as well as enhanced connectivity, this paves the way for mass roll-out of biometric technologies in a broad variety of sectors and for a broad variety of purposes, far beyond law enforcement and border control, turning biometric technologies into something like universal technologies.

Latest technological advances include improved sensors, enabling the capture of entirely new types of bio-signals, such as heart beats and brain waves via EEG or ECG, and the development of brain-computing-interfaces (BCI). BCIs measure neuro activity and translate brain activity into machine-readable input. These new technologies are potentially highly intrusive, allowing for the detection of thoughts or intent and possibly also for influencing operations of the human brain.

1.1. Biometric technologies

1.1.1 Strong, weak and soft biometrics

The last two decades have seen a rapid development of biometric technologies. The term 'biometric' consists of the two components 'bio' and 'metric', implying the measurement of biological data. According to the Oxford English Dictionary, 'biometrics' is defined as 'designating or relating to

physical characteristics that are unique identifiers of individuals (fingerprints, iris pattern, etc.)'.[1] Broadly speaking, biometrics is about the measurement of biological signals.[2]

Biometrics may be divided in various ways, one of them being 'strong', 'weak', and 'soft' identifiers. Strong identifiers allow or confirm the unique identification of a natural person, e.g. fingerprints, iris, and retina. Weak biometrics are features that are 'less unique' or 'less stable', e.g. body shape, behavioural patterns, voice, and body sounds. Soft biometrics comprise features that are generic in nature and not uniquely associated with a person, e.g. gender or age.[3]

Modern biometric technologies enable the analogue-to-digital conversion and automated processing of biometric identifiers, which makes these biometric technologies radically different from any analogue, human performed biometrics. Human agents are no longer required to capture, process and compare biometric identifiers, enabling purely automated identification. The development of advanced scanners for biometric identifiers has allowed an extremely diverse and fast-developing field of biometric techniques to emerge. A common division is that into first generation and second generation biometric technologies.[4]

1.1.2 First and second generation biometric technologies

First generation biometric technologies were focussed on strong biometrics and the unique identification or authentication of particular individuals. First large-scale use cases started in the late 1990s in the USA[5], with an enhanced spread after the 2001 terror attacks and the introduction of biometric passports, containing fingerprint and facial data. Since then, first generation biometric technologies have become more robust and advanced, substantially reducing error rates with the help of improved computer technology (especially in facial recognition technologies). First generation biometrics have since developed into a tool for quick and reliable identification or authentication in a broad variety of contexts, including for law enforcement purposes,[6] electoral voting[7] and even for social scoring systems.[8] Applications like facial recognition and fingerprint technologies have also reached the private sector, including for the unlocking of smartphones or the recognition of VIP customers. These techniques are replacing traditional passwords as a security measure, with newest facial recognition technology enabling the identification in less than one second.[9]

---

[1] 'Biometrics' in: Oxford English Dictionary (OED) *Online Edition* (March 2021), <https://www-oedcom.uaccess.univie.ac.at/view/Entry/273387?rskey=6KnFtL&result=2&isAdvanced=false#eid> (last accessed 12 July 2021).

[2] Angelos Yannopoulos, Vassiliki Andronikou, and Theodora Varvarigou 'Behavioural Biometric Profiling and Ambient Intelligence' Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen* (Springer 2008), 89.

[3] Emilio Mordini, Dimitrios Tzovaras, and Holly Ashton in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 7.

[4] Emilio Mordini, Dimitrios Tzovaras, and Holly Ashton in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 7.

[5] Philip Brey, '*Ethical* Aspects of Facial Recognition Systems in Public Places' (2004) 2 Comm & Ethics in Society 97.

[6] See Gloria González Fuster, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights' (European Parliament 2020), 24; European Parliamentary Research Service, 'The Fight Against Terrorism: The Cost of Non-Europe' (2018), 38.

[7] Peter Wolf, 'Introducing Biometric Technology in Elections' (International Institute for Democracy and Electoral Assistance 2017).

[8] Xiao Qiang, 'President XI's Surveillance State' (2019) 30 Journal of Democracy 53.

[9] Soodamani Ramalingam, Aruna Shenoy, and Nguyen Trong Viet, 'Fundamentals and Advances in 3D Face Recognition' in Mohammad S. Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems* (Springer 2019).

Rather than focusing on 'strong' biometric identifiers, such as fingerprint, iris or retina, second generation biometric technologies focus on 'weak' biometrics, ranging from motor skills to body signals, gait, and machine usage and interaction.[10] Second generation biometrics are also commonly referred to as 'behavioural biometrics', as the digital physical and cognitive behaviour of humans is analysed rather than static characteristics, such as fingerprints.[11] The distinction between first- and second-generation technologies can be blurred, however, in particular as behavioural and emotion recognition systems heavily rely on facial recognition technology.

Examples of private sector use of second-generation biometrics are targeted marketing,[12] detecting fatigue or drowsiness during driving,[13] and medical diagnostics.[14] Additionally, second-generation biometrics offer new opportunities to law enforcement and border control authorities, allowing, for example, to detect persons with suspicious behaviour that could indicate intentions to commit a crime (see a).[15]

To increase accuracy, first generation biometric technologies are regularly combined in multimodal systems. These systems combine several biometric identifiers for the identification of one and the same person. Multimodal systems can minimise dangers of fraud and help overcome difficulties caused by poor data quality or missing data[16] but also increase ethical concerns, as they enable more efficient public surveillance and can be used for the creation of elaborate profiles (see 0). Technological advances have also prompted apprehensions of a mass surveillance state and led to calls from citizens to strictly regulate the use of biometric techniques and AI in public spaces. These concerns have also been raised by petitions submitted to the European Parliament.[17]

Since brain activities are measurable biological signals, they are also considered to be biometrics. Due to the difficulties of capturing the electrochemically signals of the brain and their complexity, the relevance of brain activities was, for a long time, limited to the medical sector. However, in recent years, electroencephalography (EEG), which records the electrical activates of the brain by placing electrodes onto the scalp, and so-called brain-computer interfaces (BCI), which can translate brain activity into

[10] Emilio Mordini, Dimitrios Tzovaras, and Holly Ashton in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 9.

[11] Ayelet Biger-Levin, 'What Is Behavioral Biometrics?' (Big Catch Blog) available at <https://www.biocatch.com/blog/what-is-behavioral-biometrics> (last accessed 09 July 2021).

[12] Michael Fitzpatrick, 'Advertising Billboards Use Facial Recognition to Target Shoppers' (*GUARDIAN,* 2010) available at <http://www.theguardian.com/ media/pda/2010/sep/27/advertising-billboards-facial-recognition-japan> (last accessed 15 July 2015).

[13] Eric Taub, 'Sleepy Behind the Wheel? Some Cars Can Tell' (*NY Times*, 2017) available at https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html (last accessed 15 July 2021).

[14] Emilio Mordini and Holly Ashton 'The Transparent Body: Medical Information, Physical Privacy and Respect for Body Integrity' Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012),

[15] Gloria González Fuster, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights' (European Parliament 2020), 24.

[16] Perumal Viswanatham and others, 'Multimodal Biometric Invariant Fusion Techniques' in Mohammad S. Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems* (Springer 2019), 321.

[17] See Petition No 0221/2018 by B.O. (German) on limiting government video surveillance and the use of facial recognition technologies; Petition No 1287/2019 by Rui Martins (Portuguese) on the use of artificial intelligence for facial recognition technology.

machine-readable input (see c), have become more affordable[18] and have even been integrated in consumer products.[19]

1.1.3 Future trends and technologies

The technological advancements of recent years in particular in data analytics and AI but also in terms of hardware (fast processing computers, high resolution cameras and IoT) have elevated the potential of biometric techniques and expanded their field of application. On the one hand, the private sector has developed an increased interest in the large-scale use of advanced biometric applications that had previously only been used by law enforcement. For example, a Spanish supermarket chain has implemented a facial recognition system to detect people with restraining orders and to prevent them from entering the shop. The supermarket's CCTV collects facial images of customers entering a shop, and the software creates biometric templates, which are then compared with the templates of persons that are not allowed to enter the premises.[20] Another example is facial recognition that is used to record the working hours of employees at construction sites.[21] In addition, biometric authentication technologies are to an increasing extent included in IoT devices and digital services, replacing the traditional use of passwords or similar credentials (see 3.2.b). Similar to the evolution of fingerprint technology in smartphones, new biometric techniques could lead to a diversification of options of mobile authentication. In this context, improvements with regard to matching accuracy and reliable protection against spoofing will be key for the enhanced mass-rollout of biometric technologies.[22] Possible short-term use cases include seamless payment applications, biometric authentication for daily services and continued authentication.[23] One example being the automotive industry, which is looking at iris scans as a tool to detect driver fatigue, as well as further authentication for self-driving cars and increased personalisation.[24]

On the other hand, the public sector is increasingly relying on biometric techniques in various fields such as law enforcement and border security, health care or even for warfare. The overarching global trends of hyper-individualisation, enhanced security concerns and seamlessness of digital services continue to be strong drivers for further advancing biometric technologies.[25] While the promise is that future developments will increase the usability, accuracy and robustness of existing biometric technologies, the technical capabilities have also given rise concerning trends and applications. For instance, AI systems coupled with biometric techniques have led to a re-emergence of lie detection and other predictive systems that analyse human behaviour in order to draw conclusions about their

---

[18] Florian Gondesen, Matthias Marx, and Dieter Gollmann, 'EEG-Based Biometrics' in Mohammad S. Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems* (Springer 2019), 287.

[19] See e.g. https://www.unicorn-bi.com/brain-interface-technology/.

[20] Isabel Rubio, 'Protección de Datos abre una investigación sobre las cámaras de vigilancia facial de Mercadona' (El Pais, 2020) available at <https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html> (last accessed 20 June 2021).

[21] Chris Burt, 'Touchbyte Safe Workplace System with Face Biometrics Piloted at UK Construction Site' (*Biometric Update,* 2020) available at <https://www.biometricupdate.com/202009/touchbyte-safe-workplace-system-with-face-biometrics-piloted-at-uk-construction-site> accessed 21 July 2021.

[22] Hitoshi Imaoka and others, 'The Future of Biometrics Technology: From Face Recognition to related Applications' (2021) 10 APSIPA Transactions on Signal and Information Processing, 8.

[23] Nick Sohnemann and others, New Developments in Digital Services, Short-(2021), Medium-(2025) and Long-Term (2030) Perspectives and the Implications for the Digital Services Act (European Parliament 2020),15f.

[24] Edin Ćatović and Saša Adamović, 'Application of Biometrics in Automotive Industry - Case Study Based on Iris Recognition' (International Scientific Conference on Information Technologies and Data related Research – Sinteza 2017).

[25] Nick Sohnemann and others, New Developments in Digital Services, Short-(2021), Medium-(2025) and Long-Term (2030) Perspectives and the Implications for the Digital Services Act (European Parliament 2020).

emotions and state of mind. AI systems are fed with labelled biometric data, such as facial expression, heart rate and body temperature, to identify correlations between measurable micro expressions of humans and their emotions.[26] The uptake of biometric techniques will undoubtedly increase the likelihood of individuals coming in touch with this technology, which renders a wider discussion on the ethical concerns all the more important. The following Subchapters shall give an overview of trends and developments in the field of biometric techniques that have caused broader public concerns.

a. 'Smart' borders

Increasing their border security by using modern technologies, such as AI and biometric techniques, has been a fixed item on the political agenda of the EU and its Member States. In 2017, the EU adopted a Regulation to establish an 'Entry/Exit System' (EES),[27] which records and stores date, time, place of entry and exit as well as biometric data of third-country nationals (see 2.1.e). Under the obligations of the Regulation Member States have to implement systems that can quickly register and verify the identity of external visitors by collecting and processing fingerprints and facial biometrics. The Regulation enters into force in 2022, and consequently, Member States are deploying new systems at their ports of entry, such as high-resolution cameras that can identify travellers via face recognition and then generate a profile of that person (on the data protection concerns regarding the EES scheme see 2.1.e).[28]

However, 'smart' borders may not only encompass the use of biometric technologies for identification purposes but can also include emotion detection systems. These automated deception detection tools analyse second generation biometrics that are associated with stress, anxiety and lying to support border control officers. Although no emotion detection systems are currently in operation at EU borders, the 'Intelligent Portable Control System' (iBorderCtrl) project, which was aimed at the development of deception detection tools and risk based assessment tools for border security purposes, has received significant research funding under the Horizon 2020 scheme.[29] By analysing micro-expressions, such as eye blink, increase in face redness or head movement directions, the iBorderCtrl systems aims to identify persons that have lied about their identity, luggage, destination or other travel plans and classifies persons into 'bona fide' and 'non-bona fide' travellers. If a person falls into the latter category, an interview and further investigations are conducted by a human border officer.[30]

While iBorderCtrl is the latest project to explore the use of biometric emotion recognition for border security, there have been other notable attempts. Already in 2011, the UK Border Agency planed the trial use of a facial and thermal analysis tool to detect lies during immigration procedures. However,

---

[26] See Javier Sánchez-Monedero and Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' [2020] Information, Communication & Society 1.

[27] 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, 20-82.

[28] 'Thales Secures France's Borders' (2021) 4 Biometric Technology Today 2.

[29] EPRS, 'Artificial Intelligence at EU Borders: Overview of Applications and Key Issues' (2021), 17.

[30] Javier Sánchez-Monedero and Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' [2020] Information, Communication & Society 1, 8.

the UK Home Office only recently stated that it is not considering the use of lie detectors.[31] In the US, the National Center for Border Security and Immigration (BORDERS), a United States Department of Homeland Security Center of Excellence has developed an Automated Virtual Agent for Truth Assessment in Real-time (AVATAR). This system conducts fully automated interviews at the border during which it analyses a travellers nonverbal and verbal behaviour, such as eye movement, gestures and pitch. The AVATAR then rates the person's credibility and sends the result to border control officer. In collaboration with EU's border agency FRONTEX, the system was also tested at the airport in Bucharest.[32]

The use of these biometric deception detection systems is highly contested, as they are not based on sound science but rather on a chain of assumptions about the relationship between biometric indicators and internal intentions.[33] There are several studies that have pointed out the flaws of these assumptions and that automated deception detection tools do not yield more accurate results than mere guessing.[34] One of the fundamental issues of these systems is that emotions are complex human phenomena that cannot be clearly assigned to a set of nonverbal and verbal indicators.[35] Given the problematic nature of these systems, it is not surprising that the in particular the funding of the iBorderCtrl project has caused a major public outcry.[36] In a European Citizens' Initiative, the European Commission has been urged to ceases funding for the research/development of biometric mass surveillance technologies.[37]

b. Health care

In the health care sector, biometric techniques are increasingly used to reliably identify patients. The intention is to reduce registration times and reduce social security fraud.[38] Furthermore, it allows the identification and retrieval of medical records of unconscious or unresponsive emergency patients.[39]

---

[31] Danny Shaw, 'Asylum Applications: Home Office Urged to Use Lie Detectors' (*BBC News*, 2019) available at <https://www.bbc.com/news/uk-46830373> (last accessed 21 July 2021).

[32] Aaron Elkins and others, 'Appraising the AVATAR for Automated Border Control' (2014) available at <https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/002653/P9_RE(2019)002653(ANN3)_XL.pdf> (last accessed 20 July 2021).

[33] Javier Sánchez-Monedero and Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' [2020] Information, Communication & Society 1, 8.

[34] See Charles Bond and Bella DePaulo, 'Accuracy of Deception Judgments' (2006) 10 Personality and Social Psychology Review 214; Aldert Vrij and Pär Anders Granhag, 'Eliciting Cues to Deception and Truth: What Matters Are the Questions Asked' (2012) 1 Journal of Applied Research in Memory and Cognition 110; Javier Sánchez-Monedero and Lina Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' [2020] Information, Communication & Society 1.

[35] See Lisa Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements' (2019) 20 Psychological Science in the Public Interest 1.

[36] See e.g.Condé Nast, 'The Science behind the EU's Creepy New Border Tech Is Totally Flawed' (*Wired UK,* 2018) available at <https://www.wired.co.uk/article/border-control-technology-biometrics> (last accessed 21 July) 2021; Lucien Begault, 'Automated Technologies and the Future of Fortress Europe' (*Amnesty International*, 2019) available at <https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/> (last accessed 21 July 2021).

[37] See 'Civil Society Initiative for a Ban on Biometric Mass Surveillance Practices' ECI(2021)000001.

[38] Erika Gimbel, 'How Biometric Technologies Improve Healthcare Operations' (*Technology Solutions That Drive Healthcare*, 2019) available at <https://healthtechmagazine.net/article/2019/12/how-biometric-technologies-improve-healthcare-operations> (last accessed 22 July 2021); Jim Nash, 'EU Research Group Talks up Access Control, Biometrics in Healthcare (*Biometric Update*, 2020) available at <https://www.biometricupdate.com/202009/eu-research-group-talks-up-access-control-biometrics-in-healthcare> (last accessed 22 July 2021).

[39] Janelle Mason and others, 'An Investigation of Biometric Authentication in the Healthcare Environment' (2020) 8 Array 100042.

There are also more ambitious approaches, such as linking biometric authentication to drug prescriptions for specific contagious diseases in order to monitor epidemiological developments in real time.[40]

Biometrics, usually in combination with AI systems, also play a role in modern diagnostic tools and techniques. For instance, in the UK, an AI tool was developed that can identify signs of eye disease by scanning the patient's retina.[41] Research has also been conducted on AI aided diagnostic tools that analyse images of human skin and identify potential cases of cancer.[42] However, biometric techniques and AI are also used for more controversial medical purposes. In a recent US experiment, social media photos were analysed, using algorithmic facial recognition, metadata components and colour analysis to identify predictive markers of depression.[43]

c. Brain-computer interfaces (BCI)

Brain-computer interfaces describe a communication pathway between the brain and an external device or system (see 0). So-called output BCI detect brain activity and issue corresponding commands to a non-biological artificial component. In the medical sector, this technology can be used to enable patients, who have lost motor functions, to control prosthetic devices or a wheelchair. In this setting, BCI function as an information-processing surrogate for damaged parts of a patient's nervous system. Input BCI send signals to the brain that influence brain activity and are used in the rehabilitation of neurological disorders.[44] For example, so-called Deep Brain Stimulation implants can help treating the symptoms of Parkinson's disease.[45]

While input BCI play an increasingly important role in the treatment of neurological diseases, they have also raised delicate questions in the field of bioethics, as BCI can affect the memory of humans and their psychological features. The technology could potentially be (ab)used for mind reading, mind control or the suppression of (un)desired impulses, which would pose a severe threat to privacy, human dignity, personal autonomy and identity.[46]

In Europe, the European Group on Ethics in Science and Technology (EGE) issued already in 2005 an opinion on the use of ICT implants (including BCI). The EGE stated that BCI for medical purposes are not as such a risk for the fundamental rights of individuals, as long as such implants are necessary to achieve the objectives of saving lives, restoring health or improving the quality of life and are based on informed consent.[47] However, the EGE views non-medical applications of ICT implants as a potential threat to human dignity and democratic society. In particular, the use of ICT implants, such as BCI, to

[40] Aditya Arya and others, 'Integration of Biometric ID for the Effective Collection and Epidemiological Evaluation of Antibiotic Prescription in Tuberculosis and Other Diseases: A Medical Hypothesis' (2020) 21 Journal of Global Antimicrobial Resistance 439.

[41] Jeffrey De Fauw and others, 'Clinically Applicable Deep Learning for Diagnosis and Referral in Retinal Disease' (2018) 24 Nature Medicine 1342.

[42] Manu Goyal and others, 'Artificial Intelligence-Based Image Classification Methods for Diagnosis of Skin Cancer: Challenges and Opportunities' (2020) 127 Computers in Biology and Medicine 104065.

[43] Andrew Reece and Christopher Danforth, 'Instagram Photos Reveal Predictive Markers of Depression' (2017) 6 EPJ Data Science 15.

[44] Federica Lucivero and Guglielmo Tamburrini, 'Ethical Monitoring of Brain-Machine Interfaces: A Note on Personal Identity and Autonomy' (2008) 22 AI & Society 449, 451.

[45] See 'Deep Brain Stimulation (DBS)' (*Parkinson's Foundation*) available at <https://www.parkinson.org/Understanding-Parkinsons/Treatment/Surgical-Treatment-Options/Deep-Brain-Stimulation> (last accessed 23 July 2021).

[46] Pim Haselager and others, 'A Note on Ethical Aspects of BCI' (2009) 22 Brain-Machine Interface 1352, 1352.

[47] European Group on Ethics in Science and Technology (EGE) 'Opinion on the Ethical Aspects of ICT Implants in the Human Body' (European Commission 2005), 30.

alter or influence mental functions or personal identity is considered a violation of the right to respect for human dignity.[48]

d. EdTech

Technological advancements also have led to the emergence of adaptive learning systems. This AI-driven educational technology (EdTech) can respond to a learner's interactions in real time and automatically tailors support to their individual needs and is increasingly used in the Chinese school system. It has to be pointed out, however, that a vast part of what is considered EdTech does not rely on any biometric techniques but rather on big data analysis and machine learning. For example, AI system are used to propose learning activities that match the learner's cognitive abilities or to give targeted real time feedback, all without the need of human teacher.[49] These systems rely on the analysis of data regarding the student's learning performance, which are collected using IoT devices.[50] However, there have also been reports concerning the use of facial recognition software in Chinese Schools that monitors the students' behaviour and gives the teachers feedback on the students' concentration levels.[51] Already the collection and analysis of learning activities constitutes a severe intrusion into the privacy of children, as the collected data can provide a comprehensive picture about the development of children, their mental state, preferences and weaknesses.[52] The additional use biometric techniques intensifies the encroachments of the children's fundamental rights.[53] Reportedly, even the Chinese Ministry of Education has announced to 'curb and regulate' the use of facial recognition in schools.[54]

e. Autonomous weapon systems

The use of AI for military purposes has given rise to ethical, legal and policy discussion on its own.[55] The risks of automated decision making and a missing human in loop become particularly apparent in this context, as consequences will often be immediate, severe and irreversible. While biometric techniques play a subordinate role in autonomous weaponry, their use gained public attention when a UN report emerged documenting the use of automated drones in Libya that were programmed to attack even if connection to the operator was lost.[56] This suggests that the drones were equipped with some sort of

---

[48] European Group on Ethics in Science and Technology (EGE) 'Opinion on the Ethical Aspects of ICT Implants in the Human Body'(European Commission 2005), 32

[49] Ben Williamson and Rebecca Eynon, 'Historical Threads, Missing Links, and Future Directions in AI in Education' (2020) 45 Learning, Media and Technology 223.

[50] Yi-Ling Liu, 'The Future of the Classroom? China's Experience of AI in Education' The AI Powered State: China's Approach to Public Sector Innovation [2020] available at <https://www.nesta.org.uk/report/the-future-of-the-classroom/> (last accessed 21 July 2021), 28.

[51] Neil Connor, 'Chinese School Uses Facial Recognition to Monitor Student Attention in Class' (*The Telegraph*, 2018) available at <https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/> (last accessed 22 July 2021).

[52] Yi-Ling Liu, 'The Future of the Classroom? China's Experience of AI in Education' The AI Powered State: China's Approach to Public Sector Innovation [2020] available at <https://www.nesta.org.uk/report/the-future-of-the-classroom/> (last accessed 21 July 2021), 28

[53] See for a detailed analysis Andrew McStay, 'Emotional AI and EdTech: Serving the Public Good?' (2020) 45 Learning, Media and Technology 270.

[54] 'China to Curb Facial Recognition and Apps in Schools' (BBC News, 2019) available at <https://www.bbc.com/news/world-asia-49608459> (last accessed 22 July 2021).

[55] For extensive elaborations on these issues see Nehal Bhuta and others (eds), *Autonomous Weapons Systems* (Cambridge University Press 2016).

[56] 'Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011)', S/2021/229 available at < https://undocs.org/S/2021/229> (last accessed 25 July 2021), 17.

facial recognition software.[57] However, the UN Report does not unequivocally confirm the use of biometric techniques nor that the attack was indeed flown without human intervention. Irrespective of what had actually transpired in Libya, it is clear that autonomous decisions in modern warfare could be based on biometric techniques. The need for human control in AI used for military purposes has also recently been stressed by a Resolution of the European Parliament. The EP recommends that no authority shall certify AI-based systems intended for military purposes that are not subject to meaningful human control, so that at all times a human has the means to correct, halt or disable it in the event of unforeseen behaviour, accidental intervention, cyber-attacks or interference by third parties.[58]

1.2. Identification, categorisation, and detection

Biometric techniques can, in the light of their primary function, be divided into techniques of biometric authentication or identification, categorisation, and detection.

Biometric identification is a method of identifying or confirming a person's identity based on the individual's unique physical, physiological or behavioural characteristics.[59] In the narrower sense of the term, which is the term used in this Study, 'identification' is to be distinguished from 'authentication'. Authentication is a 'one-to-one' comparison, matching the live template of a particular person who claims to have a particular identity with the stored template in a template database that is connected with that identity in order to verify whether the claim is true. By contrast, identification in the narrower sense is defined as a 'one-to-many' comparison where the persons identified do not claim to have a particular identity but where that identity is otherwise established – often without the conscious cooperation of these persons or even against their will – by matching live templates with templates stored in a template database. Put simply, identification answers the question 'Who is this person?', while authentication answers the question 'Is this the person himself declared?'.[60]

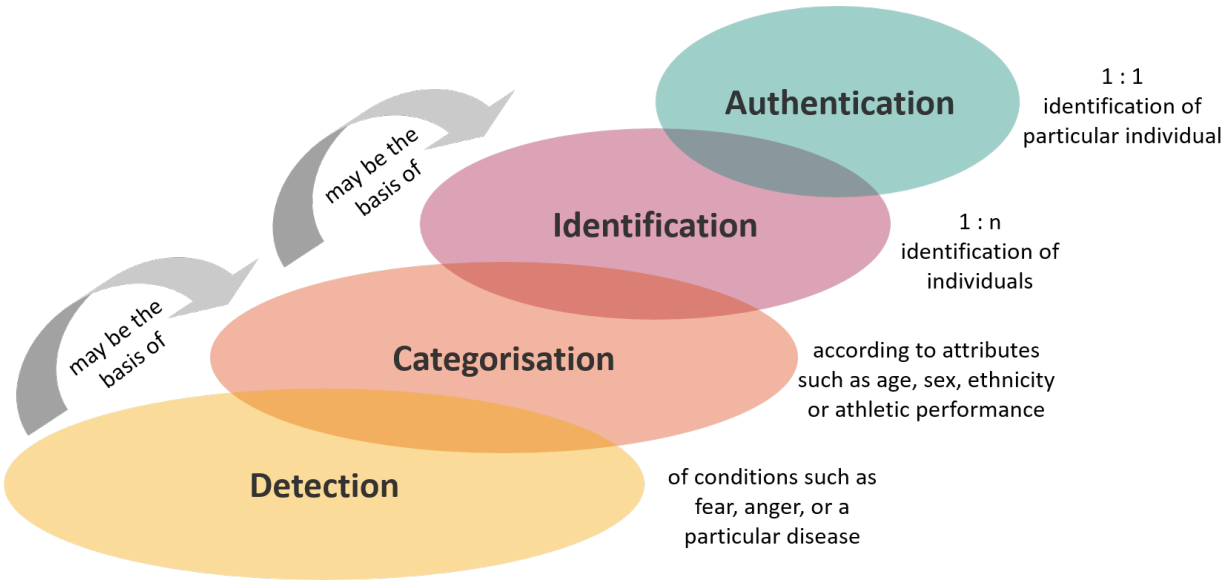
[57] Jim Nash, 'Like a Nightmare Come True: Killer Robots Fighting Humanity's Wars' (*Biometric Update*, 2021) available at <https://www.biometricupdate.com/202106/like-a-nightmare-come-true-killer-robots-fighting-humanitys-wars> (last accessed 25 July 2021).

[58] Recommendations 3 and 7 European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

[59] Association for Biometrics (AfB) and International Computer Security Association (ICSA), '1998 Glossary of Biometric Terms' (1998) 3 Information Security Technical Report, 98-108.

[60] Emilio Mordini and Carlo Petrini, 'Ethical and Social Implications of Biometric Identification Technology' (2007) 43 Annali Dell'istituto Superiore di Sanita, 5.

Figure 1: Authentication/identification, categorisation, and detection



Source: Christiane Wendehorst

Biometric categorisation is a term that is less common than biometric identification, also because the rise of biometric categorisation techniques has only come with the increasing use of 'soft' or 'weak' biometrics. Data that are as such not (or not necessarily) suited for the unique identification of a natural person may nevertheless be suited for assigning natural persons to specific categories, such as sex, age, ethnic origin or health. Needless to say, where a particular natural person is assigned to several different categories, the cumulative assignment may, depending on circumstances such as number and granularity of categories, allow or confirm the identification of that natural person.

Last but not least, the term 'biometric detection' may be used for a number of biometric techniques whose purpose it is to detect certain human conditions, such as anger, fear, a particular intention (e.g. to commit a crime) or a particular disease. Recently, emotion recognition systems, i.e. systems for the purpose of identifying or inferring emotions, thoughts or intentions of natural persons on the basis of bio-signals, have become particularly important, as they raise a number of very specific ethical issues.

With the increasing use of 'soft' or 'weak' biometrics and an ever broader range of bio-signals and behavioural traits that may be sensed and analysed with the help of machines it has become more and more difficult to draw a clear line between biometric techniques and other forms of, e.g., profiling of natural persons. Generally speaking, the term 'biometric' always implies a certain degree of immutability, i.e. that the natural person concerned has little to no chance of changing the characteristics or signals analysed, such as a person cannot, at their discretion, change their face or dactyloscopic pattern. Biometric techniques therefore clearly include, e.g., analysis of keystroke or mouse dynamics, gesture dynamics, signature dynamics, as well as voice and gait features. However, the term is normally not understood as including behaviour that can be controlled by the human will to a higher extent, such as shopping behaviour, browsing history or the content of communication.

1.3. Scope of this Study

The existing conceptual patchwork of 'biometric identification', 'biometric categorisation', 'behavioural detection', 'emotion recognition', processing of 'biometric data', 'biometric profiling' etc. calls for a clear delineation of the boundaries of this Study. This Study analyses 'biometric techniques', which should be understood as including any technology or operation that relies on specific technical processing of data relating to physical, physiological or behavioural aspects of the human body and

that measures or infers conditions characterising a particular human individual, including conditions of a genetic, physical, physiological, behavioural, psychological or emotional nature.

The Study groups techniques into authentication, identification, categorisation and detection techniques, but will not look separately at authentication, as this is a very traditional area, which is less problematic from an ethical point of view. While the Study will normally not be addressing techniques that rely on personal data other than of a biometric nature, such as shopping behaviour, browsing history or the content of communication, it will be considering the use of such data as far as conditions inferred are of a genetic, physical, physiological, behavioural, psychological or emotional nature.

2. OVERVIEW OF LEGISLATION AND CASE LAW

2.1. Legislation

Legal norms that regulate the use of biometric techniques can be found on an international, EU and national level. In particular, fundamental rights and data protection law set limits for the use of biometric techniques. Legislation on border security on the other hand, contains explicit authorisations for using biometric technology in specific situations. The following Chapter shall give an overview over relevant legal frameworks regarding biometric techniques. Particularly with regard to the legislation on a national level, only a handful of noteworthy examples from certain Member States and third countries can be provided.

2.1.1 International law

a. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)

Biometric techniques are often assessed in light of the fundamental rights afforded by the European Convention on Human Rights (ECHR) (see 0). Particularly in situations where the Charter of Fundamental Rights of the European Union[61] (CFR) is not applicable because they are not covered by EU Law (see a), the rights under the ECHR are invoked. The ECHR was drafted by the Council of Europe in 1950 and entered into force in 1953. All 47 Council of Europe member state, including the 27 EU Member States as well as the United Kingdom, Russia and Turkey, are parties to the ECHR. Although the Treaty of Lisbon provided for a duty of the EU to accede to the ECHR, the EU itself has not become a party to the Convention. The CJEU found the accession agreement to be in violation of Article 6(2) TEU because it did not provide for sufficient protection of the CJEU's exclusive jurisdiction.[62] Currently, the EU and the Council of Europe are in negations for a new accessions agreement.[63]

The ECHR consists of three sections, with section three containing miscellaneous provisions. In section one, the Convention enshrines 16 basic human rights and freedoms. With regard to biometric techniques, the right to life guaranteed under Article 2, providing that 'everyone's right to life shall be protected by law', the right to a fair trial (Article 6), no punishment without law (Article 7), and the right to respect for private and family life in Article 8, which also includes the right to privacy,[64] are especially noteworthy. The use biometric techniques for surveillance purposes (see 0) may additionally be in conflict with the freedom of expression (Article 10), which includes the freedom to hold opinions, as well as with the freedom to assembly and association (Article 11). The prohibition of discrimination set forth in Article 14 ECHR only has accessory nature, meaning that it can only be invoked together with a substantive right of the Convention.[65] A general prohibition of discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with

---

[61] Charter of Fundamental Rights of the European Union [2012] OJ C326/2.

[62] Opinion 2/13 of the Court (Full Court) of 18 December 2014.

[63] See Legislative Train Schedule, 'Completion of EU Accession to the European Convention on Human Rights', available at <https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-completion-of-eu-accession-to-the-echr> (last accessed 09 July 2021).

[64] See e.g. *Von Hannover v. Germany* (no. 2) App no 40660/08 and 60641/08 (ECtHR 7 December 2012), para 95.

[65] See Jenneke Gerards 'Prohibition of Discrimination' in Pieter van Dijk and others (eds), *Theory and Practice of the European Convention on Human Rights* (5th edn, Intersentia 2018), 998.

a national minority, property, birth or other status is contained in Article 1 of Protocol No. 12. However, only 20 States have ratified Protocol 12.[66]

None of these rights, however, are absolute and may therefore be subject to restrictions if provided for by law and the grounds set forth by the respective Article are met. For example, an interference with Article 8–11is lawful if in accordance with the law (the 'rule of law test') and necessary in a democratic society (the 'democratic necessity test').[67] According to settled case law, the democratic necessity test requires not only a pressing social need but also that the interference is proportionate to the legitimate aim pursued.[68]

To ensure an effective protection of the enshrined rights and freedoms, section two establishes the European Court of Human Rights (ECtHR). Any individual or state may apply to the Court if they see Convention rights violated by a state party but only if they have exhausted all domestic remedies[69]. ECtHR judgments are binding for all parties to the Convention and must be implemented in national law.

b. United Nations (UN)

The proclamation of the Universal Declaration of Human Rights (UDHR)[70] by the United Nations General Assembly in 1948 represents a milestone in the history of human rights. While the UDHR is not binding, it has influenced and inspired modern human rights treaties on the Member States of the UN. The proclaimed rights include the right to life, liberty and security in Article 3, the presumption of innocence in Article 11 and the right to privacy in Article 12. The freedoms of thought, opinion and expression, and peaceful assembly and association are laid down in Articles 18 to 20 respectfully.

The Security Council of the United Nations has issued several Resolutions concerning the collection and sharing of biometric data for the purpose of counterterrorism. The Security Council Resolution 2160 (2014) encourages Member States to submit photographs and other biometric data of individuals supporting the Taliban to INTERPOL.[71] Resolution 2322 (2016) broadened the recommendation for biometrics-related data sharing to terrorists and terrorist organisations in general.[72] Other than in Resolution 2160, the Security Council included a recommendation that such data sharing should occur in compliance with both domestic and international law. Resolution 2396 (2017) went even further and imposed a binding obligation to develop biometric capabilities in compliance with domestic law and international human rights law, but kept calls for sharing such data at the level of a non-binding recommendation.[73]

---

[66] For the full list of signatures and ratifications see the Website of the Council of Europe's Treaty Office available at <https://www.coe.int/en/web/conventions/cets-number-/-abridged-title-known?module=signatures-by-treaty&treatynum=177> (last accessed 21 July 2021).

[67] See Steven Greer, The Exceptions to Articles 8 to 11 of the European Convention on Human Rights (Council of Europe Publishing 1998).

[68] See *Dudgeon v. the United Kingdom* App no 7525/76 (ECtHR 23 September 1981), paras 51-53.

[69] ECHR Arts 33, 34 and 35.

[70] General Assembly, *Universal Declaration of Human Rights*, 217 A (III) (United Nations 1948).

[71] Security Council, *Security Council Resolution 2160*, S/RES/2160 (United Nations 2014), para. 18.

[72] Security Council, *Security Council resolution 2322*, S/RES/2322 (United Nations 2016), para 3.

[73] Security Council, *Security Council Resolution 2396*, S/RES/2396 (United Nations 2017), para 15.

2.1.2 EU law

a. Charter of Fundamental Rights of the European Union (CFR)

The CFR enshrines political, social, and economic rights for EU citizens and protects human dignity, freedom and equality. If EU law is applied by institutions or Member States, the rights established in the Charter of Fundamental Rights need to be strictly adhered to.[74] To a large extent the fundamental rights afforded under the CFR correspond to those of the ECHR (see 0.) Where they do, Article 52(3) CFR explicitly states that the meaning and scope of the rights guaranteed by the Charter shall be the same as those under ECHR. The Charter's provisions, however, are addressed to the Member States only when they are implementing EU law.[75] This means the fundamental rights guaranteed in the legal order of the European Union are applicable in all situations governed by EU law, but not outside such situations.[76] If EU law does not apply, fundamental rights can only be guaranteed by other legal acts, such as the ECHR or Member States' constitutions.

In the context of existing EU legislation regulating biometric techniques, the rights to respect for private life[77] and protection of personal data[78] are particularly notable, as they have been invoked in several cases before the CJEU regarding the collection of first generation biometrics for passports (see 0). A significant role in the ethical discussions concerning the use of biometric techniques is played by Article 1, which states that 'human dignity is inviolable' and 'must be respected and protected'. Human dignity is also mentioned in Article 2 of the Treaty on European Union (TEU) together with freedom, democracy, equality, the rule of law and respect for human rights as a value on which the EU is founded. At its core, human dignity is understood as prohibiting the instrumentalisation or objectification of human beings (see 0). However, the concept of dignity is extremely broad, which on the one hand gives it a very wide and flexible field of application but on the other hand makes it difficult to grasp its exact legal nature. [79] The Charter also prohibits 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 (Article 21). Unlike Article 14 ECHR, the prohibition of discrimination under Article 21 CFR is not linked to other fundamental rights of the Charter.

According to Article 52(1) CFR, any limitation on the exercise of the rights guaranteed by CFR must be provided for by law, proportionate and meet objectives of general interest or the need to protect the rights and freedom of others. Regarding human dignity, which is considered the foundation of all other fundamental rights, it is disputed whether it falls outside the scope of Article 52(1). It is argued that human dignity is inviolable and therefore absolute. The opposing argument is that 52(1) does not differentiate between human dignity and the other fundamental rights of the CFR. The mediating view is that the essence of human dignity as well as its foundational value are absolute. Where human

[74] Art 51 CFR.

[75] Art 51 CFR.

[76] Case C-418/11 *Texdata Software GmbH* (CJEU 26 September 2013), para 71.

[77] Art 7 CFR.

[78] Art 8 CFR.

[79] Catharine Dupré in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Nomos 2014), Art 1 01.32.

dignity functions as human right, it is relative and interference may be justified if the requirements of Article 52(1) are met.[80]

b. General Data Protection Regulation

With the General Data Protection Regulation (GDPR)[81], the European legislator not only introduced a definition of 'biometric data' but also imposed stricter requirements for the processing of biometric data than for other personal data. According to the GDPR, biometric data *'means 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'*.[82] The Recitals clarify that the photographs should only fall under the definition of biometric data '*when processed through specific technical means allowing the unique identification or authentication of a natural person.*'

Like other personal data, biometric data may only be processed if one of the grounds of Article 6(1) GDPR is met. The processing is, *inter alia*, justified if the data subject has given consent, or if the processing is necessary for compliance with a legal obligation to the processing. As the processing of biometric data could create significant risks to the fundamental rights of data subjects, Article 9(1) GDPR generally prohibits the processing of biometric and other sensitive data for identification purposes. This general rule is subject to exceptions exhaustively listed in Article 9(2) GDPR.[83] While most of these exceptions are similar but slightly stricter than the legal grounds listed in Article 6(1), Article 9(2) also provides for exceptions that go beyond the general grounds for lawful processing. This, however, does not mean that biometric data can be processed without satisfying one of the requirements set out by Article 6(1). Recital 51 explicitly clarifies that the specific requirements for processing of biometric and other sensitive data apply *in addition* to the conditions for lawful processing.[84]

The GDPR also limits the use of automated individual decision making. Article 22(1) gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or affects them in similarly significant manner. A fully automated decision is one where there is no human intervention, and the result of the processing is not checked by a person responsible for the decision.[85] Paragraph 2 provides three exceptions: an automated decision is in compliance with the GDPR if (i) necessary for entering into, or performance of, a contract, (ii) authorised by Union or Member State law, or (iii) based on the data subject's explicit consent. However, even if one of the exceptions applies, automated processing needs to be subject to suitable safeguards.[86] These should include specific information to data subjects and the right to obtain human intervention, to express their point of view, to obtain an explanation of the decision reached

---

[80] Catharine Dupré in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Nomos 2014), Art 1 01.39.

[81] 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, 1-88 (GDPR).

[82] Art 4(14) GDPR.

[83] Art 9 GDPR.

[84] Sebastian Dienst in Daniel Rücker and Tobias Kugler (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Nomos 2017), 101.

[85] Joachim Schrey in Daniel Rücker and Tobias Kugler (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Nomos 2017), 149.

[86] Art 22(2) (b) and 22(3) GDPR; Recital 71 GDPR.

after such assessment and to challenge the decision.[87] For automated individual decision-making based on biometric data, Article 22(4) sets out even narrower exceptions. Only if the data subject has given its explicit consent or if the processing is necessary for reasons of substantial public interest, an automated decision may be based on biometric data.[88]

c. Law Enforcement Directive

The processing of personal data (including biometrical data) for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties is excluded from the GDPR's scope[89] but is covered by the Law Enforcement Directive (LED). [90] Other than the GDPR, the LED does not provide grounds for the lawful processing of personal data but only sets out general principles for law enforcement authorities.[91] The LED, however, does strictly limit the processing of biometric and other sensitive data. According to Article 10, the processing of biometric data for the purpose of uniquely identifying a natural person by law enforcement is only allowed if deemed strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subject. Furthermore, the processing must either (i) be authorised by Union or Member State law, (ii) protect the vital interests of the data subject or of another natural person, or (iii) relate to data which has manifestly been made public by the data subject. If the processing infringes Article 10 LED, data subjects have the right to request the erasure of the data concerning them.[92]

Pursuant to Article 11 LED, the use of automated decision-making that may produce adverse legal effects for data subjects is only permitted if sufficient safeguards for the rights and freedoms of the data subjects, in particular the right to obtain human intervention, are in place. Regarding automated decisions that are based on biometric data, the LED's limitations are less concrete than those under the GDPR. Article 11(2) LED merely sets out that suitable measures to safeguard for the protection of the data subject's rights and freedoms and legitimate interests need to be in place. Paragraph 3 of said provision clarifies that profiling which leads to discrimination against natural persons on the basis of sensitive data is prohibited.

The LED also requires Member States to implement appropriate security measures, including confidentiality and the current state of the art, especially concerning special categories of personal data like biometric data. These include measures like user control, storage control, access control and integrity[93] and should take into account the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage.[94]

---

87 Recital 71 GDPR.

88 See Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01).

89 Art 2(2) (b) GDPR.

90 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, OJ L 119, 89-131.

91 Art 4(1) LED.

92 Art 6(2) LED.

93 Art 29 LED.

94 Recital 60 LED.

d. Council Regulation No 2252/2004

On an EU level, the first specific authorisation for the collection, storage and use of first generation biometrics were introduced by Council Regulation No 2252/2004, which sets out security requirements for EU passports[95]. According to Art 1(2) of the Regulation, passports and travel documents issued by Member States need to include a highly secured storage medium that contains a facial image and two fingerprints. The European legislator considers the collection and storage of these biometric identifiers necessary to establish a reliable link between the genuine holder and the document, and to make travel documents more robust against fraudulent use.[96] In order to protect the biometric data from unauthorised access and misuse, the Regulation requires Member States to ensure that the data is secured and the storage medium has a sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.[97] Article 1(b) clarifies that only staff of the national authorities responsible for issuing passports shall be authorised to collect the biometric identifiers and shall do so in accordance with the European Convention on Human Rights (ECHR) and the UN Convention on the Rights of Child. In case there are problems regarding the collection of the biometric identifiers, the Member States shall ensure that there are appropriate procedures in place that guarantee the dignity of the concerned person. Article 4(2) explicitly states the biometric identifiers may only be used for the verification of the authenticity of the document and to verify the identity of the holder by comparing the identifiers to directly available features when the presentation of a travel document is required by law.[98]

e. Border control and security legislation

In the context of border control and security, there are a handful of EU laws that allow for the collection, storage and sharing of biometric data. Most notable is the Entry-Exit System Regulation (EES Regulation),[99] which is the centrepiece of the European Commission's Smart Border Package. Also worth mentioning in connection with the use of biometric techniques for border security are the regulations making up the Schengen Information System (SIS)[100], the Prüm Decision[101], as well as the EURODAC (European Dactyloscopy) system, which was the first European wide biometric data base

---

[95] Regulation (EC) 2252/2004 of the Council of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 1-6; amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009, OJ L 142, 1-4.

[96] Recital 2; 3 Regulation (EC) 2252/2004.

[97] Article 1(2) Regulation (EC) 2252/2004.

[98] Art 4(3) Regulation (EC) 2252/2004.

[99] 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, 20-82.

[100] 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, 1-13; 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, 14-55; 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, 56-106.

[101] Decision (EC) 2008/615/JHA of the Council of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 1-11.

and enables the comparison of fingerprints of asylum applicants.[102] While the use of biometrics is considered to improve security, the increasing deployment of biometrics-based surveillance techniques has also sparked criticism and fuelled fears of a mass-surveillance state (see also 1.1.a and 0).

The EES Regulation's objectives are twofold. Firstly, the improved management of external borders and prevention of irregular immigration and overstays.[103] To this end, Member States need to set up an Entry-Exit System that records and stores the date, time and place of entry and exit of any third-country nationals crossing the outside Schengen border. This information is combined with fingerprint data, a facial image and the information in the travel document.[104] By 2022, when the Regulation enters into force, this scheme will replace the stamping of passports, which was the only way to verify the duration of a stay in the European Union.[105] The data collected under the EES scheme can also be used for the Regulation's second objective, which is to prevent, detect and investigate terrorist or other serious criminal offences.[106]

While the Recitals explicitly state that the EES Regulation has sufficient safeguards to be compatible with the CFR, and Article 10 provides that the national authorities may only capture and use biometric data in accordance with the CFR and ECHR, concerns as to the Regulation's effects on the right data protection and private life have been voiced. With regard to the initial proposal, the European Data Protection Supervisor (EDPS) has pointed out that the EES scheme constitutes a significant interference with Articles 7 and 8 CFR, as it processes highly sensitive data and affects a large number of persons. While the EDPS recognised the need for coherent and effective information systems for borders and security as an objective in the general interest, he questioned, *inter alia*, the proportionality of the EES Regulations prescribed five-year retention period for the collected data.[107] Although the retention period has been shortened to three years in the final Regulation, [108] concerns are still being raised over the proportionality of the EES scheme, as sensitive data of millions of people is collected in an untargeted manner and stored for an extended period of time.[109]

The SIS is a centralised European database containing information of missing or wanted persons. It enables the exchange of information between national authorities and EU agencies for purposes of law enforcement and border security. In 2019, several regulations reforming the SIS entered into force.[110] The SIS allows for the upload of biometric data, including fingerprints, hand marks and facial images.

---

[102] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 1-30.

[103] Recital 15 EES Regulation.

[104] See Arts 15 – 19 EES Regulation.

[105] Recital 7 EES Regulation.

[106] Recitals 20 and 22 EES Regulation.

[107] EDPS, 'Opinion on the Second EU Smart Borders Package' (Opinion 06/2016).

[108] See Article 31 EES Regulation.

[109] See e.g. Julia Wojnowska-Radzińska, 'Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) versus Data Protection – Is It Done in the Right Way?' (2020) 37 Review of European and Comparative Law 121.

[110] Regulation (EU) 2018/1860; Regulation (EU) 2018/1861; Regulation (EU) 2018/1862.

Since the latest reform also DNA profiles of missing or wanted persons can be uploaded.[111] The new SIS regulations also require Member States to be able to use the fingerprint search functionality in all operational circumstances.[112]

The Prüm Decision[113] obliges Member States to have a system in place that allows authorities of other EU states to allow automated searches of national DNA[114] and fingerprint [115] databases for security reasons (e.g. preventing terrorist attacks) or investigating criminal offences. In its essence, the Prüm decision establishes a decentralised network for the exchange of biometric data, consisting of national databases that are interconnected.[116] Non-EU-Member States participating in the Prüm system are Norway, Switzerland and Iceland.

2.1.3 Proposals by the European Commission

a. Artificial Intelligence Act (proposal)

In spring 2021, the European Commission published a proposal for a Regulation setting out rules on artificial intelligence, the so-called Artificial Intelligence Act (AIA).[117] The proposed AIA lays down rules for the development, placement on the market and use of AI systems in the Union. The Commission chose to follow a risk-based approach and therefore differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk.[118] Depending on the risk classification, an AI application may need to be in conformity with a range of mandatory requirements.

The AIA specifically addresses biometric identification systems and the use of AI for processing biometric data, which are outlined and discussed at length in Chapter 6 together with recommendations for adaptations. Here only a brief overview shall be given.

Following the GDPR and LED the AIA 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*'.[119] The processing of biometric data is listed in the AIA's Annex III as high-risk AI system.[120] This means their use is not prohibited but subject to a number of mandatory requirements. These requirements include, inter alia, the implementation of a risk management system and appropriate data governance and management practices as well as ensuring transparency and

[111] Report from the Commission to the European Parliament and the Council on the state of play of preparations for the full implementation of the new legal bases for the Schengen Information System (SIS) in accordance with Article 66(4) of Regulation (EU) 2018/1861 and Article 79(4) of Regulation (EU) 2018/1862, COM(2020) 72 final.

[112] Report, COM(2020) 72 final.

[113] Decision (EC) 2008/615/JHA.

[114] Art 2 Decision (EC) 2008/615/JHA.

[115] Art 8 Decision (EC) 2008/615/JHA.

[116] For a detailed analyis of the Prüm system see Niovi Vavoula, 'Police Information Exchange - The Future Developments Regarding Prüm and the API Directive' (2020 European Parliament).

[117] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain union legislative acts, COM(2021) 206 final (Artificial Intelligence Act).

[118] Art 12 Proposal for a Regulation COM(2021) 206 final; Although the proposal only lists three categories, it actually distinguishes between four different degrees of risk: 1) prohibited AI systems that pose unacceptable risk, 2) high-risk AI systems that are permitted but subject to several requirements, 3) applications that are only subject to transparency requirements and 4) AI systems that pose minimal or no risk and are permitted without any restrictions. See in more detail 6.3.1.

[119] Art 3(33) Proposal for a Regulation, COM(2021) 206 final.

[120] See Art 6(2) and Annex III Proposal for a Regulation, COM(2021) 206 final.

appropriate human oversight.[121] Additionally, the provider of high-risk AI has to comply with a stricter conformity assessment procedure, involving a notified body, unless the system is in full conformity with harmonised standards. In the latter case, a conformity assessment procedure based on internal control is sufficient[122]

The use of AI for 'real time' remote biometric identification systems in publicly available places for law enforcement purposes is considered an 'unacceptable risk' and therefore prohibited. However, Articles 5 (1) (d) and Articles 5 (2) to (4) list a number of conditions under which the use of such systems is permitted. The use of an AI for 'real time' remote biometric identification needs to be strictly necessary for the search for victims of crimes, prevention of a specific imminent threat to life or the search for perpetrators of specific criminal offences.[123] Furthermore, it needs be take into account the seriousness, probability and scale of the harm if the system would not be used as well as the consequences for the rights and freedoms of affected persons. 'Real time' remote biometric identification also needs to comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations. Another condition is the compulsory prior authorisation by a judicial or independent administrative authority, which can only be circumvented in in duly justified situations of urgency.[124]

b. Digital Services Act (proposal)

On 15 December 2020, the Commission published its proposal for a Digital Services Act (DSA).[125] The proposed Regulation builds on the e-Commerce Directive and introduces new rules for the provision of intermediary services in the internal market. Chapter 2 sets out conditions under which providers of intermediary services are exempt from liability for third-party information they transmit and store. The DSA proposes due diligence obligations that aim to ensure a transparent and safe online environment for all providers of intermediary services. Additional and more far-reaching obligations are proposed for providers hosting services, online platforms and very large online platforms. The provisions of DSA concern in particular the obligation of platforms regarding the handling of illegal content. For example, it is set out that platforms should treat take-down notices of trusted flaggers with priority, but also adopt measures against misuse of the notice and take down system.[126] Furthermore, online platforms have to comply with transparency requirements regarding any advertising on their online interfaces. They have to inform about the person on whose behalf the advertisement is being served and about the main parameters used to determine to whom the advertisement is displayed.[127] Additionally, very large online platforms have to inform in a clear, accessible and easily comprehensible manner, about the main parameters used in their recommender systems.[128] As the DSA does not contain any specific provisions on biometrics, its influence on the use of biometric techniques may, at best, be indirect and 'soft' (see 0).

---

[121] See Arts 11–14 Proposal for a Regulation, COM(2021) 206 final.

[122] Art 43(1) Proposal for a Regulation, COM(2021) 206 final.

[123] Laid down in Art 2 para 2 of Council Framework Decision 2002/684/JHA, including e.g. rape, terrorism, murder, computer-related crime.

[124] See Art 5(d), and 5(2) – (4) Proposal for a Regulation, COM(2021) 206 final.

[125] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.

[126] Arts 19 and 20 Proposal for a Regulation, COM(2020) 825 final.

[127] Art 24 Proposal for a Regulation, COM(2020) 825 final.

[128] Art 29 Proposal for a Regulation, COM(2020) 825 final.

2.1.4 National law

a. Austria

Regulation No 2252/2004, which lays down security requirements for EU passports, is complemented by the Austrian Passport Act (*Passgesetz*). The Passport Act recognises the particular sensitivity of biometric data and imposes stricter rules on the use and storage of fingerprints than for other data. However, other than in Germany (see 2.1.i), the Austrian Passport Act introduces additional safeguards only for fingerprints and not for facial images, which are largely treated like other personal data. For example, facial images may be shared with other agencies if necessary for administrative tasks, while fingerprints may only be processed to identify the passport holder or to verify the authenticity of the passport.[129] Moreover, only fingerprint data needs to be deleted not later than two months after the passport has been issued.[130] The Passport Act also contains an authorisation to store the collected data in a centralised databases only for facial images and other data but not for fingerprints. The processing of the facial images is, however, limited to specific reasons and the images need to be physically deleted eight years after expiry of the last validity period.[131]

The Law Enforcement Directive has been transposed in the Austrian Data Protection Act (*Datenschutzgesetz,* DSG), which prohibits the processing of biometric data, unless it is necessary for the protection of a person's rights and freedom, allowed by law, or the data has been made public by the person itself (see 2.1.d). [132]

Collecting biometric data for law enforcement purposes is also governed by the Federal Security Police Act (*Federal Security Police Act,* SPG). The collection of DNA samples is only allowed, if the suspected crime carries a minimum sentence of one year of imprisonment. An exception may be made if a person asks for the collection of their biometric data. The collected data may only be passed on to other security authorities under strict rules and must be deleted five years after the death of the affected person.[133]

b. Germany

The German Passport Act (*Passgesetz)* accompanies Council Regulation No 2252/2004 and lays down additional rules for the collection and use of biometric data. The security requirements for EU passports set out in Regulation No 2252/2004 (see 2.1.d) are further specified in the German Passport Act (*Passgesetz*). For example, Section 4(3) explicitly sets out that no nationwide database containing the biometric data collected for issuing a passport shall be established. In Section 16a it is clarified that the biometric data stored on the chip of the passport may only be read and used for the purpose of verifying the authenticity of the document or the identity of the passport holder. The biometric data may only be stored by competent passport authorities and needs to be deleted at the latest after the passport has been handed to the passport applicant.[134] The Passport Act also prohibits the automatic

[129] § 22a(3) Austrian Passport Act 1992.
[130] § 22a(5), (6) Austrian Passport Act 1992.
[131] § 22b(2), (3); § 22c(2), (4) Austrian Passport Act.
[132] § 39 Austrian Data Protection Act.
[133] § 64 ff Sicherheitspolizeigesetz.
[134] § 16(2) Passport Act 1992.

retrieval of personal data from passports, except for purposes of border control, criminal prosecution or customs surveillance. [135]

In Germany, the provisions of the GDPR are accompanied by the provisions of the Federal Data Protection Act (*Bundesdatenschutzgesetz,* BDSG). Noteworthy is that Section 4 BDSG provides specific requirements for video surveillance in public places. The use of optical-electronic devices to surveil public places is only allowed if (i) necessary for fulfilling tasks of public authorities, (ii) to exercise of domiciliary rights (iii) or for legitimate interests for specifically defined purposes except where they are overridden by protected interests of the data subject. Section 4(3) BDSG provides that data collected by video surveillance may be stored if necessary to achieve the purpose pursued and not overridden by interests of the data subject. The legislator intended that the special grounds set out in Section 4 BDSG apply for video surveillance by public and private controllers.[136] However, the German Federal Administrative Court – Supreme Court (*Bundesverwaltungsgericht*, BVerwG) held that Section 4(1) as legal ground for video surveillance measures by non-public bodies violates EU law, as Article 6(1) GDPR exhaustively regulates such processing activities. Video surveillance by public bodies may, however, still be based on Section 4(1), because Articles 6(2) and (3) GDPR provide Member States sufficient leeway in this regard.[137]

Surveillance by public agencies falls within the competences of the states. Therefore, the LED has not transposed on federal level but needs to be implemented by each of the 16 states. In 2019, the European Commission opened infringement proceedings against Germany, as only 10 states had adopted measures implementing the LED.

c. United Kingdom

The main legal document regulating aspects of biometric techniques is the Data Protection Act (UK-DPA).[138] Despite Brexit, the UK-DPA still mirrors EU data protection law. The second part contains the provisions of the GDPR, while the LED's provisions have been transposed in Part 3. Based on Council of Europe's modernised Convention 108[139] part 4 of the UK-DPA stipulates specific provision for intelligence services. In contrast to the legislation of other Member States, the UK-DPA regulates processing by intelligence services separately from processing by law enforcement authorities. However, both parts contain comparable data protection principles[140] as well as sections regulating rights of data subjects and safeguards for processing.

Post Brexit, the UK is intending to set up several platforms in order to share biometric data for security and border control purposes with other countries to compensate for the withdrawal from the EU-wide real-time alert agreements.[141]

---

[135] § 17 Passport Act 1992.

[136] Thomas Becker, 'Rechtsgrundlagen der Verarbeitung personenbezogener Daten' in Kai-Uwe Plath, DSGVO/BDSG (3rd edn 2018), § 4 BDSG.

[137] Federal Administrative Court (BVerwG) 27 March 2019, 6 C 2.18.

[138] Data Protection Act 2018.

[139] Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data (1981) ETS 108.

[140] Section 35-40 Data Protection Act 2018.

[141] HM Government, *2025 UK Border Strategy* (2020) CP 352, 44.

d. Beyond Europe

In the United States of America, several states have proposed and even passed legislation restricting the use of biometrics. In 2008, Illinois adopted the Biometric Information Privacy Act (BIPA),[142] which regulates the use of consumers' biometric information by private entities. The BIPA defines 'biometric identifiers' as retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry and explicitly excludes writing samples, photographs and physical descriptions such height and weight. Where private entities want to collect biometric data, they must inform the data subject in writing about the fact that their information is being collected and stored and about the specific purpose and duration of the collection and storage. Furthermore, a written release must be obtained from the data subject.[143] The collected data may only be disclosed under certain conditions and with the consent of the data subject.[144] Selling or profiting otherwise from the consumers' biometric data is generally prohibited.[145]

The BIPA is considered the leading statute in the US when it comes to legislation restricting the use of biometrics. Texas and Washington also have statutes that condition the use of biometric identifiers by private entities to the consent of data subjects. Other than the BIPA, they do not afford a right to private action but authorise the state attorney general to enforce the law. Several states, such as Maryland and New York, are planning to adopt similar legislation but have not yet successfully passed it. In California, the use of biometric data is covered by the California Consumer Privacy Act (CCPA), which sets out general limits on the processing of personal information (including biometric data).[146] The need to regulate the use of biometric information has also been identified on a federal level, and a bill for a National Biometric Information Privacy Act was introduced in the US Congress.[147] While state and federal efforts have been limited to regulating the use of biometric data by private parties, some cities (such as Portland, Boston and San Francisco) have gone further and placed strict limits on the use of facial recognition by law enforcement[148] due to risks of racial bias and misidentification posed by this technology.[149]

Under the Japanese Act on the Protection of Personal Information (AAPI) the notion of personal information also covers 'codes into which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers.'[150] This includes first biometric identifiers, such as DNA, facial templates, finger and palm prints.[151] A person who provides a database of personal

---

[142] (740 ILCS 14/) Biometric Information Privacy Act.

[143] Sec 15(b) BIPA.

[144] See Sec 15(d) BIPA.

[145] Sec 15 15(c) BIPA

[146] For an overview see Dmitry Shifrin and Mary Buckley Tobin, 'Past, Present and Future: 'What's Happening with Illinois' and Other Biometric Privacy Laws' (*The National Law Review, 2021*) available at <https://www.natlawreview.com/article/past-present-and-future-what-s-happening-illinois-and-other-biometric-privacy-laws> (last accessed 24 July 2021).

[147] S. 4400 — 116th Congress: National Biometric Information Privacy Act of 2020.
<https://www.govtrack.us/congress/bills/116/s4400> (last accessed 21 July 2021).

[148] Jay Peters, 'Portland Passes Strongest Facial Recognition Ban in the US' (The Verge, 2020) available at <https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology> (last accessed 4 August 2021).

[149] See Portland, Oregon, City Code, Title 34.10.010.) (on this issue, see 3.3.2.)

[150] See the English translation of the AAPI by the Japanese Personal Information Protection Commission available at <https://www.ppc.go.jp/files/pdf/APPI_english.pdf> (last accessed 21 July 2021).

[151] See Daniel Hounslow and Ryuichi Nozaki, 'Japan - Data Protection Overview' (*DataGuidance*, 2020) available at <https://www.dataguidance.com/notes/japan-data-protection-overview> (last accessed 24 July 2021).

information for business use may do so only if the data subject is notified about the purpose and has given consent.[152]

China is currently planning to adopt a Personal Information Protection Law (PIPL). While the law has not been enacted yet, a second draft has been released by the Chinese legislator in summer 2021.[153] Very similar to the GDPR, Article 4 PIPL defines personal information as any information recorded by electronic or other means relating to an identified or identifiable natural person. Article 13 PIPL sets out legal grounds for the processing of personal information, which include the data subject's consent, and the necessity to fulfil a contract that is in the interest of the data subject. Article 14 PIPL clarifies that consent needs to be voluntary, and the data subject has the be informed about the purpose of the processing. Biometric information is considered sensitive data according to Article 29 PIPL, and therefore the additional requirements of Section II apply. Biometric information may only be processed for specific purposes and if sufficiently necessary, and the data subject has to be notified of the necessity and effects of the processing.

2.2. Case Law

2.2.1 European Court of Human Rights (ECtHR)

The case law of the ECtHR covering the collection and use of biometric data includes the judgements Murray v United Kingdom,[154] S. and Marper[155], Van der Velden[156], Gaughran v. the United Kingdom[157], M.K. v France,[158] and P.N. v. Germany.[159]

The first case, concerning the retention of biometric data, related to the storage of photographs of convicted terrorists in Ireland. The Grand Chamber of the ECtHR held that the retention and storage of basic personal details about the arrested person, or even about other persons present at the time, is not outside the legitimate limits of the procedure for investigating terrorist offences.[160]

In S. and Marper v the United Kingdom, the Grand Chamber of the ECtHR had to decide on the retention of fingerprints and cellular samples in DNA databases. According to the Court's assessment, a '*DNA profile's capacity to provide a means of identifying genetic relationships between individuals is in itself sufficient to conclude that their retention interferes with the right to private life of the individuals concerned*'[161]. Therefore, the retention of fingerprints, requires a minimum of safeguards concerning duration, storage, and usage destruction, especially if the data is automatically processed.[162] The ECtHR also stated that the level of interference may vary between the different categories of personal data,

---

[152] Arts 15 and 16 PPA.

[153] An unofficial English translation of the second draft is available here: <https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-draft-second-review> (last accessed 21 July 2021).

[154] *Murray v. United Kingdom* App no 14310/88 (ECtHR 28 October 1994).

[155] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008).

[156] *Van der Velden v the Netherlands* App no 21203/10 (ECtHR 31 July 2012).

[157] *Gaughran v. the United Kingdom* App no 45245/15 (ECtHR 13 February 2020).

[158] *M.K. v. France* App No 19522/09 (ECtHR 18 April 2013).

[159] *P.N. v. Germany* App No 74440/17 (ECtHR 11 June 2020).

[160] *Murray v. United Kingdom* App no 14310/88 (ECtHR 28 October 1994).

[161] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008), para *75.*

[162] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008), para 78f; for judgements concerning photographs see *Friedl v Austria* App no 15225/89 (ECtHR 26 January 1995); for voice *P.G and J.H v the United Kingdom App no 44787/98* (ECtHR 25 September 2001).

stating that fingerprints have less of an impact on private life than DNA samples. '*The mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.*'[163] The ECtHR recognised that the retention of DNA samples pursues the legitimate purpose of detecting criminal offences.[164] The Grand Chamber held that the retention of DNA data violates Article 8 of the Convention, because not only the data of convicted persons but also the data accused person that have already been acquitted was stored indefinitely.[165]

In the case Van der Velden, the ECtHR held that the collection of DNA samples does not infringe Article 7 of the Convention. The ECtHR deemed the obligation to undergo DNA testing for persons convicted of offences of a certain severity reasonable and to be necessary in a democratic society, especially noting the substantial contribution DNA records have made to law enforcement.[166] However, the ECtHR also recognised that due to '*the use to which cellular material in particular could conceivably be put in the future, the systematic retention of that material goes beyond the scope of neutral identifying features such as fingerprints, and is sufficiently intrusive to constitute an interference with the right to respect for private life set out in Article 8 § 1 of the Convention*.'

Reiterating the necessity of protection of personal data for the right to a private life, in M.K. v France the ECtHR emphasised that '*the protection of personal data is of fundamental importance to a person's enjoyment to a private life, especially when the data is used for police purposes and undergoes automated processing.*'[167]

The necessity for a minimum of safeguards and limitations regarding the retention of fingerprints and DNA profiles was reiterated in Gaughran v the United Kingdom.[168] The ECtHR considered the permissible margin of appreciation to be exceeded when fingerprints and DNA profiles of persons convicted of minor offences are stored indefinitely without the possibility of requesting the deletion of these data. Such interference with the applicant's right to respect for private life cannot be regarded as necessary in a democratic society.[169] Additionally, in its considerations, the ECtHR accepted that retention of fingerprints and photographs until after death could be considered comparable to indefinite retention.[170]

Finally, in line with its judgement in S. and Marper v the United Kingdom, when assessing the proportionality of the retention of fingerprints and photographs, the ECtHR stated that it '*constitutes a less intrusive interference with the applicant's right to respect for his private life notably than the collection of cellular samples and the retention of DNA profiles, which contain considerably more sensitive information.*'[171] Thus, the retention of fingerprints and facial images for a duration of 25 years was deemed 'relevant and sufficient' and not in violation of Article 8 of the Convention.[172]

---

[163] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008), para 121.
[164] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008), para 100.
[165] *S. and Marper v the United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008), para 122.
[166] *Van der Velden v the Netherlands* App no 21203/10 (ECtHR 31 July 2012).
[167] *M.K. v. France* App No 19522/09 (ECtHR 18 April 2013), para 35.
[168] *Gaughran v. the United Kingdom* App no 45245/15 (ECtHR 13 February 2020).
[169] *Gaughran v. the United Kingdom* App no 45245/15 (ECtHR 13 February 2020), para 97.
[170] *Gaughran v. the United Kingdom* App no 45245/15 (ECtHR 13 February 2020), para 80.
[171] *P.N. v. Germany* App No 74440/17 (ECtHR 11 June 2020), para 84.
[172] *P.N. v. Germany* App No 74440/17 (ECtHR 11 June 2020), para 90.

2.2.2 Court of Justice of the European Union (CJEU)

Currently, there is no EU case law regarding highly sophisticated identification techniques. However, the CJEU has, in several decisions, addressed the question of whether the use of first generation biometrics is compatible with fundamental rights.

In the case *Schwarz,* the CJEU was asked whether Article 1(2) of Regulation No 2252/2004, which obliges national authorities to take and store fingerprints when issuing a passport, violates a person's rights to respect for private life and the protection of personal data. While the Court acknowledged the threat of this obligation to the rights afforded by Article 7 and 8 CFR, it concluded that the processing of fingerprints does not go beyond what is necessary to achieve the Regulation's aim of protecting against the fraudulent use of passports.[173] In its proportionality test, the CJEU specifically mentioned that Article 4(3) of Regulation No 2252/2004 ensures that a mismatch between the fingerprints of the holder of a passport and the data in that document does not lead to an automatic decision, such as the refusal to enter the European Union. Rather, any irregularities will draw the competent authorities' attention to the person concerned and will result in a more detailed check of that person in order to definitively establish their identity.[174] By providing that the fingerprints are stored only on a highly secure medium in the passport itself and in any centralised manner, Article 1(2) of Regulation No 2252/2004 also provides sufficient guarantees that the data is not used for any other purposes than verifying the authenticity of a passport and the identity of its holder.[175]

However, due to the limited scope of Regulation No 2252/2004 and the lack of an overarching framework on the use of first generation biometrics, the rights afforded by Charter only provide very limited protection. This has become particularly apparent in *Burgemeester* case.[176] The CJEU was asked whether Articles 7 and 8 CFR together with Regulation No 2252/2004 requires Member States to guarantee that the biometric data collected and stored pursuant to that Regulation will not be collected, processed and used for purposes other than issuing passports. The court held that Regulation No 2252/2004 does not apply to the use and storage of biometric data for other purposes than issuing a passport. These matters are exclusively within the competence of the Member States. Since the fundamental rights guaranteed by the Charter apply only where national legislation falls within the scope of EU law,[177] the Court could not determine whether the storage and use of biometric data for purposes other than issuing passports are compatible with Articles 7 and 8 of the Charter.[178] It would be for the national courts to assess whether the national measures relating to the use and storage of biometric data are compatible with the ECHR.[179]

While the question of whether the central storage of biometric data is compatible with Article 7 and 8 CFR was left open in the *Burgemeester* decision, the CJEU provided guidance in a case relating to national rule that made the issuance of a temporary residence permit to third-country nationals conditional upon the collection, recording and retention of their biometric data in a central filing system. The matter related to EU law because the affected persons were Turkish nationals, and the EEC-Turkey Association Agreement stipulates that no new restrictions on the conditions of access to

[173] Case C-291/12 *Schwarz v Stadt Bochum* (CJEU 17 October 2013), para 63.

[174] Case C-291/12 *Schwarz v Stadt Bochum* (CJEU 17 October 2013), para 44.

[175] Case C-291/12 *Schwarz v Stadt Bochum* (CJEU 17 October 2013), paras 56-61.

[176] Joined Cases C-446/12 to C-449/12 *Burgemeester* (CJEU 16 April 2015).

[177] Case C-418/11 *Texdata Software GmbH* (CJEU 26 September 2013), para 71-73.

[178] Joined Cases C-446/12 to C-449/12 *Burgemeester* (CJEU 16 April 2015), para 47-50.

[179] Joined Cases C-446/12 to C-449/12 *Burgemeester* (CJEU 16 April 2015), para 51.

employment are introduced unless they are justified by public policy, public security or public health.[180] In its decision, the CJEU came to the conclusion that the central storage of biometric data interferes with Art 7 and 8 CFR but is proportionate and necessary to combat identity and document fraud. The Court argued that fingerprints and facial images are a reliable way for identification and are not of an intimate nature and do not cause any particular physical or mental discomfort for the person concerned. Furthermore, the national rule limits the access to and use of the biometric data contained in the central filing system, which is limited to officials of the national authorities responsible for the implementation of national legislation on foreign nationals for the purpose of establishing or verifying the identity of third-country nationals to the extent necessary for the performance of their tasks. The CJEU also found that the required retention period of five years is not excessive and justified in light of the rule's objective of preventing and combating identity and document fraud.[181]

2.2.3 National courts/data protection authorities

a. Austria

In Austria, a hospital required biometric finger scanning for their employees to record their working time. It was argued that such a measure needs to be approved by the works council because it touches upon the human dignity of employees. The Austrian Supreme Court of Justice (*Oberster Gerichtshof*, OGH) ruled in favour of the employees and held that the biometric templates are obtained for the comparatively trivial aim of determining the employee's times of coming and going. The use of biometric scanning is neither the least invasive nor the most effective means of control for workers. Since the creation of fingerprint templates reaches a considerable level of control over employees, it affects their human dignity and therefore requires approval by the works council. The security measures taken by the employer, such as ensuring that the template cannot be traced back to the original fingerprint, do not change this conclusion according to the OGH.[182]

b. France

The question of whether the collection and use of first generation biometrics for passports is compatible with fundamental rights was not only addressed on EU (see 0) but also on national level. In France, the storage of fingerprints in a database was the subject of ruling by the *Conseil Constitutionnel* (see also 0). Article 5 of the Identity Protection Act provided for the creation of a database in which fingerprints and other personal data required for the issuance of a passport would be stored. However, the fingerprints could be retrieved not only for the issuing of a passport but also for investigations into certain criminal offenses as well as to prevent attacks against France. The *Conseil Constitutionnel* considered the creation of such a biometric database, which allows the identification of virtually the entire French population by their fingerprints, an unconstitutional interference with the right to respect for privacy. While the legislation's objective to render passports more save and prevent fraud serves justified interests of the general public, the interference with the right to privacy was not regarded as proportionate to the goal pursued.[183]

---

[180] Arts 13 and 14 Decision No 1/80 of the Association Council of 19 September 1980 on the Development of the Association.

[181] Cases C-70/18 Staatssecretaris van Justitie en Veiligheid v A and Others, (CJEU 3 October 2019), paras 53-69.

[182] Austrian Supreme Court of Justice 18 October 2006, 9 Ob 109/06d; Austrian Supreme Court of Justice 22 January 2020, 9 Ob 120/19s.

[183] Conseil Constitutionnel 22 March 2012, No 2012-652 DC.

The storage of fingerprints for passport purposes was additionally extended by a decree of the French Ministry of the Interior in 2005, which required the submission of eight fingerprints for the issuance of a new passport. Pursuant to the ministry, this change was made to reduce the risk of identification errors. According to EU law, only two fingerprints were stored on the passport and the *Conseil d'Etat* could not find any demonstrable usefulness during investigations and repealed the relevant article. However, the central processing of the biometric data was not considered an encroachment on the personal rights of the persons concerned. The linking of the facial image and fingerprint data with other data was considered appropriate for the required purpose.[184]

c. Germany

In Germany, complainants before the German Constitutional Court (*Bundesverfassungsgericht,* BVerfG) argued that the national Passport Act constitutes a disproportionate interference with their right to informational self-determination. The BVerfG rejected the constitutional complaint due to lack of substantive reasoning and did not answer the question of how the challenged provisions are to be assessed under constitutional law. However, the BVerfG provided some general guidance regarding the proportionality test, stating that the more serious the interference, the more restrictive the conditions for the use of the data have to be. The proportionality of the collection of biometric data therefore depends largely on the provisions limiting the storage and use of the data. The German Passport Act, for example, contains provisions on data security,[185] requires that no nationwide database of biometric data is set up,[186] regulates the storage and deletion of biometric data at passport authorities and passport manufacturers,[187] and defines purposes for which the biometric data stored in the chip of the passport may be used.[188] The complainants, however, did not contest that the various provisions determining the use of their biometric data are not suitable to ensure a proportionate protection of their right to informational self-determination. The BVerfG therefore rejected the complaint and did not rule on whether the collection and use of biometric data for passports violates fundamental rights.

The large-scale use of facial recognition software in public places by the Hamburg police during the G20 summit without a specific legal basis was declared unlawful by the Hamburg Data Protection Officer. It was held that biometrically measuring of all faces included in the extensive footage, even though the vast majority of those concerned were not involved in criminal activity, drastically disturbs the balance between citizens' right to informational self-determination and the law enforcement powers of the state. The Data Protection Officer concluded that the generation of mathematical facial models of an unlimited number of citizens without suspicion over a period of at least several days and their storage for an indefinite period requires a special legislative authorisation. The conditions and extent of the mass use of facial recognition software need to legally defined and procedural guarantees that protect the rights and freedoms of data subjects against the generation of facial templates. The Hamburg police was therefore ordered to delete the respective database.[189]

---

[184] Conseil D'Etat 26 October 2011, No 317827.

[185] § 4(3) sentence 2 Passport Act 1992.

[186] § 4(3) sentence 3 Passport Act 1992.

[187] § 16(2) Passport Act 1992.

[188] § 16a Passport Act 1992.

[189] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg (2018); German Federal Constitutional Court 11 March 2008, 1 BvR 1254/07, para 67.

d. Netherlands

The storage of fingerprints required for issuing a passport in centralised database, which could also be accessed for judicial and security purposes, was disputed in several Dutch municipalities[190] and gave rise to CJEU's *Burgemeester* decision (see 0). [191] The Court in Luxembourg did not assess whether the storage of biometric data in such a database was compatible with the CFR, as it considered it a matter of national to which the CDR is not applicable (see 2.1.a). Before the referring *Raad van State* could take a final decision on whether the storage of fingerprints in a database interferes with Article 7 and 8 ECHR, the relevant provision in the national Passport Act had already been amended. The *Raad van State* therefore did not rule on the merits of the case, but merely reiterated the Minister of the Interior's explanation for amending the law. The Minister had stated that the permanent storage of fingerprints was an inappropriate measure for the verification and identification of persons.[192]

Another case concerned the obligation by an employer to use fingerprint scanner for cash registers in shoe stores, which was considered as a violation of Article 9(1) GDPR, by the Court of Amsterdam. The employer argued that the use of fingerprint scanners was justified by Article 29 of the Dutch Act Implementing the GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*), which further specifies the legal grounds for processing sensitive data set out in Article 9(2). Article 29 of the Act Implementing the GDPR allows the processing of biometric data, such as fingerprints for the purpose of unique identification if the same is a necessity to fulfil authentication or security purposes. However, the court held that the use of the fingerprint scan authorisation system was a disproportionate measure for the level of security required in the shoe shops and, as a result, an unjustified violation of the employees' employer's privacy. Furthermore, the employer did not sufficiently explore other, less invasive, solutions.[193]

e. Sweden

The Swedish Authority for Privacy Protection has issued decisions regarding two instances where biometric techniques were used.

The first decision concerned a school in northern Sweden that used facial recognition software in a pilot trial to monitor student attendance at school. The Swedish Authority for Privacy Protection found that the school's use of the facial recognition software violated several Articles of the GDPR. It argued that the processing took place in the children's everyday environment and is therefore a severe intrusion of the students' privacy. Since the purpose of registering school attendance can be achieved with less privacy invasive measures, the use of facial recognition was considered disproportionate to the purpose and in violation of the principles of purpose limitation (Article 5(b) GDPR) and data minimisation (Article 5(c) GDPR). Furthermore, the Swedish Authority for Privacy Protection held that by using the facial recognition software, the school processed biometrical data without a legal basis and therefore violated Article 9 GDPR. The students' consent to participate in the pilot project was not considered voluntary due to the unequal relationship between school board and students and the fact that attendance records are a one-sided control measure. Finally, it was held the school failed to comply

[190] See Raad van State 25 May 2016, 201105172/2/A3; Raad van State 25 May 2016, 201110934/3/A3; Raad van State 25 May 2016, 201110242/3/A3; Raad van State 25 May 2016, 201205423/3/A3.

[191] Joined Cases C-446/12 to C-449/12 *Burgemeester* (CJEU 16 April 2015).

[192] Raad van State 28 September 2012, 201105172/1/A3.

[193] Court of Amsterdam 12 August 2019, 7728204 CV VERZ 19-9686.

with Articles 35 and 36, as it neither conducted a data protection impact assessment nor consulted Swedish Authority for Privacy Protection prior to deploying the facial recognition software.[194]

In the second decision, the Swedish Authority for Privacy Protection fined the Swedish Police Authority for using facial recognition software for law enforcement and investigation purposes. The software allows images to be uploaded, which then – with the use of facial recognition – are compared to the software provider's database, which is made up of images scraped from social media sites and webpages. Although the Swedish Police Authority did not recommend the use of the facial recognition software and employees had decided to use it of their own accord, the Swedish Authority for Privacy Protection considered the Police Authority to be the controller of relevant data and responsible for legal compliance. The Swedish Authority for Privacy Protection held that the police failed to implement sufficient technical and organisational measures and to conduct a data protection impact assessment. Both would have been required under the Criminal Data Act and therefore the police's use of biometric data for facial recognition was considered unlawful. The Police Authority was ordered to inform the data subjects, whose data had been disclosed to software provider and to ensure the erasure of any transferred data.[195]

f. United Kingdom

The trial use of facial recognition software on members of the public by the South Wales Police was brought before the High Court in Cardiff. [196] The complainant argued that such measures violate the right to privacy as contained in Article 8 ECHR. The software extracted biometric data from CCTV footage and compared it to biometric information of offenders on a watchlist.

The High Court ruled that the collection of biometric data by facial recognition software constitutes an interference with the right to privacy under Article 8(1) of the Human Rights Act 1998, which gives effect to the fundamental rights of the ECHR in the UK. Interferences are only allowed if they are in accordance with the law, necessary and proportionate. The High Court found that power afforded to the police to use imagery for the purpose of preventing and detecting crime also allows them to use facial recognition software. Furthermore, the Data Protection Act (both the UK-DPA 1998 and UK-DPA 2018), the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 and police's own policies sufficiently limited how and when the software was to be used. The High Court also considered that a fair balance has been struck between the rights of individuals and the interests of the community and that the use of the facial recognition software was proportionate. The factors justified that decision were that the software was used in an open and transparent way (the police published a fair processing notice on social media and posted signs near the surveillance area) and that its purpose was limited to identify specific individuals on a watchlist. Furthermore, the interference was limited to near instantaneous algorithmic processing and the biometric data was not retained

[194] Swedish Data Protection Authority 20 August 2019, DI-2019-2221.

[195] Swedish Authority for Privacy Protection 10 February 2021, DI-2020-2719.

[196] High Court of Justice (Divisional Court of Cardiff) 4 September 2019, EWCH 2341 (Admin), para 159.

3. ETHICAL ASPECTS OF BIOMETRIC IDENTIFICATION

KEY FINDINGS

The main ethical issue raised specifically by biometric identification is related to the enrolment phase, i.e. the creation and storage of a unique template that identifies a particular person. The enrolment phase and the deployment phase may overlap where templates are refined during deployment, e.g. through supervised learning in the field. Creating unique templates means transforming unique physical features of a human being into digital data, leading to a 'datafication' of humans. Since the features that uniquely identify a person are part of a person's body, their collection and use interfere with a human's personal autonomy and dignity. Once this template is created and stored, anyone who comes into possession of it in the future has the power to trace and recognise that individual anywhere in the world and potentially for any purpose. There is no way for the individual to escape it as an individual cannot normally change 'strong' biometric identifiers. Considering also data security concerns, collecting and storing biometric templates has a significant potential for harm.

Apart from this, ethical issues raised by the use of biometric identification methods in public spaces do not only relate specifically to biometrics, but to large-scale surveillance of individuals as such (i.e., they are similar to issues raised by, for example, large-scale surveillance using mobile device signals), or otherwise to the purposes for which the technology is used, and how it is used. The dimension of ethical issues raised depends, in particular, on

- the concrete purpose of identification;
- the place, manner or dimension of identification;
- the transparency of the identification measures taking place;
- the reactions (e.g. arrest) triggered by a high matching score;
- the evidentiary force ascribed to a high matching score and possibilities of the individual to demonstrate error or identity fraud; and
- any storage and further processing of matching data (e.g. for the creation of mobility profiles).

Issues of discrimination or stigmatisation arise mostly as part of a more general deficiency of a system. For instance, facial recognition should not be less accurate with people of colour, and diminished accuracy must, in any case, be duly taken into account in the context of the last three points mentioned (as must any other lack of accuracy).

3.1. Characteristic steps involved in biometric identification

Biometric identification usually involves a number of characteristic steps, each of which raises its own characteristic ethical issues.

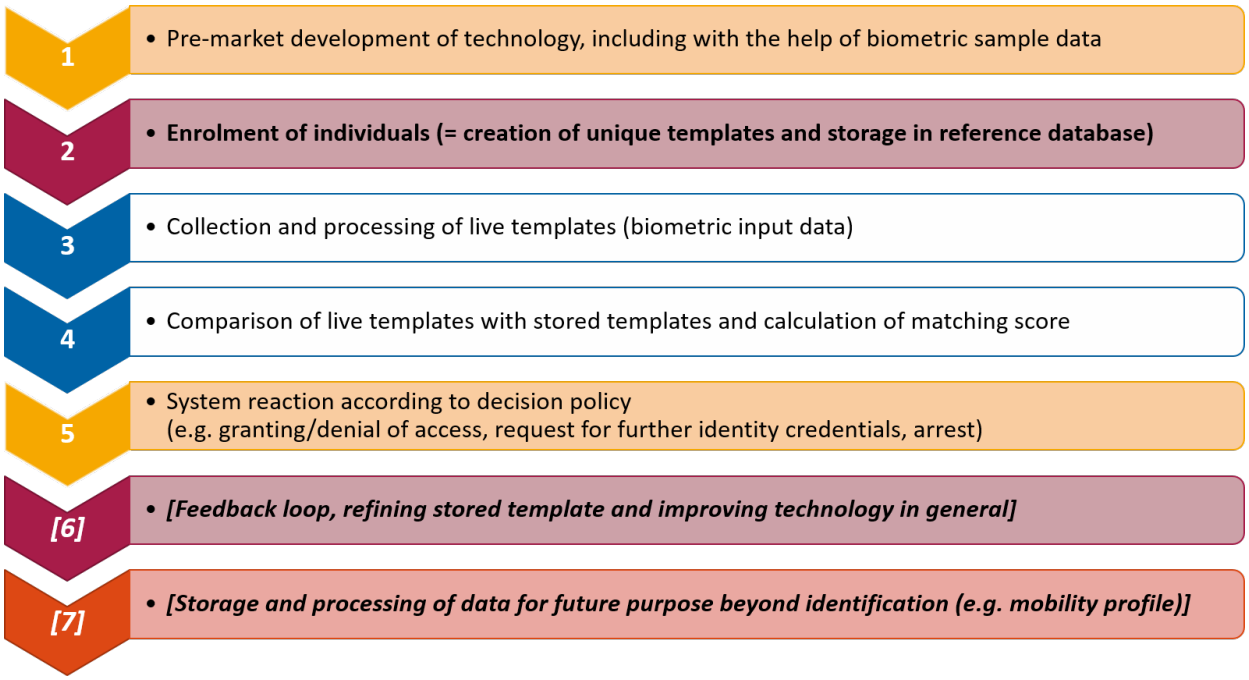
The first step consists in the pre-market development of the technology, which already includes processing of biometric sample data the use of which needs to be justified in legal as well as in ethical terms. The legal and ethical issues raised by this step are not very different from the legal and ethical issues raised by the development of data-driven technologies in general. However, given the sensitivity of biometric identification systems, particular caution is required against any potentially discriminating

effects (e.g. where a biometric identification system has higher rates of false-positives for individuals with a particular ethnic origin).

The decisive step involved in biometric identification is the enrolment phase, i.e. the creation of biometric templates by way of collecting biometric data, extracting specific features, assembling the features in a template, and storing the templates in a reference database.[197]

Once the system goes live, the next step consists in the collection and processing of live templates, i.e. of biometric input data collected from the persons to be identified, such as from persons walking by on the street. Again, this biometric input data requires specific processing, including the extraction of specific features. What follows is the comparison of live templates with stored templates and the calculation of a matching score. Depending on the decision policies of the system (which are usually coded by the developers according to the specific needs of users), different matching scores will usually trigger different reactions, e.g. a high matching score may lead to the granting or denial of access to the building, to a request for further identity credentials, or to enhanced surveillance. Depending on what kind of reactions are triggered (gravity, whether irreversible or not, how they can be challenged), a range of ethical issues may arise, which are generally associated with algorithmic decision making.

Figure 2: Steps involved in biometric identification



Source: Christiane Wendehorst

While the steps described so far are present in any kind of biometric identification activity, further steps may be involved as the case may be. In particular, when the system is one that learns in the field, stored templates may be refined and enriched through combination with confirmed live templates. If that is the case, use of the system becomes a 'second enrolment phase', triggering similar ethical issues as the initial enrolment phase. In addition, data resulting from identification (such as the information that a particular individual was present in a particular place at a particular point in time) may be stored and

[197] Isaac Cooper and Jimmy Yon, 'Ethical Issues in Biometrics' (2019) 30 Science Insights 63.

further processed for purposes beyond identification (such as the creation of a mobility profile), with ethical issues raised depending very much on those purposes and conditions.

3.2. Ethical issues raised by enrolment

3.2.1. 'Datafication' of humans, power and human dignity

For the unique identification of natural persons, 'strong' biometric identifiers need to be captured, transformed into digital data and ultimately into a standardised template. Suitable 'strong' biometric identifiers include fingerprints, facial images, iris and retina scans, and palm prints. These identifiers can be captured by appropriate physical scanners, with the active conscious cooperation of the data subject, remotely without such cooperation (such as with surveillance cameras), or with the help of existing other data (such as existing photographic images). Often these 'strong' biometrics are collected together with 'weak' biometric identifiers, such as gender, age, ethnicity or height, which may be used in conjunction with the strong identifiers in order to improve success rates of identification techniques.[198]

Capturing biometric identifiers means transforming unique physical features of a human being into digital data, leading to a 'datafication' of humans. Since the features that uniquely identify a person are part of a person's body, their collection and use interfere with a human's personal autonomy and dignity. Once a biometric template has been created and stored in a reference database anyone in possession of that template is able to identify and trace the relevant person anywhere on the globe, creating a severe risk for that person of being tracked and put under surveillance. The template may be used for identifying the person for an indefinite range of purposes and in different situations. What makes possession of biometrical templates so powerful and potentially so risky from a fundamental rights perspective is the fact that individuals will, during their lifetime, not be able to change their biometric features. Being traceable by way of biometric data is thus irreversible, and traceability close to inescapable. Other personal data, such as social security number or address (so-called 'indexical data'), is not inextricably tied to the physical features of a human but is only contingently linked to a person.[199]

It is argued that creating biometric templates digitalises the unique characteristics of person, which leads to a loss of control over how a person's bodily features are used by others. The transformation of biometric identifiers into digital data objectifies the human body and gives others the possibility to use unique bodily characterises for their own purposes, even if these purposes are in contradiction to the data subject's interests. The use of objectified characteristics of humans for identification purposes by others is viewed as a contradiction to Kant's fundamental principle that people are to be treated as ends in themselves, never merely as a mean (see 2.1.a).[200]

Considering that a biometric template digitalises the human body and represents bodily features, it has even been argued that the collection of biometric identifiers not only interferes with a person's private life and right to data protection but also with the integrity of a person's body. The use of biometric identification has therefore been compared to bodily searches or other measures that

[198] Anil Jain, Sarat Dass and Karthik Nandakuma, 'Soft Biometric Traits for Personal Recognition Systems' in David Zhang and Anil Jain (eds), *International Conference on Biometric Authentication* (Springer 2004).

[199] Anton Alterman, 'A Piece of Yourself: Ethical Issues in Biometric Identification' (2003) 5 Ethics and Information Technology 139, 144.

[200] Anton Alterman, 'A Piece of Yourself: Ethical Issues in Biometric Identification' (2003) 5 Ethics and Information Technology 139, 145.

interfere with the physical integrity of a person. According to this view, biometric templates create a 'digitalised body' that can be searched remotely and indefinitely, without individuals knowing they are being searched.[201]

However, any kind of datafication of unique physical human features needs to be seen in relation to the purpose of the operation. It is commonly agreed that public security and law enforcement may, in principle, justify certain infringements of private life, considering that a balance needs to be struck between individual rights and the interests of society at large,[202] and provided certain conditions, including the proportionality principle, are complied with. For example, forensic databases and their use to identify persons involved in crime are widely viewed as being justified by the public good.[203] In its Resolution, the European Parliament acknowledges the AI, biometric techniques and related technologies can increase public security and safety in the area of law enforcement and border control. However, it also stresses that '*extensive and rigorous public scrutiny and the highest possible level of transparency both with regards to the risk assessment of individual applications*' is needed.[204]

3.2.2 Potential for harm

a. Unauthorised disclosure and access

The uptake of biometric identification goes hand and hand with the creation and storage of an increasing number of biometric profiles. As any other data, biometric profiles are prone to confidentiality and cybersecurity risks. More servers storing biometric templates also means more potential targets for cyberattacks and the larger databases are the more interesting they become for malicious actors. While breaches of personal data always lead to interferences with the data subjects' right to data protection and private life, risks for fundamental rights are enhanced if the breach concerns biometric templates. Firstly, because biometric templates can be used to remotely track and surveil individuals anywhere in the world. Secondly, biometric identifiers are increasingly used for authentication purposes. Therefore, whoever is in control of biometric templates can use them to create fakes ('spoofs') and commit identity fraud'. Finally, both of these risks are elevated by the fact that individuals only have a limited number of first-generation biometric identifiers, which are practically unchangeable.[205]

Attacks to gain unauthorised access to biometric templates can be directed against a biometric system's database or at the transmission of biometric templates. Where biometric systems transfer templates between different subsystems, interferences with the communication channel during the transmission may allow interception of the biometric templates. An even more attractive target is the database that stores the biometric templates for later comparison, as it will allow access to a high number of templates at once.[206]

---

[201] Irma van der Ploeg, 'Genetics, Biometrics and the Informatization of the Body.' (2007) 43 Annali dell'Istituto superiore di sanita 44, 48.

[202] Parliamentary Assembly of the Council of Europe, The Need for a Global Consideration of the Human Rights Implications of Biometrics, Resolution 1797 (2011).

[203] Margit Sutrop, 'Ethical Issues in Governing Biometric Technologies' in Ajay Kumar and David Zhang (eds), *Ethics and Policy of Biometrics* (Springer 2010).

[204] Recommendation 71 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 (2020/2012(INL))

[205] Jeroen Breebaart and others, 'Biometric Template Protection' (2009) 33 Datenschutz und Datensicherheit - DuD 299.

[206] Anil Jain, Karthik Nandakumar and Abhishek Nagar, 'Biometric Template Security' (2008) 2008 EURASIP J. Adv. Signal Process 1,4.

b. Biometric templates as amplifier of fundamental rights risks

If biometric templates are disclosed, the risk for the data subject is not only that sensitive information can be extracted from the stored biometric template itself, such as the ethnic origin of a person or (the probability of) certain diseases. Due to their uniqueness biometric templates allow efficient identification and tracking without any limitations regarding time or place. Furthermore, biometric templates are often tied to other personal data and can be cross-matched with data from different sources, which allows malicious actors to create elaborate profiles of individuals.[207] Such profiles can reveal more than the sum of the individual pieces of data and can therefore have a severe impact on a person's private life (on this issue see also 0).

Biometric templates in the hand of the wrong actors also increase the risk of so-called spoofing, i.e. circumventing biometric systems by presenting 'fake' (spoofed) biometric identifiers. While some identifiers, such as the iris, are rather difficult to replicate, others can be forged more easily.[208] For example, the biometric template of fingerprint can be used to create artificial fingers with the same dactyloscopic traits.[209] The fact that biometric identifiers are increasingly used for authentication purposes poses additional risks to an individual's private life and protection of personal data. Many electronic devices today are unlocked by using facial recognition and fingerprint scanning, and these methods of identification can further be used to access banking applications or email accounts. In a way a person's biometric identifiers have become a key to unlock a vast amount of extremely sensitive personal data. If more actors create and store biometric templates for identification purposes, it increases the risk that they are hacked. The more copies of a key exist and circulate, the less secure and the less control one has over who has access to the locked items. However, while locks and passwords can be changed if they have been compromised, it is not possible to change one's biometric identifiers.[210] Hence, a person may no longer be able to securely use biometric authentication to protect valuables once biometric templates have been leaked. Concerns over the storage and security of the biometric identifiers required for issuing an EU passport has given rise to a number of court decisions, in which claimants argued that their national laws on the storage of the fingerprints and passport picture violate their fundamental rights (see 0).

c. Safeguards

In order to prevent data breaches and unintentional sharing of templates, strong safeguards must be put in place and the technical robustness of any biometric identification system must be guaranteed at any time (template protection).[211] To reduce the risk to fundamental rights posed by storing and creating biometric templates, linkages between the template and other personal data can be reduced to a necessary minimum and additional de-identification techniques can prevent identification after data breaches.[212] If templates can be created on the basis of different reference points of the some

[207] Jeroen Breebaart and others, 'Biometric Template Protection' (2009) 33 Datenschutz und Datensicherheit - DuD 299, 300.

[208] Jeroen Breebaart and others, 'Biometric Template Protection' (2009) 33 Datenschutz und Datensicherheit - DuD 299, 300.

[209] Raffaele Cappelli and others, 'Fingerprint Image Reconstruction from Standard Templates' (2007) 29 IEEE Transactions on Pattern Analysis and Machine Intelligence 1489.

[210] Sudeep Tanwa, Ethical, Legal, and Social Implications of Biometric Technologies in Mohammad Obaidat, Issa Traore and Isaac Woungang (eds), *Biometric-Based Physical and Cybersecurity Systems* (Springer 2019), 551.

[211] Anil Jain, Karthik Nandakumar and Abhishek Nagar, 'Biometric Template Security' (2008) 2008 EURASIP J. Adv. Signal Process 1, 6; Emilio Mordini and Holly Ashton, 'The Transparent Body: Medical Information, Physical Privacy, and Respect for Body integrity' in Emilio Mordini and Dimitros Tzovaras (eds), *Second Generation Biometrics* (Springer 2012), 281.

[212] Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks' in Emilio Mordini and Dimitros Tzovaras (eds), *Second Generation Biometrics* (Springer 2012), 223.

biometric identifier, affected individuals should be able to request the creation of a new template.[213] The need for strengthened protection of biometric templates is wideley recognised and even specific guidelines on the protection of biometric information during storage and transmission have been developed.[214]

3.3. Ethical issues raised by application in public spaces

3.3.1 Large-scale surveillance

a. Biometric identification and the risk of total surveillance

The (potential) use of large-scale video surveillance has raised privacy concerns long before the technical means existed to install video cameras in public (and private) places on a wide scale.[215] However, even with the instalment of CCTV cameras in more and more public places and the roll-out of the internet many of the potential privacy risks that were voiced in the last decade over large-scale surveillance[216] did not immediately materialise to their full extent. Without disregarding the efforts of democratic societies to protect the freedom and privacy of individuals, it should be pointed out that until the information age, governments and private actors simply did not have the technical possibility to effectively process the large amounts of data captured by public surveillance. Looking back from today's perspective, it can – of course, with some exaggeration – be said that governments were striking oil before inventing internal combustion engines.[217] With the increased capabilities of computers and new data analytics techniques, information from large data sets can be extracted at an unprecedented speed and combined with other personal data and therefore intensifies the privacy risks related to large scale surveillance.[218]

Remote biometric identification is one of these technological capabilities that have increased the ethical concerns regarding large scale surveillance. It allows for the identification of large numbers of individuals, in real-time, in public spaces, without any kind of cooperation on the part of the individuals identified and, maybe even more importantly, without the individuals even noticing that they are subject to surveillance. The technique as such is not particularly new and has already been used since the turn of the millennium. For example, at the Superbowl in the summer of 2001, law enforcement installed CCTV and compared the footage to a database of active warrants (the most important category), people convicted of past sexual offenses in the state of Florida, and missing children and runaway teens. If there was an 80% match, law enforcement officers confronted the individuals and asked for identification. The terrorist attacks shortly after drastically increased the deployment of CCTV in public places combined with biometric identification.[219]

Already 20 years ago concerns had been raised that the large-scale use of biometric identification goes beyond merely observing the public sphere, as the information gathered can be stored and combined

---

[213] Jeroen Breebaart and others, 'Biometric Template Protection' (2009) 33 Datenschutz und Datensicherheit - DuD 299, 302.

[214] ISO/IEC 24745:2011, Information security, cybersecurity and privacy protection — Biometric information protection available at <https://www.iso.org/standard/75302.html> (last accessed 12 July 2021).

[215] George Orwell started writing his famous book '1984' already in 1946.

[216] See for example Thomas Miller, *The Assault on Privacy* (Signet 1971), 45.

[217] To borrow a quote from Alex Garland's blockbuster 'Ex Machina'.

[218] For an overview with further references regarding the different possibilities of data analysis, see Brent Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303, 305.

[219] Philip Brey, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 Communication & Ethics in Society 97.

with other information. By aggregating disparate pieces of personal data, information can be derived that goes beyond the mere sum of the separate pieces of data. Large scale surveillance in combination with biometric identification allows to assign movements and behaviour of individuals in the public to a specific person.[220]

The concerns that were raised back then regarding large-scale surveillance of the public sphere are not only still valid today but have even more weight due the enhanced technological possibilities. The increased availability of personal images on the internet as well as the technological advancements of the past years have also changed the capabilities of biometric identification. Applications using artificial intelligence can scrape digital photographs from social media profiles and webpages and convert them into biometric templates, which are stored in databases.[221] These templates can then be combined with images from the CCTV and other relevant data such internet searches to create an elaborated profile of a person. [222]

The central issue of mass surveillance is that it interferes with the autonomy and self-determination of individuals, as they constantly have to fear that their behaviour is evaluated and scrutinised. Monitoring a society is the first step to controlling a society. First, total surveillance can effectively eliminate the fundamental rights to free speech and assembly, which ensure political participation and effective opposition in a democratic system. Based on detailed profiles about persons in combination with big data analysis, political opinions can even be predicted, and opposition against the government can pre-emptively be eliminated.[223] The effects total surveillance can have on the behaviour of an entire population become particularly apparent when looking at China's social credit score system, punishes citizens for their non-compliance with social norms.[224]

b. Surveillance by other means

While it cannot be denied that biometric identification opens up vast possibilities of large-scale surveillance, which increases the risks to fundamental rights, it needs to be noted that similar effects can result also from surveillance by other means. More and more devices of our daily use are equipped with sensors that constantly collect data about their users, such as behaviour, preferences, or location. Due to the connectivity of these devices data from various sources can be combined with each other and linked to create user profiles. Like biometric identification, this monitoring happens without any kind of cooperation on the part of the users of the devices or even without the users' knowledge.[225]

The concerns described above are not specifically related to the large-scale use of biometric identification but rather to any mass surveillance. Risks to the freedom and dignity of individuals can arise without the use of biometric technologies. Tracking people's movements, recording their conversations, analysing their use of connected devices, such as connected cars and refrigerators, to draw interferences about their behaviour and personality concern aspects of human life that are

[220] Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

[221] For an elaborate assessment of the increased possibilities of modern face recognition, see Alessandro Acquisti, Ralph Gross and Fred Stutzman, 'Face Recognition and Privacy in the Age of Augmented Reality' (2014) 6 Journal of Privacy and Confidentiality 1.

[222] Marcus Smith and Seumas Miller, 'The Ethical Application of Biometric Facial Recognition Technology' [2021] AI & Society 1.

[223] See European Parliamentary Research Service, 'The Ethics of Artificial Intelligence: Issues and Initiatives' (2020), 14.

[224] Xiao Qiang, 'President XI's Surveillance State' (2019) 30 Journal of Democracy 53.

[225] Lambèr Royakkers and others, 'Societal and Ethical Issues of Digitization' (2018) 20 Ethics and Information Technology 127, 129.

profoundly private. It can therefore be concluded that biometric identification is one element that – if abused – may enable total surveillance, but similar concerns also apply to other technologies such as AI, big data and IoT.

c. Purpose of surveillance

Whether the potential risks of modern technologies and large-scale surveillance for human dignity, autonomy and fundamental rights materialise or not depends to large extent on the purpose which is pursued by the surveillance measures. The general justification for large-scale surveillance measures by law enforcement authorities is that they serve the legitimate objective of increasing public safety and security.[226] After all, the right to life (Article 2 CFR and Article 2 ECHR) entails a positive obligation on the part of the State to take appropriate measures to safeguard life.[227] The problem is that safety is an elastic concept and does as such not prevent unjustified restrictions of freedom and autonomy of individuals. No government will deploy large scale surveillance measures explicitly with the aim to suppress its population but will rather argue that the measures are necessary for public safety. The potential risks of large-scale surveillance can be mitigated if the criteria for legitimate purposes are formulated more precisely. For example, by limiting surveillance to measures that serve a concrete objective for a substantial public interest, are consistent with fundamental rights as well as subject to judicial review and democratic scrutiny.[228]

d. Modalities of surveillance

The ethical concerns regarding the use of large-scale surveillance depend on the modalities, i.e. how and where it is used. Regarding surveillance measures in the public space, it may be argued that they are less problematic, as people accept to disclose some kind of information to others when stepping into the public space. However, it has already been pointed out that the use of biometric identification in combination with other forms of modern surveillance techniques is much more intrusive than mere observations by other people. [229] Furthermore, public spaces can often not be avoided; and the measures affect a very large number of people. Lastly, the use of large-scale surveillance in public spaces may influence how people behave and can have a chilling effect on how they exercise their fundamental rights, such as the freedom of expression or freedom of assembly.[230]

It should not be inferred from the latter point that large surveillance is less problematic if concealed because it cannot have a chilling effect. Rather the opposite is true. Awareness that covert large-scale surveillance might be used clandestinely creates a feeling of constant observation, since any place could potentially be under surveillance. The knowledge that one might be under surveillance can therefore lead to more extensive changes in behaviour than the knowledge that one is being watched in certain situations.[231]

---

[226] On difficult excise of balancing security and privacy see European Group on Ethics in Science and New Technologies (EGE), 'Ethics of Security and Surveillance Technologies' (European Commission 2014), 70.

[227] See Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania App no 47848/08 (ECtHR 17 July 2014), para 130.

[228] See also Recommendation 71 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 (2020/2012(INL)).

[229] Stephen Graham and David Wood, 'Digitizing Surveillance: Categorization, Space, Inequality' (2003) 23 Critical Social Policy 227, 228.

[230] See John Guelke, 'Surveillance: Ethical issues, legal limitations, and efficiency' (Surveille Deliverable D4.8 E, 2014), 9.

[231] Gary Gumpert and Susan J Drucker, 'Public Boundaries: Privacy and Surveillance in a Technological World' (2001) 49 Communication Quarterly 115.

Large-scale biometric identification and other surveillance measures can be targeted towards specific persons and/or limited to a certain time. For example, biometric identification in public spaces might be used for one night to locate a terrorist on the loose. The less targeted the measures, the closer they are to total surveillance and increase the risks to fundamental rights, human dignity and autonomy (see 6.3).

e. Conclusion

From all of the above, it can be concluded that the main ethical concerns associated with the actual application of remote biometric identification measures (i.e. beyond the crucial phase of enrolment of individuals) are part of the wider ethical concerns associated with modern large-scale surveillance techniques. However, these concerns are amplified by the fact that biometric identifiers cannot be changed, and technological capabilities allow to efficiently and remotely compare large amounts of data with biometric templates. While risks to individual freedom are inherent in large-scale surveillance, the dimension of ethical issues raised depend, in particular, on[232] the concrete purpose of identification, the place, manner or dimension of identification and the transparency of the identification measures taking place.

3.3.2 Stigmatisation and discrimination

Where biometric identification is used for public surveillance, individuals are assigned matching scores, which may trigger further actions, such as enhanced surveillance, identity checks by officers or even arrest (see 3.1). For a while, it was assumed that automated decision making with the help of biometric identification systems might reduce discrimination as a decision such as whether or not to arrest a particular person of colour would no longer be influenced by any potential prejudice on the part of law enforcement officers.[233] Eventually, however, the wide-scale use of biometric identification rather gave rise to its own issues of discrimination or stigmatisation. These are mostly not specific to biometric techniques but arise as part of more general deficiencies of algorithmic decision making by way of AI. While algorithmic decisions are often perceived to be objective, the code is – at the end of the day – either developed by humans or by way or training with data reflecting past human judgment, and may therefore reflect general structural inequalities.[234]

For instance, an issue that is often raised in ethical discussions regarding the use of biometric identification is the lack of accuracy of facial identification software with black faces.[235] Especially when used for purposes of law enforcement, being erroneously assigned a high matching score can have drastic consequences for the affected individuals, such as a wrongful arrest or, in the worst-case, wrongful conviction. Even if the false decision by the algorithmic system is corrected, the mere fact that one has been assigned to a stigmatising category, such as 'drug dealer', 'sex offender' or 'terrorist', can

[232] See also Ron Iphofen, 'Ethical Issues in Surveillance and Privacy' in Glyn Lawson and Alex Stedmon (eds), *Hostile intent and counter-terrorism* (CRC Press 2017), 61 who states that 'all ethical issues can be framed by asking the same sets of questions: who is doing what to whom, why and how?'.

[233] Gary Marx, 'The Engineering of Social Control: The Search for the Silver Bullet' in Ruth Peterson and John Hagan (eds), *Crime and Inequality* (Stanford University Press 1995).

[234] See Paul Henman, 'Computer Technology – a Political Player in Social Policy Processes' (1997) 26 Journal of Social Policy 323, 335.

[235] See Joy Adowaa Buolamwini, 'Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers' (2017), available at <https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf> (last accessed 12 July 2021), 30.

in itself severely affect a person's private life (on the issue of mis-categorisation based on behaviour see 5.2).

The described discrimination, however, is not rooted in the technology as such but in systemic inequalities that influence the development and/or use of biometric identification software.[236] Regarding the first point, research has shown that the face recognition software developed by Western countries recognised Caucasian faces more accurately than East Asian faces while software from East Asia yielded more accurate results for East Asian than for Caucasian faces.[237] These findings suggest that it is not technically impossible to create facial recognition software than can accurately identify different ethnicities. The functional limitations are rather caused by a lack of access to large and high-quality datasets of minorities, biases in previous research on facial recognition techniques, and/or practices and choices made by developers and coders.[238]

Discriminatory and stigmatising effects resulting from the use of inaccurate facial recognition software could be mitigated if actors using the software would acknowledge the potential biases in the development, assess them before deployment and adapt its use in the field. For instance, if facial recognition is – despite best efforts – less accurate with people of colour, the diminished accuracy must be duly taken into account when it comes to the evidentiary force ascribed to a high matching score and the possibilities of the individual to demonstrate error or identity fraud (as must any other lack of accuracy, such as where facial images are blurred because of poor light or fog). Furthermore, the reactions triggered by a high matching score should be limited to minimally invasive measures aimed at verifying the results. Since the issue of stigmatisation may result directly from the automated decision, the risks cannot immediately be mitigated by human intervention. However, it can be ensured that the data is safely stored to avoid leakages, further processing is limited, and that the data is instantly deleted if there are signs of error.

While human oversight can mitigate the risks of inaccurate and potentially discriminatory algorithmic decisions, it may reintroduce the problem of individual bias into the decision process.[239] For instance, even a perfectly accurate and unbiased recognition software will lead to discriminatory results if more weight is given to positive identifications of people of colour. This is why decision policies and the rights of the individual to challenge identification are of utmost importance to protect individuals from infringements of their fundamental rights. Any deficiencies in this regard may lead to severe unfairness or even to massive discrimination, including on racial or ethnic grounds, and to the undermining of procedural rights, including access to justice and the right to a fair trial.

---

[236] On the influence of existing systemic flaws and injustices on AI systems see European Union Agency for Fundamental Rights, 'Getting the future right – Artificial intelligence and fundamental rights' (2020), 70.

[237] Jonathon Phillips and others, 'An Other-Race Effect for Face Recognition Algorithms' (2011) 8 ACM Transactions on Applied Perception, 1.

[238] Ali Breland, 'How White Engineers Built Racist Code – and Why It's Dangerous for Black People' (*the Guardian*, 2017) available at <http://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police> (last accessed 12 July 2021); Peter Yeung, 'Biometrics Ethics: Why Facial Recognition Still Has Racial Bias' (*Raconteur*, 2020) available at <https://www.raconteur.net/technology/biometrics-ethics-bias/> (last accessed 12 July 2021).

[239] See London Policing Ethics Panel, 'Final Report on Live Facial Recognition' (2019) available at <http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/live_facial_recognition_final_report_may_2019.pdf> (last accessed 12 July 2021), 43.

4. ETHICAL ASPECTS OF BIOMETRIC CATEGORISATION

KEY FINDINGS

The main ethical issues raised by the biometric categorisation of human individuals (e.g. allocation to risk groups within an airport security system, assessment of job applicants) are related to the development and concrete use of categorisation systems. In particular, ethical issues arise in relation to the definition of categories, the associated assumptions and the conclusions or reactions triggered by the system, leading to risks such as discrimination, stigmatisation, and the drawing of inappropriate inferences. Further risks include manipulation and exploitation of vulnerabilities.

Most ethical issues raised by the use of biometric categorisation do not relate specifically to biometrics, but to, in particular

- the concrete purpose, context and conditions of categorisation;
- the degree of sensitivity of data collected and of inferences drawn;
- the accuracy of the system, the appropriateness of inferences drawn, and any control mechanisms, including human oversight;
- the gravity (including potential irreversibility) of consequences triggered by the system;
- the awareness of the individual of the categorisation and the possibility of the individual to challenge the output; and
- any storage and further processing of data for profiling purposes.

It follows that the fundamental rights risk to be addressed in this context is primarily associated with standardised profiling and/or scoring as a means to achieve a given end in a given social context. The fact that categorisation includes biometrics (e.g. that a person's age is inferred from wrinkles in their face rather than from their shopping history) adds some ethical relevance, as an individual cannot easily change biometric traits, but is not the decisive factor (as compared, e.g., with age-specific targeting that might follow categorisation). Generally speaking, biometric inferences, i.e. inferences drawn with regard to permanent or long-term physical, physiological or behavioural characteristics, may be ethically even more relevant than the use of biometric techniques as such.

4.1. Characteristic steps involved in biometric categorisation

While biometric identification normally uses 'strong' biometric identifiers to uniquely identify natural persons, biometric categorisation systems may also use 'soft' biometrics that do not, at least not as such, allow for the unique identification of a natural person, but only for the assignment of a natural person to a particular group or category of persons. Such categories may be related to features that would normally be clearly visible to a human, such as ethnicity, gender, (dis-)ability or age.[240] However, categories may also be much more sophisticated, such as relating to the concrete regional background,

[240] Irma van der Ploeg, 'Security in the Danger Zone: Normative Issues of Next Generation Biometrics' in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 288.

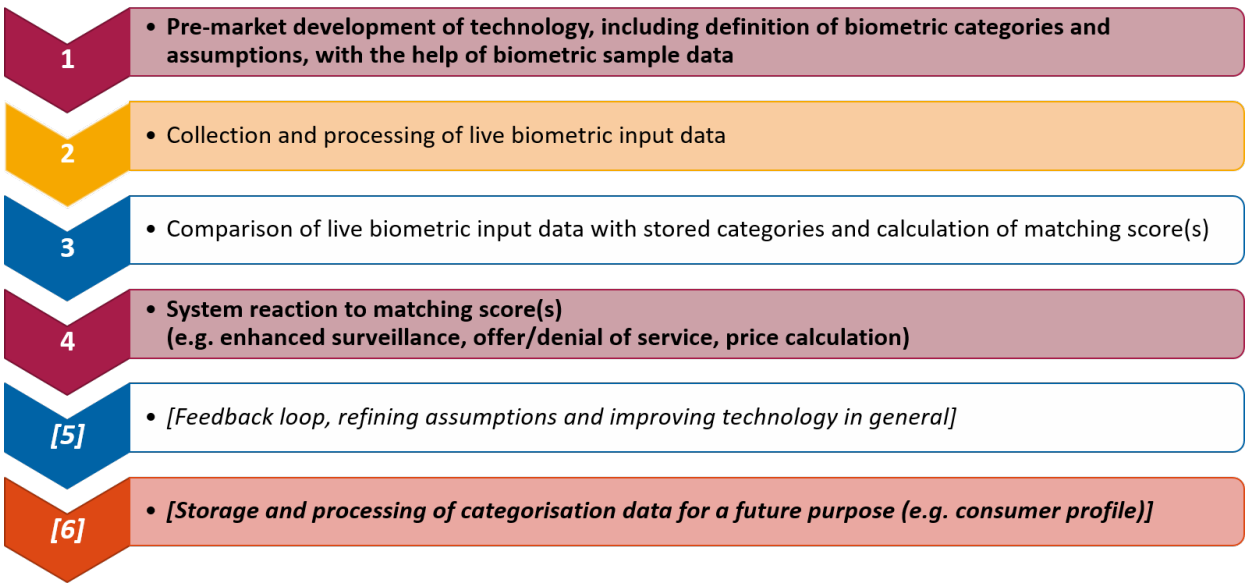
a particular risk group, or certain personality traits (in which case biometric categorisation is usually combined with detection techniques, on which see below at 5.

The characteristic steps involved in biometric categorisation deviate to some extent from the characteristic steps involved in biometric identification. Generally speaking, for biometric categorisation systems, the phase of pre-market development is ethically even more sensitive. This is so because the development phase is decisive for the definition of the biometric categories and assumptions, which are much more complex than in the case of biometric identification systems. This includes the prevention of any potentially discriminating or stigmatising effects the system might have when put into operation.

The next essential steps involved are the collection and processing of live biometric input data as well as the comparison of live biometric input data with stored categories of data and calculation of matching scores. What is still more sensitive from an ethical point of view, however, is decision policies, i.e. the system's reaction to a particular matching score, such as the making or denial of a contractual offer or the calculation of a price. These issues, however, are not very different from issues raised by algorithmic decision making in other contexts and with the help of other technologies.

Also in the context of biometric categorisation, systems may learn while already in operation, i.e. confirmed categories may lead to better training of the system. Needless to say, the ethical assessment also depends to a large extent on any storage and processing of categorisation data for future purpose, such as creating a consumer profile.

Figure 3: Steps involved in biometric categorisation



Source: Christiane Wendehorst

4.2. Ethical issues raised

A central ethical concern related to the classification of humans based on soft biometrics is that it may lead – in some form or another, intentional or not – to discrimination. Looking at it from a historic perspective, these concerns are certainly not unfounded, as the worst kinds of discrimination have often been based on what we now call 'soft' biometric identifiers. Ethical concerns, however, not only relate to discriminatory actions based on the established categories (such as filtering out job applicants based on their ethnicity or gender) but may already concern the construction of the categories. The use of automated decisions making adds another layer of ethical concerns.

The definition of certain categories can be blatantly unethical already at the outset if they are based on unscientific, discriminatory beliefs and considerations (e.g. if humans are categorised into 'superior' and 'less superior'). However, also less drastic, and more commonly used categories can be controversial from an ethical point of view. For example, the category 'race' clearly is rooted in racial thinking and needs to be seen in the light of historical and contemporary racial discrimination. More generally, concerns have been voiced that the categorisation of humans according to existing patterns of disadvantage or discrimination entails the risk of reinforcing these tendencies, even if the categorisation is based on scientific grounds and motivated by the intention of counteracting disadvantages.[241]

Grouping persons into (even uncontroversial) categories based solely on the decision of biometric recognition systems raises further ethical concerns, as the personal identifiers are only alleged. For example, a person's ethnicity, gender or disabilities, or sexuality cannot be inferred exclusively from external appearance because they are much more complex phenomena. Although most 'soft' or 'weak' biometrics are likely to persist over time, others may be open to change. The risk of misclassification may be enhanced by the fact that systems are often not trained in a 'real-world' environment and unable to cope with the variety and complexity of biometric phenomena. For example, a person's ethnicity, gender or disabilities cannot be inferred exclusively from external appearance, since they are much more complex phenomena.[242] From an ethical point of view the fact that a machine decides over the central characteristics that define who a human is purely on biometric data points can also be seen as an interference with an individual's right to self-determination.[243]

The use of biometric recognition systems to automatically categorise humans also bears the risk that the (mis)categorisation may be taken as a basis for decisions that interfere with the fundamental rights of the data subject (e.g. denial of asylum). This is particularly apparent if the decision is taken directly by the system. However, even if the final decision-maker is a human being, the categorisation made by biometric recognition systems may be seen as such strong evidence that the human will simply follow the recommendation of the automated system. For example, a system may, based on second generation biometrics, assume that a person seeking asylum is from a region that is considered a 'safe country of origin' and the responsible authority may therefore deny asylum. The overreliance on automated advice ('automation bias') and the selective acceptance of this advice when consistent with pre-existing beliefs and stereotypes ('selective adherence)', however, is not specific to biometric categorisation but rather a general problem of automated recommendations.[244]

Categorising humans based on 'soft' biometrics, such as gender, age, or ethnic background, entails the risk that past behaviour and corresponding assumptions associated with people that share the same characteristics determine whether an individual is put into a certain category.[245] This not only disregards that every individual is unique but may also reinforce existing inequalities as well as

[241] Paul Martin and others, 'Reviving Racial Medicine? The Use of Race/Ethnicity in Genetics and Biomedical Research, and the Implications for Science and Healthcare' (2007).

[242] Irma van der Ploeg, 'Security in the Danger Zone: Normative Issues of Next Generation Biometrics' in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 288.

[243] Lee Bygrave in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020), Article 22.

[244] Saar Alon-Barkat and Madalina Busuioc, 'Decision-Makers Processing of AI Algorithmic Advice: Automation Bias versus Selective Adherence' (2021) abs/2103.02381 SSRN Electronic Journal

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794660> (last accessed 12 July 2021).

[245] Aleš Završnik, Big Data, Crime and Social Control (, Routledge 2019), 196.

prejudices against certain groups. Furthermore, categories based on 'soft' biometrics may trigger discriminatory decisions, be they automated or human.[246] Even if no decisions beyond mere categorisation are taken, the fact that a person is put into a category such as 'suspect', 'criminal' or 'potential terrorist' can have stigmatising effects and severely impact the private life of affected individuals (see 5.2). Whether and to what extent these risks materialise, of course, depends on the concrete circumstances, purpose and modalities. For example, an AI that filters out, on video material, all male individuals above a certain body size and with dark hair when investigating a sexual assault on airport premises where the victim has described the person as 'male, very tall, dark hair' seems justified and not *per se* discriminatory where the purpose is further investigation (e.g. by confronting the victim with material). Putting every person who fits the description and that has been on the premises when the assault happened on a 'potential sex offenders' list, on the other hand, could certainly not be considered a proportionate mean. It also needs to be pointed out that described risks of discrimination are not caused by biometric technologies as such but rather arise as part of a more general deficiency of a system, mostly due to systemic biases (see 0).

What makes risks of mis-categorisation by algorithmic systems much more dangerous than mis-categorisation by humans is scalability. Where a human makes a mistake or takes an unreasonable decision, the next human decision maker may act more reasonably and make no or only minor mistakes. Where, on the other hand, the algorithmic system developed by one company dominates the market (be it that this company dominates the market, or that it sells its algorithm to competitors who then build their own AI system on the basis of the first one) there may suddenly be situations where almost all decisions taken in particular contexts (such as asylum or recruitment procedures) will suffer from similar deficiencies, often without sufficient possibilities to detect the deficiencies and rectify them.

Where AI and other sophisticated algorithmic systems are used for the purpose of assigning natural persons to particular categories based on their physical, physiological or behavioural characteristics, individuals are therefore exposed to risks of being subject to discrimination and misclassification. However, the underlying ethical issues are similar to those of categorisation based on other data. Challenges include the degree of human oversight, transparency, explainability of decisions, and the evidentiary force ascribed to categorisation as well as the reactions it triggers.[247] The rights of the individual to challenge automated categorisation afforded by Article 22 GDPR is an essential safeguard to ensure at least some kind of control over decisions related to categorisation.[248]

[246] See Gloria González Fuster, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights' (European Parliament 2020), 42.

[247] On the ethical principles guiding trustworthy AI see HLEG on AI, Ethics Guidelines for Trustworthy AI (2019).

[248] On the extent of this right, see Isak Mendoza and Lee Bygrave, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer 2017).

5. THE ETHICAL ASPECTS OF BIOMETRIC DETECTION

KEY FINDINGS

The main ethical issues raised by the biometric detection of human conditions (e.g. intention to commit a crime, fear, fatigue or illness) follow from its potentially intrusive nature, often analysing very intimate traits, some of them beyond the individual's consciousness. Further risks include manipulation and exploitation of detected vulnerabilities. In addition, previously unknown conditions, when revealed to the individual, may cause stress or anxiety.

Most ethical issues raised by the use of biometric detection do not relate specifically to the fact that biometric data are used for inferring a condition, but to detection of that condition as such (i.e., they are largely identical to issues raised by, for example, detection on the basis of a shopping or browsing history). Again, the fact that an individual has little control over their physical, physiological or behavioural signals, many of which will be subconscious, may give their use to detect conditions a special ethical dimension.

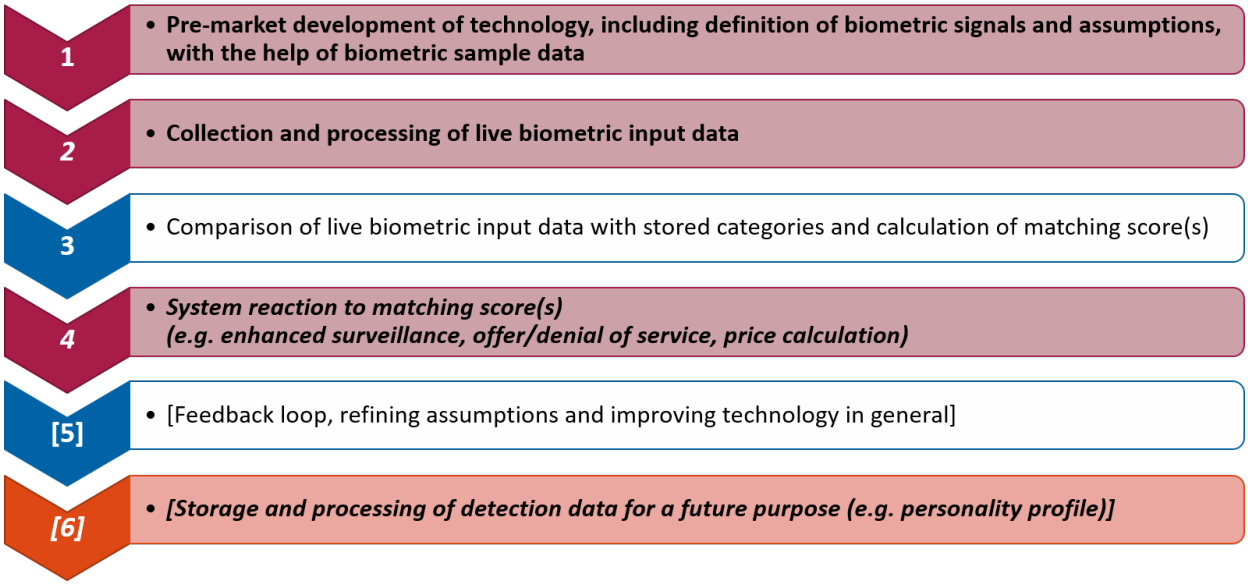
Fundamental rights risks posed by biometric detection techniques are very similar to those posed by biometric categorisation, which does not come as a surprise as conditions detected often serve as a basis for biometric categorisation. However, within the field of biometric detection systems, it is systems detecting human emotions, thoughts and intentions that deserve particular attention from an ethical and regulatory perspective, potentially calling for a new set of 'neuro-rights' (such as the right to mental privacy and mental integrity).

5.1. Characteristic steps involved in biometric detection

The characteristic steps involved in biometric detection coincide to a large extent with the steps involved in biometric categorisation (see above at 4.1). This does not come as a surprise because biometric categorisation and biometric detection are closely linked with each other, and the biometric detection of certain conditions (e.g. a particular health condition) is often the basis for assignment of natural persons to particular categories (e.g. persons with disabilities). As in the case of biometric categorisation systems, the development phase is a crucial phase, defining which bio-signals lead to what kind of assumptions. Also the reactions triggered by the system are again of utmost ethical relevance.

Given that biometric detection is often about very intimate conditions, including emotions, thoughts and intentions of a natural person, the collection and processing of live biometric input data tends to be ethically much more problematic than in most situations where biometric categorisation is used. Ultimately, collecting this kind of input data may raise issues of human dignity, integrity of the human self, and mental privacy. However, it is difficult to make any general statements about different degrees of ethical sensitivity, as context and purposes of both biometric categorisation and biometric detection may vary to a great extent.

Figure 4: Steps involved in biometric detection



Source: Christiane Wendehorst

5.2. Ethical issues raised

The development of biometric detection techniques was driven by the desire not only to identify persons but also to predict whether they are a potential threat. Large scale surveillance coupled with biometric identification are of no help preventing a terrorist smuggling a bomb onto a plane unless the terrorist is already on some kind of watch-list. The use of second-generation (or behavioural) biometrics, such as gait, face dynamics, heart rate, eye movements or body temperature allows to draw conclusions about a person's state of mind and to predict future actions and behaviour.[249] While the identification and categorisation techniques ask the questions 'Who are you?' or 'To which group do you belong?', detection techniques ask 'How are you?' and 'What are you going to do?'. [250]. In most instances, detection will be coupled with some kind of automated categorisation based on the conclusion and predications, such as 'potential aggressor' or 'potential threat'.[251] As second-generation identifiers generally allow drawing inferences about human behaviour, they have a broad field of application, such as targeted marketing or for calculating insurance premiums, and are not limited to law enforcement and security purposes.[252]

What characterises second-generation identifiers is that although humans may be able to exercise some kind of control over them, they are in most situations controlled by the subconscious. This is also what distinguishes second-generation biometrics from other behaviour, such as online activities or shopping behaviour, which – together with other data – may also be used to predict actions of data subjects.[253] For example, nervous motions together with increased heart rate and respiration in the

[249] Paul McCarthy, in Ruth Chadwick (ed), Encyclopedia of Applied Ethics (Elsevier Science 2012), 288.

[250] Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks' in Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012), 288.

[251] Paul McCarthy, in Ruth Chadwick (ed), Encyclopedia of Applied Ethics (Elsevier Science 2012), 293.

[252] ENISA, 'Behavioural Biometrics' (2010) available at <https://www.enisa.europa.eu/publications/behavioural-biometrics> (last accessed 09 July 2021).

[253] On the possibility of big data analytics to draw inferences about individuals and groups see Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' [2019] Columbia Business Law Review 494.

security line at the airport may suggest malicious intentions of an individual based on behavioural biometrics. However, the analysis of social media profiles together with data about purchases of explosive materials and internet searches may also be used to predict dangerous behaviour but is not based on any second-generation biometrics. However, the distinction between behavioural biometrics and other behaviour is not clear-cut, and often they will be combined to provide an even more comprehensive analysis of an individual's intentions (see 6.6). The way in which behavioural biometrics can be utilised and the conclusion that can be drawn from them depend on the specific biometric features. However, many biometrics such as gait or facial expression dynamics do not require contact or participation from the individual and may even be captured from a distance, increasing the risk that individuals are analysed without their knowledge.[254]

It has already been pointed out that even first-generation biometrics facilitate the creation of profiles that are more detailed than the sum of the individual pieces of information, giving deep insights into a person's private life (see 3.3). Detection techniques amplify this ethical issue, as profiles of individuals can be supplemented with data about their intentions and future behaviour. Furthermore, detection techniques may reveal highly private information such as personal health issues and disabilities that have previously not been known to the relevant persons themselves. This often gives rise to another ethical dilemma as, on the one hand, the affected person has a right to receive full information on the outcome of biometric detection, but on the other hand, informing the affected person of the condition without their consent may interfere with their right to not know.[255]

The most central ethical issue, however, is that analysing biometric identifiers may provide indications about a human's intent, inner motivation or planned actions but are never hard proof. In contrast to inferences from first-generation biometrics about a person's identity, the results of behavioural recognition cannot be fully verified. For example, the results of fingerprint matching can be verified using DNA comparison. While there are biometric stress indicators that suggest a person is not telling the truth, individual baselines vary widely, and there are no means to confirm the conclusion that a person is in fact lying. Therefore, suspicious indicators alone should not be taken as proof, and should not even shift the burden of proof to the relevant person, but only as a basis for, e.g., making further investigation.[256]

Moreover, basing decisions on second-generation biometrics collected in public spaces may have severe chilling effects on society, as people may adapt their behaviour based on assumptions about what could be viewed as suspicious by biometric detection systems.[257]Also, the unreliability of detection techniques increases the risk of persons being put in stigmatising categories, which again may change people's behaviour in public places.

(Mis)categorising a person as 'potential terrorist' not only entails the risk of being the subject of law enforcement measures, but also that of drastic reputational damage if this false assumption is leaked. Once the information is public, stigmatisation of such kind may persist even if the mistake is corrected. The longer a person is associated with a classification, the 'stickier' the assumptions associated with the

[254] Margit Sutrop and Katrin Laas-Mikko, 'From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics' (2012) 29 Review of Policy Research 21, 27.

[255] Irma van der Ploeg, 'Security in the Danger Zone: Normative Issues of Next Generation Biometrics' in Emilio Mordini and Dimitrios Tzovaras (eds), *Second generation biometrics: the ethical, legal and social context* (Springer 2012), 294.

[256] Margit Sutrop and Katrin Laas-Mikko, 'From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics' (2012) 29 Review of Policy Research 21,33.

[257] Irma van der Ploeg, 'Security in the Danger Zone: Normative Issues of Next Generation Biometrics' in Emilio Mordini and Dimitrios Tzovaras (eds), *Second generation biometrics: the ethical, legal and social context* (Springer 2012), 295.

relevant category become.[258] It is therefore of outmost importance that biometric profiles are protected by high security standards and are regularly reviewed and updated.

[258] Günter Schumacher, 'Behavioural Biometrics: Emerging Trends and Ethical Risks' in Emilio Mordini and Dimitros Tzovaras (eds), *Second Generation Biometrics* (Springer 2012), 223

6. CONCLUSIONS WITH REGARD TO THE PROPOSAL FOR AN ARTIFICIAL INTELLIGENCE ACT

KEY FINDINGS

The ethical analysis of issues raised by biometric techniques calls for a number of changes in the AIA Proposal as it currently stands.

The definitions in Article 3 should be amended:

- The definitions of 'emotion recognition system' and 'biometric categorisation system' should be detached from the concept of 'biometric data' as defined in the GDPR and rather based on a new definition of 'biometrics-based data';
- The definitions of 'remote' and 'real-time' with regard to biometric identification should be slightly modified.
- An additional definition for 'biometric inferences' should be introduced;

Title II on prohibited AI practices should be amended:

- The current Article 5(1)(d) and (2) to (4) on real-time remote biometric identification should be removed from Article 5 and transferred to a new Title IIa on 'restricted AI practices';
- The list of prohibited AI practices in Article 5(1) should be enriched, at least, by a prohibition of total or comprehensive surveillance of natural persons in their private or work life and of infringements of mental privacy and integrity (further extensions being beyond the scope of this Study);
- The Commission should have the possibility to adapt the list of prohibited AI practices periodically, potentially under the supervision of the European Parliament;
- There should be a clarification that prohibitions following from other laws (such as data protection or consumer protection law) remain unaffected.

A new Title IIa on 'restricted AI applications' should be inserted:

- The new Title IIa should deal with 'real-time' remote biometric identification (or even with other forms of real-time remote identification) in a more comprehensive way, without limitation to law enforcement purposes;
- It should also include a provision on other biometric identification systems, emotion recognition systems and biometric categorisation systems, limiting the admissibility of such systems and integrating the transparency obligation which is currently in Article 52(2);
- Title IIa should likewise include a new provision on decisions based on biometric techniques
- Title IIa might possibly also include provisions that put substantive limits to the drawing of biometric inferences and provide for automated consent management.

Annex III point 1 should be extended so as to cover emotion recognition systems in (at least) the same way as biometric categorisation systems.

The ethical analysis of biometric identification, categorisation and detection suggests that the main conclusions in legal terms should be drawn with regard to the further development of the Proposal for an Artificial Intelligence Act (AIA Proposal)[259]. There are also other legislative initiatives that are currently in the pipeline, including a potential revision of the GDPR,[260] the E-Privacy Regulation,[261] the Digital Services Act,[262] the Digital Markets Act,[263] the Data Governance Act[264] and the Data Act[265]. Among these initiatives it would arguably only be a revision of the GDPR that might specifically address biometric techniques in the context of Articles 9 or 22 GDPR. However, there seems to be currently very little appetite for significant changes of the GDPR. Given that the AIA Proposal already contains provisions on biometric techniques and that it is currently being considered by the European Parliament and other EU institutions, this study restricts itself to evaluating the AIA Proposal and to submitting suggestions for its further development.

6.1. General approach of the AIA Proposal

6.6.1 Biometric techniques and the risk-based approach

The AIA Proposal takes a risk-based approach, dividing AI systems into four different risk levels: unacceptable risk (Title II – prohibited AI practices), high risk (Title III), transparency risk (Title IV), and other AI systems which do not require specific legislation in the light of the minimal degree of risk they pose.

Biometric techniques may be assigned, depending on their nature and the context in which they are used, to any of the four risk levels.

Particular forms of biometric identification, namely biometric identification that occurs remotely in publicly accessible spaces, in real-time, and for law enforcement purposes, are included in the list of **'prohibited AI practices'** and dealt with under Article 5 (1)(d) and (2) to (4) of the AIA Proposal. However, at a closer look, they are not prohibited *per se* under these proposed provisions, but permitted only under certain conditions.

The main part of the AIA Proposal is devoted to **'high-risk' AI systems**. This is where the full set of mandatory requirements listed under Title III and the requirement of ex ante conformity assessment apply. The AI systems that qualify as high-risk systems are partly defined by Article 6(1) in conjunction with particular product safety legislation listed in Annex II, and partly in Annex III, which may be extended or otherwise modified according to criteria explained in Article 7. Biometric techniques are covered by the current version of Annex III as follows:

[259] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final

[260] See, e.g. European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)).

[261] See mandate for negotiations with EP of 10 February 2021, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Council Document no. 6087/21.

[262] Proposal for a Regulation, COM(2020) 825 final.

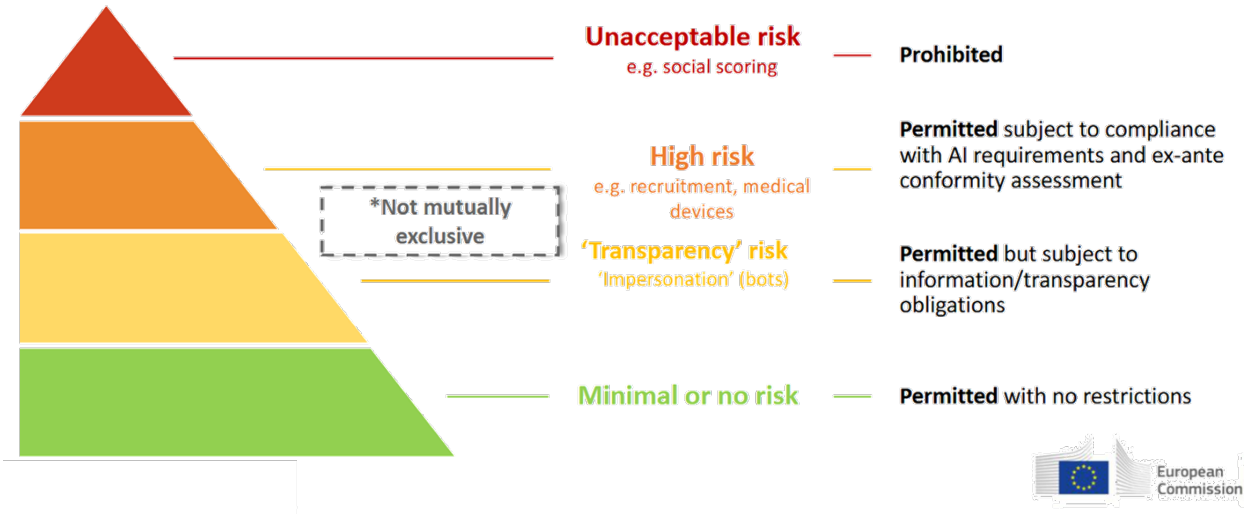
[263] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

[264] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

[265] See schedule at https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.

- According to Annex III 1(a), all AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons always qualify as high-risk AI systems, irrespective of the context in which they are used.
- The category of high risk AI systems also includes, according to Annex III 6 (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, i.e. a particular case of biometric detection. The same applies, according to Annex III 7 (a), where such AI systems are used by competent public authorities for purposes of migration, asylum and border control management.
- Annex III 6 (e) qualifies as high risk 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, i.e. a particular case of what may possibly include biometric categorisation.

Figure 5: Risk-based approach of the AIA Proposal

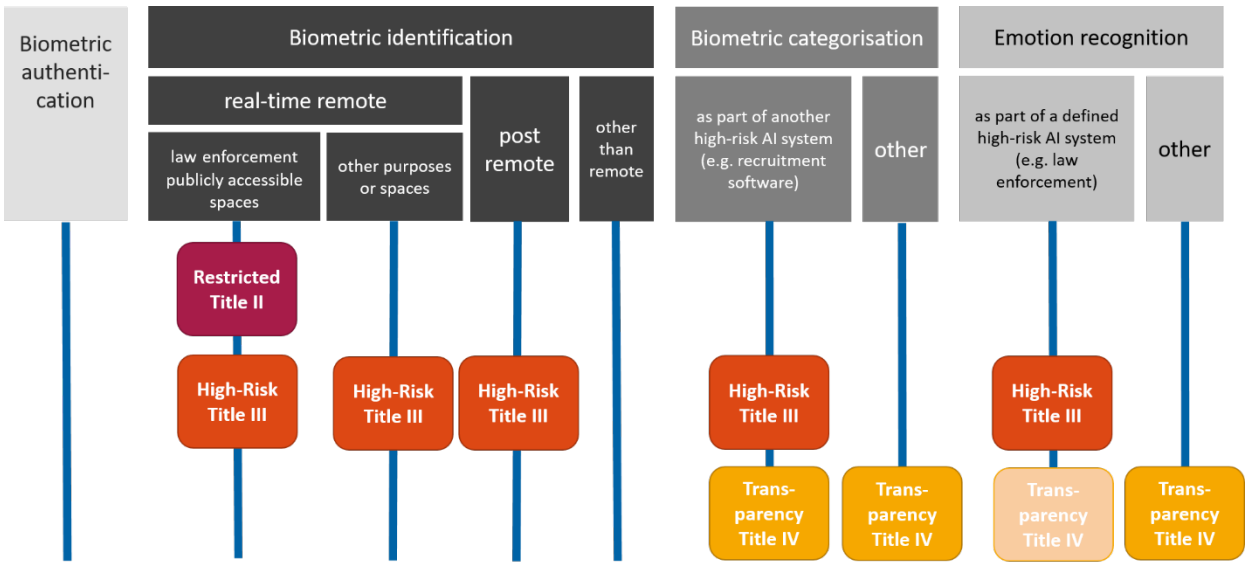


Source: European Commission, DG CNCT

Beyond the biometric techniques qualified as 'high-risk' within the meaning of Title III, some biometric techniques are also referred to under Title IV, which deals with AI systems posing a particular **'transparency risk'**. According to Article 52(2) of the AIA Proposal, emotion recognition and biometric categorisation systems call for a particular transparency measures, which is why the user of such systems must inform those exposed to it of the operation of the system.

It is important to stress that the risk levels are **not mutually exclusive**. This means that a real-time remote biometric identification system dealt with under Title II (and not already prohibited by that Title) must, at the same time, fulfil all the requirements under Title III. In a similar vein, emotion recognition systems and biometric categorisation systems are normally only subject to Title IV, but where they qualify, in the light of their concrete purpose, as a high-risk system, they must also fulfil the requirements listed in Title III.

Figure 6: Biometric techniques under the risk levels of the AIA Proposal



Source: Christiane Wendehorst

Within Title III, there are several provisions that apply specifically to biometric techniques. Article 10(4) provides that, for biometric identification and categorisation systems, **logging capabilities** shall provide, at a minimum, recording of the period of each use of the system (start date and time and end date and time of each use), the reference database against which input data has been checked by the system, the input data for which the search has led to a match, and the identification of the natural persons involved in the verification of the results. Article 14(5) provides that, for such systems, human oversight measures shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and **confirmed by at least two natural persons**.

It is also important to note that, while stand-alone high-risk AI systems are normally subject to a **conformity assessment** that is implemented through internal control checks by the providers, remote biometric identification systems are mostly subject to third party conformity assessment, cf. Article 43(1).

6.1.2 Interplay of the AIA Proposal with other EU legislation

The AIA Proposal does not deal with AI systems in an exhaustive way. This is obvious, in particular, when it comes to **data protection law**. As far as AI systems require the processing of data as training, validation and testing data or, even more importantly, as input and output data, Union and Member State data protection law must apply to the extent that there is no more specific rule under the AIA Proposal that derogates general data protection law. Given that the definition of 'biometric data' coincides with the respective definition under the GDPR and that the majority of definitions referring to biometric techniques under the AIA Proposal is based on the definition of biometric data, there is a strong link between the AIA Proposal and relevant data protection law. This is in particular the GDPR

and national provisions implementing the LED,[266] but to a certain extent also the EUDPR[267] as well as national provisions implementing the E-Privacy Directive.[268]

In essence, this means that, on top of compliance with the requirements under the AIA Proposal, processing of input and output data must occur in conformity with the GDPR, the LED or other applicable data protection law.[269] Restrictions on the use of biometric techniques may therefore have their origin in the 'data perspective' as well as in the 'AI perspective', and both types of restrictions may have the same or a similar effect, while referring to different concepts and categories.[270]

The following table illustrates the way in which the AIA proposal and data protection law interact when it comes to the admissibility of particular practices, indicating whether the GDPR, the LED and the AIA would normally allow a particular practice.

Table 1: Admissibility of biometric techniques (based on simplified assumptions)

AI Application	GDPR	LED	AIA
1. Police uses real-time remote biometric identification to trace down a terrorist	n.a.	Yes	Yes*)
2. Police uses real-time remote biometric identification to create mobility profiles of the population and detect anomalous behaviour	n.a.	MS law	No
3. Company operating an airport uses real-time remote biometric identification on airport premises	MS law	n.a.	Yes
4. Owner of residential premises applies remote biometric identification to people passing by on the street	No	n.a.	Yes
5. Asylum authorities use biometric categorisation system for age-verification of juvenile migrants	Yes	n.a.	Yes*)
6. Police uses biometric categorisation for targeted surveillance of individuals with a particular ethnic origin (and without any further justification)	n.a.	No	Yes*)

[266] 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, p. 89–131.

[267] 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, 39-98.

[268] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 37-47.

[269] Cf. Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (pre-print - SocArXiv Papers 2021) available at <https://osf.io/preprints/socarxiv/38p5f> (last accessed 09 July 2021), 8.

[270] Data Ethics Commission of the Federal Government, 'Opinion of the Data Ethics Commission' (2019) available at <https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf> (last accessed 09 July 2021), 77.

7. Provider of video game uses biometric categorisation for age-verification of gamers for child protection purposes	Simple consent	n.a.	Yes
8. Store uses biometric categorisation of customers (e.g. according to age groups) for targeted economic exploitation of vulnerabilities	Simple consent	n.a.	Yes
9. Police uses emotion recognition system during interrogation of suspect	n.a.	Yes	Yes*)
10. Statistics authorities use emotion recognition in voting booths to find out about people's attitude towards democracy (e.g. anger, satisfaction)	MS law	n.a.	Yes
11. Q&A chat-bot uses emotion recognition to react appropriately to very dissatisfied customers	Yes	n.a.	Yes
12. Social network uses emotion recognition (detecting fear, anger and other emotions) for targeted political advertising, exploiting individual vulnerabilities.	Simple consent	n.a.	Yes

n.a.= not applicable MS = Member State *) = but high-risk, i.e. Title III AIA applies

Source: Christiane Wendehorst

The Table, which includes desirable as well as undesirable practices, demonstrates how data protection law on the one hand and the AIA Proposal on the other serve similar functions by **'filtering out' certain undesirable practices**. However, due to its very cautious regulatory approach and the narrowness of most of its provisions, the AIA Proposal only filters out very few undesirable practices. These are practices in the context of law enforcement that use real-time remote biometric identification and where there is no particularly strong justification in terms of gravity of an offence etc. for a certain practice (see illustration no. 2). Other undesirable practices are either filtered out by data protection law (see illustrations nos. 4 and 6) or not at all. Undesirable practices that are not filtered out at all include practices that do not use biometric data within the narrow definition of the GDPR (i.e. data that are suitable for allowing or confirming the unique identification of a natural person). Such practices are subject to simple consent within the meaning of Article 6(1)(a) GDPR as contrasted with explicit consent under Article 9(2)(a) GDPR, which often does not mean a very high threshold in the light of information overload and a tendency of most people to click on 'OK' buttons (see illustrations nos. 8 and 12).[271] Also, Member States have quite some leeway in defining public interests in a way that allows for AI applications posing significant fundamental rights risks, including a high potential for 'function creep' (see illustration no. 10).

Needless to say, there is also other Union and Member State law in place that could help 'filtering out' undesirable practices. For instance, if racial profiling in illustration no. 6 were not prohibited by Article 11 LED it would arguably be directly in violation of fundamental rights, and possibly also of **non-discrimination law** and other law at Member State level.

[271] Giovanni Sartor, Francesca Lagioia and Federico Galli, 'Regulating Targeted and Behavioural Advertising in Digital Services' (2021 European Parliament), 103.

Likewise, exploitation of consumer vulnerabilities in illustration no. 8 should be qualified as an **unfair commercial practice** within the meaning of the Unfair Commercial Practices Directive (UCPD)[272] and be considered illegal under the rules implementing the UCPD. In this context, it is, however, deplorable that also the most recent revision of the UCPD,[273] which was designed to modernise the UCPD in the light of new digital developments, fails to include such forms of exploitation of vulnerabilities in the blacklisted practices.

However, there are always gaps, i.e. **undesirable practices that are not addressed by any body of law**, such as exploitation of vulnerabilities to manipulate voting behaviour in illustration no. 12. This is not covered by the UCPD as the user does not make any economic decisions with regard to the political advertising. It is potentially covered by the future Digital Services Act, but in a very 'soft' manner, as part of online advertising transparency (Article 24) or of new provisions on recommender systems used by very large online platforms (Article 29). Likewise, where customers in illustration no. 8 are not consumers, but owners of small or even very small businesses, they are not protected by provisions implementing the UCPD, so whether or not there may be any sort of protection largely depends on national law and general doctrines such as *culpa in contrahendo*.

6.2. Recommendations with regard to definitions

6.2.1 Biometric data and biometrics-based data

The definitions of 'biometric identification system', 'biometric categorisation system' and 'emotion recognition system' all build on the **definition of 'biometric data'**. This definition, in turn, has been copied from Article 4(14) GDPR and is defined as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of the natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'. Recital 51 of the GDPR clarifies that, e.g., 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.

While it is certainly essential to stress the requirement of specific technical processing (for, otherwise, almost any everyday activity might potentially be covered), the requirement that the data must allow or confirm the unique identification of a natural person makes the definition **far too narrow**. It essentially reflects the dominant concepts during times of 'first generation biometric technologies' and **fails to keep pace with technological developments** (see above at 0 and 0). This means that biometric categorisation systems and emotion recognition systems are covered only if they are based on data that would allow or confirm the unique identification of the natural person concerned. By way of contrast, an emotion recognition system based on pulse frequency, body temperature and non-unique facial expressions (such as smiling, raising of the brow or yawning) or non-unique voice signals (such as volume or trembling) would not be covered by the definition of emotion recognition system

[272] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ L 149, 22-39.

[273] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules OJ L 328, 7-28.

under the AIA. This is so simply because the data used would not qualify as biometric data in the narrow sense.

There would be three different possibilities to solve this problem:

- the definition of 'biometric data' could be modified so as to be no longer identical with the respective definition in the GDPR; or
- the definitions of 'biometric categorisation system' and 'emotion recognition system' could be defined without reference to any particular type of data; or
- a new definition of, e.g., 'biometrics-based data' (formulation to be discussed) could be included, to which the definitions of 'biometric categorisation system' and 'emotion recognition system' would then refer.

At the end of the day, the third option seems to be the least disruptive one, which is why it is suggested to include a **new definition of 'biometrics-based data'**. This definition would largely coincide with the definition of biometric data, but would differ from that definition in that biometrics-based data may or may not allow or confirm the identification of a natural person. It is important to stress that there would still be the requirement of specific technical processing, i.e. a video showing a person who is smiling would not amount to biometrics-based data, but the use of specific analytic tools that tell a smiling person from a person in a different mood would qualify as biometrics-based data.

Illustration 1: Differentiating biometrics-based data and other personal data

When customers call the helpline of company H they are prompted to state the reason why they are calling. Their oral statement is analysed by an AI system that (a) is a natural language processing (NLP) system analysing the content of the statement, such as whether the customer has a question or is complaining, or (b) analyses the customer's voice with regard to pitch, volume, trembling, accent etc. in order to find out about the customer's background and emotions, both (a) and (b) with the aim of allowing a chat-bot to react in a very targeted way. While data used by the AI system in (b) are biometrics-based data, the data used by the AI system in (a) are not.

Source: Christiane Wendehorst

The Illustration also shows that the fact an AI system uses biometrics-based data says little about the purpose and 'level of criticality' of that data use, i.e. the same or very similar effects as can be achieved with the help of biometrics-based data can often be achieved with the help of other data. However, it is still advisable to create provisions specifically for AI systems using biometrics-based data as otherwise the scope of provisions would become very fuzzy and too much uncertainty would be created (for a recommendation on biometric inferences see, however, below at 0 and 6.6). Also, use of biometrics-based data raises very specific and additional ethical concerns, due to the fact that a person cannot easily change such data, that justify stricter regulation.

To summarise, it is suggested to phrase the definition as follows:

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

[…]

(33) 'biometric data' means 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;

(33a) 'biometrics-based data' means personal data resulting from specific technical processing relating to physical, physiological or behavioural signals or characteristics of a natural person, such as facial expressions, movements, pulse frequency, voice, keystrokes or gait, which may or may not allow or confirm the unique identification of a natural person;

6.2.2 Real-time and post remote biometric identification

Also the definition of biometric identification systems (as contrasted with, in particular, biometric authentication or verification systems) may need to be slightly modified.

Article 3(36) defines a 'remote biometric identification system' as an AI system 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. The drafters of this definition obviously found the absence of prior knowledge whether the person identified will be present or not to be the decisive factor that makes identification techniques different from authentication or verification techniques. However, it seems questionable whether this is in fact the decisive factor. Arguably, one can speak about identification (i.e. a 'one to many' matching exercise) also where the person using the AI system knows that a particular person identified will be present. For instance, where remote biometric identification is used on company premises for the monitoring of employees (i.e. in order to know where employees have spent their day and to analyse their movements) the identity of the employees and that they will most likely be identified by the system is well known. It should therefore be considered to focus more on the fact whether or not the persons to be identified **consciously cooperate** for authentication purposes, e.g. by putting their thumb onto the fingerprint scanner at the entrance of a room. Admittedly, this modification is a matter of rather low priority.

What seems more important is a modification of the definition of 'real-time' biometric identification system. Article 3(37) defines a **'real-time'** remote biometric identification system as a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. The definition further clarifies that this comprises not only instant identification, but also limited short delays in order to avoid circumvention. However, whether or not there is a delay, and the length of that delay, can hardly be the decisive factor. Where all people walking down a particular street are constantly being filmed, but the video material is analysed (and the identities of the people walking by established with the help of biometric identification systems) only on the next day, the risks for fundamental rights are almost as high as if the data were analysed on the same day. What seems to be the decisive factor, rather, is whether surveillance by means of biometric

identification occurs **on a continuous basis or otherwise on a large scale** over a period if time and without focus on a particular past incident.

Illustration 2: Differentiating 'real-time' and 'post' remote identification

Source: Christiane Wendehorst

To summarise, it is suggested to modify definitions as follows:

Video surveillance is in action at various points on High Street. Video material is stored for 24 hours and then deleted. It is streamed in real time to police headquarters, where policemen can watch the scenes on High Street if required, and analysed in real time by an AI system trained to recognise incidents (such as violence or accidents) that require police action. In particular where a crime has been committed, the police would analyse the video material with the help of biometric identification techniques, checking whether the offender's live template matches with any template in an existing database. This should not qualify as 'real-time' remote identification even where the delay between recognition of the incident and biometric identification of the offender is minimal. Rather, this should be a case of 'post' biometric identification. On the other hand, if the video material is analysed, after 23 hours, to identify all the participants in a particular demonstration, this should count as 'large scale' and therefore fall under the definition of 'real-time' despite the significant delay.

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

[…]

(36) 'remote biometric identification system' means an AI system 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 **the conscious cooperation of the persons to be identified** ~~prior knowledge of the user of the AI system whether the person will be present and can be identified~~ ;

(37) ''real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification ~~all~~ occur **on a continuous or large-scale basis over a period of time and without limitation to a particular past incident (such as a crime recorded by a video camera);** ~~without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~

6.2.3 Emotion recognition and biometric categorisation

Some further modifications are recommended as far as the definition of emotion recognition system is concerned. First of all, in line with what has been stated earlier (see above at 0), the definition should not refer to 'biometric data', but to **'biometrics-based data'**. Furthermore, the list of conditions to be detected could be extended and should, at least, include **'thoughts'**. This is essential because many brain-computer-interfaces (BCI) will indicate thoughts (such as where a person is thinking of food or

drink) rather than emotions (such as joy, fear or anger) or intentions (such as the intention to stand up or walk).

Similar considerations as for biometric categorisation systems also apply to biometric categorisation systems. The definition should not refer to the very narrow notion of 'biometric data', but to the new and broader concept of 'biometrics-based data'. Also, the **indicative list of categories** seems to be not ideal as it focuses too much on categories which every human could easily assign at first sight. This is why it is recommended to add 'health, mental ability and behavioural traits' to the indicative list of biometric categories.

To summarise, this would mean changing definitions as follows:

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

[…]

(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions**, thoughts** or intentions of natural persons on the basis of their ~~biometric~~**biometrics-based** data;

(35) 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories such as sex, age, hair colour, eye colour, tattoos, ethnic origin**, health, mental ability, behavioural traits** or sexual or political orientation, on the basis of their ~~biometric~~**biometrics-based** data;

6.2.4 Biometric inferences

The definition of biometric categorisation system relies on the types of data used, while it is irrelevant whether the category itself is of a biometric nature or not. However, it is clear that also the opposite situation is ethically relevant and may require to be addressed within the AIA, i.e. where personal data of any kind, biometrics-based or not, are used to draw inferences with regard to **permanent or long-term physical, physiological or behavioural characteristics** of a natural person. This deserves to receive a definition (and further provisions) of its own. It is important to note that biometric categorisation and biometric inferences overlap to a great extent, i.e. biometric categorisation may of course lead to biometric inferences.

Illustration 3: Relationship between 'biometric categorisation' and 'biometric inferences'

The conclusion that a natural person is suffering from depression, or is very susceptible to depression, is a conclusion that relates to long-term physical, physiological or behavioural characteristics of a natural person and that therefore qualifies as a biometric inference. Where that conclusion has been drawn on the basis of data such as posts in social media in which the person expressed suicidal intentions, and frequent searches on the internet for keywords such as 'depression', the practice of drawing the conclusion does not qualify as biometric categorisation. Where, however, the conclusion has been drawn on the basis of keystroke and gait patterns and the analysis of facial expressions, the practice qualifies both as biometric categorisation and as drawing of biometric inferences.

Source: Christiane Wendehorst

It is therefore recommended to add a definition of 'biometric inferences', which could be phrased as follows:

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

[…]

(35a) 'biometric inferences' mean conclusions with regard to permanent or long-term physical, physiological or behavioural characteristics of a natural person, on the basis of biometrics-based data or other personal data;

6.3. Recommendations with regard to Title II

6.3.1 Differentiating between *per se*-prohibitions and restrictions

Upon closer inspection, the rules on real-time remote biometric identification seem to be an **alien element within Title II**, which is about 'prohibited AI practices'. While Article 5(1)(a) to (c) address AI practices that are clearly incompatible with European values and that should therefore be prohibited under all circumstances, Article 5(1)(d) and (2) to (4) on real-time remote biometric identification is not about a *per se* prohibition. Rather, those provisions contain a number of significant restrictions as well as conditions under which the use of real-time remote biometric identification systems for law enforcement purposes in publicly accessible spaces should be allowed.[274] It is therefore suggested to remove paragraphs (1)(d) and (2) to (4) from Article 5 and to include them in a **new and separate Title IIa** (eventually to become Title III after re-numbering) which should be devoted to 'restricted artificial intelligence practices'.

6.3.2 Adding total surveillance and infringements on mental privacy and integrity as prohibited AI practices

In the light of the fact that the major ethical issue raised by real-time remote biometric identification is the aspect of surveillance, it is suggested to add **total surveillance** as an **additional prohibited AI practice**. The prohibition should be restricted to surveillance in natural persons' private or work life (so as not to capture situations such as the surveillance of passengers on airport premises). In line with some of the other prohibited AI practices listed in Article 5(1), and in order not to create a rule that is overreaching, the prohibition should be restricted to cases where the surveillance would cause, or be likely to cause, the affected natural persons physical or psychological harm.

In addition, infringements on mental privacy and integrity through BCIs by direct or remote measurement and/or manipulation of brain data should be added as a prohibited AI practice. This does not automatically mean a ban on polygraphs and other biometric detection systems that are used for inferring a person's thoughts or intentions, but only where such systems use specific technical

[274] It is, of course, possible to say that any kind of mandatory restriction or mandatory requirement amounts to a prohibition of practices that are not in compliance with restrictions or requirements. However, this is true for most regulatory regimes, and it is clearly not the spirit in which Article 5(1)(a) to (c) have been formulated.

processing of brain data, such as brain waves. Needless to say, where such measurement or manipulation occurs for medical reasons (e.g. for the steering of exoskeletons that assist a person in moving limbs), for research purposes or otherwise in accordance with the person's (free) will it cannot be covered by a prohibition. This is why the prohibition should only apply where the use occurs against the relevant person's will or in a manner that causes or is likely to cause that person or another person physical or psychological harm. It should be noted that 'against the will' is not identical to 'without the will'. Hence, the use of BCI for treating unconscious patients would of course not be prohibited.

The new Article 5(1)(d) could therefore read as follows:

Article 5

1. The following artificial intelligence practices shall be prohibited:

[…]

(d) **the putting into service or use of an AI system for the comprehensive surveillance of natural persons in their private or work life to an extent or in a manner that causes or is likely to cause those persons or another person physical or psychological harm**; ~~the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives […]:~~

(e) the placing on the market, putting into service or use of an AI system for the specific technical processing of brain data in order to read or manipulate a person's thoughts against that person's will or in a manner that causes or is likely to cause that person or another person physical or psychological harm.

[…]

6.3.3 Allowing for flexible adaptation of the list of prohibited AI practices

Given the fast pace at which technology is developing it strikes as somewhat odd that there is **inbuilt flexibility** in most of the provisions of the AIA Proposal, but not with regard to the prohibited AI practices in Article 5. For most of the central parts of the AIA, including with regard to the definition of artificial intelligence system (Annex I), the list of AI systems covered by safety legislation and posing a high safety risk (Annex II), and the list of other high-risk AI systems (Annex III), the European Commission may adapt the instrument to changes in the technological landscape, without having to initiate a regular legislative procedure. There seems to be no justification for 'carving in stone' (i.e. allowing for changes only in a regular legislative procedure) precisely the list of prohibited AI practices in Article 5.

It is therefore suggested to add a new Article 5(2) that would replace the previous paragraph with that number and that might be formulated as follows:

Article 5

[…]

2. In addition to the prohibited AI practices referred to in paragraph (1), AI practices referred to in Annex Ia shall also be considered prohibited. The Commission is

empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex Ia on the basis of a similar threat to fundamental rights and European values as posed by the practices listed in paragraph (1).

[…]

6.3.1 Clarifying the relationship with prohibitions following from other laws

Clearly, those who drafted the AIA Proposal have done so with the intention to fill gaps in existing legislation, but at the same time to avoid any sort of overlap with existing legislation. For instance, the prohibition of manipulation and exploitation of vulnerabilities was restricted to practices that cause physical or psychological harm, while omitting manipulation and exploitation that causes economic harm, as the latter would have been too close to the domain of the UCPD. This comes at the price of **many gaps** (e.g. manipulation or exploitation of vulnerabilities of individuals acting for MSME and not qualifying for consumer protection, see above at 0) and of a regulatory regime that looks, at least at first sight, **rather arbitrary** in its policy choices.

Keeping the scope and regulatory focus of different legal instruments apart makes sense where overlap would create the risk of inconsistencies and/or of unnecessary cumulative effects of varying sets of requirements. However, within a blacklist of prohibited practices, it is not necessary to avoid overlap: it is totally acceptable (and in fact an indication of coherence and consistency of the acquis) to have harmful and manipulative practices banned by not only one, but by two, three or even more EU legal instruments. This is because there is no need to reduce bureaucracy and red tape for practices that are blacklisted because of their incompatibility with fundamental European values.

As has been demonstrated above (see at 0), the prohibitions currently listed in Article 5 **cannot be properly understood** without analysing them within the wider framework of existing Union law, in particular data protection law, non-discrimination law, consumer protection law and competition law. However, the interplay between the AIA Proposal and such other law is not clarified in the blackletter, possibly even allowing for an interpretation that, to a certain extent, the AIA Proposal derogates or modifies such other law within the scope of application of the AIA Proposal, although this is certainly not intended. In this context, one should not forget that the AIA is going to be the first, or at least one of the first, legal frameworks for AI worldwide. As has been the case with other EU legislation, it has the potential of becoming a **global role model** for the regulation of AI applications. However, in order to fulfil this role, it must be easy to understand and reflect the underlying policy choices and assumptions in a consistent manner. A piece of legislation which is understood only by very few experts worldwide, because in order to understand it one has to have a very profound knowledge of the remaining acquis and the scope of application of various other legal instruments, will not easily become a legal instrument from which other States and regions in the world draw inspiration.

While the authors of this Study would like to mention that some of the prohibitions in Article 5(1)(a) to (d) seem to be formulated with far too many restrictions and with a scope that is far too narrow, she will refrain from revising this part of Article 5 because this would clearly be beyond the scope of the Study. However, for purposes of this Study, she recommends that, at the very least, a new paragraph (3) be added that **clarifies the relationship with prohibitions following from other laws**.

It is therefore suggested to phrase a new Article 5(3) that would replace the existing paragraph (3) (the latter recommended to be moved to a new Title IIa) and that might read as follows:

Article 5

[…]

3. Paragraphs (1) and (2) are without prejudice to prohibitions that apply where an artificial intelligence practice violates other laws, including data protection law, non-discrimination law, consumer protection law, and competition law.

6.4. Recommendations with regard to biometric identification

6.4.1 Limitations on scope of the existing proposal

Turning to the provisions that would be moved to, or inserted in, the new Title IIa on restricted AI practices, the first provision would deal with remote biometric identification that is currently being dealt with under Article 5(1)(d) and (2) to (4) of the AIA Proposal. One of the most conspicuous points about the current provisions on real-time remote biometric identification is a whole range of limitations on scope.

The first general limitation is to be found in Article 1(3) of the AIA Proposal according to which the AIA does not apply to AI developed or used exclusively for military purposes. Furthermore, the provisions (currently) in Article 5 on identification measures apply only where identification occurs

- with the help of biometric data;
- remotely;
- in real-time;
- in publicly accessible spaces; and
- for law enforcement purposes.

Each of these limitations requires justification, as explained in more detail in the following table. In the first place, there must be a justification for limiting the scope of the rather elaborate provisions that are currently found in Article 5(1)(d) and (2) to (4) of the AIA Proposal in precisely this way. In the second place, the question arises whether it is justified to have no restrictions at all for biometric identification techniques outside this limited scope.

Table 2: Limitations on scope with regard to identification measures

Limitation	Definition	Possible justification for limitation	Objections to justification
Biometric	Based on biometric input data	Means that method is inescapable and builds on a particularly sensitive category of data	Sensitive data already captured in enrolment phase, not during application. Other methods of large-scale surveillance (e.g. using mobile phone signals) are not easily escapable either.
Remote	At a distance	Allows for large-scale surveillance that goes mostly unnoticed by individuals (chilling effect)	Maybe better focus on whether conscious cooperation is required or not

		Excludes very traditional identification methods.	
Real-time	Without significant delay	Affects many individuals. Allows for seamless surveillance. Allows immediate action to be taken (such as arrest).	Time factor fails to hit the focus of ethical concerns, better focus on continuous or large-scale identification.
In publicly accessible spaces	Physical place accessible to the public, regardless of whether certain conditions for access may apply	Freedom to move around freely in publicly accessible spaces is particularly essential in fundamental rights terms.	Other spaces (e.g. workplace, school), including online environments, may be as inescapable as publicly accessible spaces.
For the purpose of law enforcement	Activities carried out by relevant 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	Means that technology is in the hand of state actors that can exercise immediate power. Under the LED, state actors have the most leeway for data processing. High risk of function creep as state actors can themselves create the legal basis for further activities.	Why are there no restrictions for, e.g., purposes of public planning activities or private purposes? Should law enforcement not rather be a privileged purpose?

Source: Christiane Wendehorst

a. Limitation of scope of (current) Article 5(1)(d) and (2) to (4)

As far as the limitation of the scope of (current) Article 5(1)(d) and (2) to (4) of the AIA Proposal to **biometric** identification techniques is concerned, this restriction is only partly justified. From an ethical point of view, what counts most in terms of fundamental rights concerns is the fact that someone (e.g. law enforcement authorities) holds a biometric template of a particular person and is thus able to identify and trace that person anywhere on the globe. Where this is the case, it is only of secondary importance whether large-scale remote identification actually occurs by using the biometric templates or by some other means, such as by tracking people's mobiles. In other words, what is ethically problematic is (a) storing people's biometric templates in a way that potentially allows to trace those people, and (b) mass surveillance of people, whereas, if both (a) and (b) is fulfilled, the fact that mass surveillance occurs by biometric means is not the decisive point.

However, there may nevertheless be good reasons for limiting the provision to identification by biometric means. First of all, it is self-evident that the more biometric techniques are used, the more encouragement there will be for the storing and refining of biometric templates. Limiting the use of biometric identification techniques may thus indirectly discourage the investment in biometric templates of the whole population. The authors also realise that there is a lot of **public anxiety** about biometric techniques and that, from a political point of view, it may be advisable to introduce a rule specifically on biometric identification. Still, the authors would like to suggest considering whether the relevant provision in the AIA could **include other forms of real-time remote identification** (such as by tracking mobile phone signals) while still stressing biometric identification techniques in a prominent way.

Limiting the strictest regulatory regime to **remote** identification techniques as well as to **real-time** identification (if changes to the definitions are implemented, see above at 0) seems justified in the light of the additional risks posed, in particular the fact that identification occurs largely unnoticed and on a

large scale. However, it is not convincing to have no restrictions at all where biometric identification only occurs ex post – even though, in this case, existing restrictions under the LED and GDPR may be sufficient, it may be advisable to stress these restrictions also under the AIA in order to create a consistent regime.

Upon closer inspection, the same holds true for the limitation to **publicly accessible spaces**, i.e. it can be justified to limit the strictest regulatory regime to measures in publicly accessible spaces. Where spaces are not publicly accessible, but accessible only to a limited number of persons (such as the employees of a company, or the inmates of a prison) fewer people are affected and the use of biometric identification techniques is much closer to biometric authentication. Where spaces are accessible to an indefinite number of people, but the spaces are not physical (but online) spaces, Article 9 GDPR defines rather strict limits for the use of biometric data in the narrow sense, so the level of protection is already quite high. Usually, the only possible justification will be explicit consent within the meaning of Article 9(2)(a) GDPR.

However, the limitation of restrictions to **law enforcement purposes** is highly questionable. Generally speaking, law enforcement should be a privileged purpose when compared with other purposes (such as data collection for public planning activities). Article 10 LED allows the processing of biometric data for purposes of identification where this is strictly necessary for law enforcement purposes, subject to appropriate safeguards for the rights and freedoms of the data subject, and only where further requirements are met, such as that the processing of biometric data is authorised by Union or Member State law. Under Article 9(2)(g) GDPR, national authorities may process biometric data, including for identification purposes, where the processing of biometric data 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. There is thus not much difference between the leeway for public authorities under the LED on the one hand and the GDPR on the other. So if there is a danger of excessive use of real-time remote biometric identification by law enforcement authorities, the same danger exists with regard to public authorities that process biometric data on the basis of the GDPR for purposes other than law enforcement.

Illustration 4: Undesirable remote biometric identification beyond law enforcement

> Municipality M would like to get a better idea of who lives in the city or visits the city, what are the citizens' habits, and how they move around during the day. The data is to be used for planning purposes, e.g. for improvement of the public transport system, or for the management of crowds and assemblies in public spaces. On the basis of national law, which includes details as to pseudonymisation and other safeguards, M uses real-time remote biometric identification for collecting the data. This practice may be considered disproportionate to the aim pursued and thus not to be in conformity with Article 9 GDPR, but then also disproportionate use of biometric techniques for law enforcement purposes would theoretically be prohibited by the LED. It is difficult to understand why the one is dealt with under the AIA Proposal, but not the other.

Source: Christiane Wendehorst

There are also grey zones around law enforcement, which might allow public authorities to circumvent restrictions, e.g. in the area of migration, asylum and border control management.

Illustration 5: Remote biometric identification in grey zones around law enforcement

State S uses real-time remote biometric identification in public spaces to detect foreigners without a residence permit. S claims that staying in the territory of S without a residence permit does not qualify as a 'criminal offence' and that the measure is also taken without regard to any threat to public security, i.e. that this does therefore not qualify as 'law enforcement' and does not fall under the prohibition in Article 5.

Source: Christiane Wendehorst

While there is no comparable urgency to also regulate private use of remote biometric identification in publicly accessible spaces (as this is more likely to be fully captured by Article 9 GDPR) there is no harm in including it in the restriction, provided the provision is formulated in a way that is fully consistent with Article 9.

b. No restrictions at all for other instances of biometric identification?

Other than real-time and remote biometric identification raises fewer ethical concerns than biometric identification that is either not remote, because it requires the affected persons' conscious cooperation (such as placing their face before a scanner), or that is not in real-time because it occurs only punctually, e.g. after a crime has been observed. The same applies to biometric identification that occurs in other than publicly accessible spaces. It is therefore defensible to restrict oneself, with regard to these forms of biometric identification, to Article 9 GDPR. However, in order not to create a legal framework that looks inconsistent at first sight, it could as well be advisable to include these forms of biometric identification in the **rule on other biometric techniques** (on which see below at 6.5).

6.4.2 A new regulatory approach

It would therefore be preferable to list, against the background of Article 9 GDPR and Article 10 LED, the **purposes for which real-time remote biometric identification is permitted**, including law enforcement, as further specified. Law enforcement would then rightly be treated as a privileged purpose, alongside qualified consent, the use for scientific research purposes, the use for the protection of the vital interests of the person identified, and use for migration, asylum or border control management.

Whether or not additional specifications, beyond the restrictions that already follow from the current text, should be added to the use for migration, asylum or border control management, is a political question. In any case, and assuming that migration, asylum or border control management do not generally/always qualify as 'law enforcement' (see also the division in Annex III), there is currently no restriction at all in the AIA proposal.

The newly structured Article 5a might read as follows:

TITLE IIa

RESTRICTED ARTIFICIAL INTELLIGENCE APPLICATIONS

Article 5a
'Real-time' remote [biometric] identification

1. **AI systems may be used for 'real time' remote biometric identification *[Opt.: or other 'real time' remote identification]* in publicly accessible spaces only when such surveillance is limited to what is strictly necessary for:**

(a) **the use for a specific purpose to which the persons identified have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;**

(b) **the use for purposes and under conditions referred to in Article 9 (2)(b) and (j) of Regulation (EU) 2016/679;**

(c) **the use for migration, asylum or border control management;**

(d) the use ~~of 'real-time' remote biometric identification systems in publicly accessible spaces~~ for the purpose of law enforcement, ~~unless and~~ in 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 public security, in particular** 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.

2. The use of 'real-time' remote [biometric] identification systems in publicly accessible spaces for the purpose~~s of law enforcement for any of the objectives~~ referred to in paragraph 1 point**s c) and** d) 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.

In addition, the use of 'real-time' remote [biometric] identification systems in publicly accessible spaces ~~for the purpose of law enforcement~~ for any of the objectives referred to in paragraph 1 point**s c) and** d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point**s c) and** d) and 2, 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 the detailed rules of national law referred to in paragraph 4. 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.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use

	of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point**s (c) and** (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.
4.	A Member State may decide to provide 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~~ within the limits and under the conditions listed in paragraphs 1, point**s (c) and** (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point**s (c) and** (d), including which of the criminal offences referred to in point **(d)** (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

6.4.3 Clarifications with regard to data collection and storage

It is recommended that the new Article 5a on real-time remote biometric identification (or, as the case may be, also other forms of real-time remote identification) **clarify that other areas of the law apply to fill the gaps**, in particular data protection law and non-discrimination law. In addition, the new paragraph should stress explicitly the controller's duty not to collect any data beyond what is strictly necessary to achieve the purpose on which biometric identification is based, and to erase any personal data collected from biometric identification as soon as these data are no longer strictly necessary to achieve the purpose for which the data have been collected.

Illustration 6: Data collection and storage in the context of biometric identification

Police has received information from intelligence services that individuals X and Y are planning a terrorist attack on a Christmas market. This is why real-time remote biometric identification is used to trace and stop any of X or Y in case one of them were to be seen in the city or even in the vicinity of the market. In a situation such as this, use of real-time remote biometric identification would be justified. However, it is only necessary to compare the live templates of people walking by (such as that of innocent bystander B) with the stored templates of X and Y. By contrast, it would not be permissible to fully identify B by way of comparison with any stored template of B because this is not necessary for achieving the purpose. In the given situation it may be justified to store video recordings for a longer period than usual (as there may be situations where, ex post, it turns out that previously unknown person Z was cooperating with X and Y and exploring the area to prepare for an attack). However, unless such a situation arises later and B was acting in a suspicious manner, it would not be necessary to identify B.

Source: Christiane Wendehorst

The new Article 5a(5) could read as follows:

Article 5a
'Real-time' remote [biometric] identification

[…]

5. Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law and non-discrimination law, remain unaffected. In any case, only such personal data may be collected through remote biometric identification as are strictly necessary to achieve the purpose stated in paragraph (1), and must be erased as soon as they are no longer necessary in relation to this purpose.

6.5. Recommendations with regard to emotion recognition and biometric categorisation

6.5.1 Emotion recognition and biometric categorisation as restricted AI practices

While, in the case of biometric identification systems, there was still Article 9 GDPR and Article 10 LED as a kind of safety net because biometric identification relies on the processing of biometric data within the definition of the GDPR and LED, this is not the case with emotion recognition and biometric categorisation systems. The reason is that those systems do not rely on the processing of biometric data within the meaning of Article 9 GDPR, but only on what has here been called 'biometrics-based data' that may or may not allow or confirm the unique identification of a natural person (see above at 0). This is why, in the majority of cases, processing of personal data for purposes of emotion recognition or biometric categorisation will **only be subject to Article 6 GDPR**, including simple consent within the meaning of Article 6(1)(a) and other legal grounds available for personal data in general. Of course, it seems hardly convincing that Article 9 GDPR qualifies personal data revealing political opinions, religious beliefs or trade union membership as particularly sensitive categories of data, while emotions, thoughts and intentions (e.g. identified by way of brain-computer-interfaces) only qualify as general personal data. However, unless the GDPR is changed in that respect (which would create other problems), we have two accept this unsatisfactory situation.

This means that any protection which fails to be provided by Article 9 GDPR must be provided by the AIA itself. At the end of the day, this can be achieved by qualifying the use of emotion recognition and biometric categorisation systems as **restricted AI practices**, subjecting them to a very similar regulatory approach as real-time remote biometric identification. However, the situations in which the use of emotion recognition systems or biometric categorisation systems is justified will have to be more broadly defined, as they include also the full range of medical purposes and many further purposes listed in Article 9 GDPR.

6.5.2 How to design the restrictions?

Which of the **purposes in Article 9 GDPR** to include and which to exclude is not easy to decide. While explicit consent as well as purposes such as medical purposes or scientific research purposes must clearly be listed as admissible, and whereas some are clearly not applicable from the outset, things are less clear, e.g., with 'processing that is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity' (Article 9(2)(f) GDPR). Ultimately, this is a political decision, but from an ethical point of view such use would raise a number of issues.

Illustration 7: Justification of emotion recognition or biometric categorisation

The judiciary of a Member State introduces the use of emotion recognition systems in order to find out whether persons in the courtroom (defendant, witnesses, etc.) are telling the truth. As the AIA Proposal currently stands, this would arguably be qualified as a high-risk application under point 8 (a) of Annex III, but would otherwise be permissible if based on Member State law. It is highly questionable whether this is the right policy choice.

Source: Christiane Wendehorst

For the sake of simplicity and clarity of drafting, the **transparency provisions**, which are currently found in Article 52(2) AIA Proposal, should be inserted in the new Article 5b.

There should likewise be a reminder that Article 5b is without prejudice to further restrictions following from **other laws**, in particular data protection law.

To summarise, the new Article 5b could be phrased as follows:

Article 5b
Other use of biometric techniques

1. Biometric identification systems not covered by Article 5a, emotion recognition systems and biometric categorisation systems may be used only when such use is limited to what is strictly necessary for:

(a) the use for a specific purpose to which the affected persons have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;

(b) the use for purposes and under conditions referred to in Article 9 (2)(b), (c), (h), (i) and (j) of Regulation (EU) 2016/679;

(c) the use for the purpose of law enforcement, migration, asylum or border control management in as far as purposes are proportionate to the aim pursued, respect the essence of the fundamental rights and interests affected and provide for suitable and specific measures to safeguard them.

2. Users of AI systems within the meaning of paragraph (1) shall inform of the operation of the system the natural persons exposed thereto unless this is inconsistent with the purpose within the meaning of paragraph (1) for which the system is used.

3. Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law, non-discrimination law and consumer protection law, remain unaffected.

Furthermore, Annex III point 1 should be extended so as to cover emotion recognition systems in (at least) the same way as biometric categorisation systems.

6.6. Recommendations with regard to decisions taken

6.6.1 Mirroring and adapting the rule in Article 14(5)

Article 14(5) of the AIA Proposal provides in the context of human oversight that, for high-risk AI systems referred to in point 1(a) of Annex III, human oversight measures shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons. Given that this is more than a design requirement this rule should, as a **restriction on use**, be mirrored in Title IIa.

At the same time however, the rule needs to be **significantly modified** in several respects because it is both insufficient and overreaching. 'No action or decision' would mean that not even identity control (such as requesting a passport) may follow from a high matching score, which would turn biometric identification by AI close to completely useless. This is aggravated by the fact that, in a situation where immediate action is of the essence, any two natural persons who may be available could only quickly compare photos that are displayed on their screens, probably acting with a similar (or much higher) error rate than the system. This is why, in line with Article 22 GDPR, actions or decisions should only be captured by the provision if they produce legal effects or similarly significantly affect the natural person concerned. The authors of this study are well aware of the fact that Article 22 GDPR is far from perfect and raises a number of difficult issues of interpretation, but creating inconsistency with Article 22 GDPR should likewise be avoided.

On the other hand, the rule in Article 14(5) is insufficient because it does not give any guidance as to the independence of the two natural persons, nor on the training they have received or on the means they use. This is why a more open provision, focussing on the independence and on the reliability and accuracy of the means used for verification, would be preferable.

6.6.2 Use as legal evidence

While biometric identification may, at least in most cases, be open to verification, this is not so with emotion recognition, and often also not with biometric categorisation. This is why there should be a provision that emotion recognition and biometric categorisation systems (or rather the results they produce) may, as such, not be used as **legal evidence** that the person concerned has, in fact, had the emotions, thoughts or intentions recognised by the system or belongs in fact to the category assigned by the system.

Illustration 8: Emotion recognition or biometric categorisation used as legal evidence

> Migration authorities use an AI system to analyse the spoken voice of a migrant seeking asylum with the aim of verifying whether the person seeking asylum actually originates from the geographic region from which the person purports to originate. While the result of this analysis may be an important factor, together with other factors, in establishing the relevant facts with regard to the asylum seeker's geographic origin, it should not already in itself count as legal evidence that the asylum seeker in fact originates from the region indicated by the system.

Source: Christiane Wendehorst

The new Article 5c could read as follows:

Article 5c
Decisions based on biometric techniques

1. No action or decision which produces legal effects concerning the person exposed to biometric identification, emotion recognition or biometric categorisation, or which similarly significantly affects that person, is taken by the user on the basis of the output from the system unless this has been verified by means that are independent from the system and that provide a degree of reliability and accuracy appropriate to the significance of the action or decision.

2. Emotion recognition systems and biometric categorisation systems must, as such, not be used as legal evidence that the natural person concerned has in fact had the emotions, thoughts or intentions recognised by the system or belongs in fact to the category assigned by the system.

3. Further requirements or restrictions following from other Titles of this Act or from other laws remain unaffected.

6.7. Recommendations with regard to biometric inferences

As has been demonstrated above (5.2 and 0), ethical issues not only arise where emotion recognition or categorisation of natural persons occurs on the basis of biometrics-based data, but also where permanent or long-term physical, physiological or behavioural characteristics of a natural person are inferred on the basis of other data. This is why biometric inferences should be included in Title IIa.

However, these inferences cannot be subject to the same type of 'hard' regulation as emotion recognition systems and biometric categorisation systems within the meaning of the definitions of the AIA. Emotion recognition systems and biometric categorisation systems rely on biometrics-based data, i.e. on very specific technical processing of data relating to the physical, physiological or behavioural characteristics or signals of a natural person. Anyone who places on the market, puts into service or uses such systems knows, or should know, that their AI system is subject to a specific legal regime. It is hardly imaginable that someone places on the market, puts into service or uses an AI system for some general purpose (e.g. as a recommender system on an online marketplace) and is then caught by surprise that the AI system is qualified as an emotion recognition system or biometric categorisation system. This is so because, for being qualified as an emotion recognition system or biometric categorisation system, very specific technical arrangements must be in place, including the use of camera, microphone, body sensors and the like, accompanied by very specific software that allows the targeted analysis of signals recorded. Where, on the other hand, biometric inferences are drawn in other ways, such as by analysing text which a person has posted or a person's browsing or shopping history, it is very difficult for someone placing on the market, putting into service or using an AI system to decide whether or not their system is included in the definition of biometric inferences. After all, quite a lot can be seen as relating to, e.g., long-term human characteristics, so the **scope of application is potentially extremely broad**.

As 'hard' regulation (e.g. restricting such inferences to particular purposes or situations or submitting them to particular procedures) would therefore easily be overreaching, there could be a **general fairness rule** prohibiting certain forms of use of AI systems that are both likely to cause **significant harm** to affected natural persons and inconsistent with the way the affected persons contributed to the drawing of the inferences. The 'significant harm' test would already make sure that the provision is

not overreaching because, as a general rule, anyone engaging in activities (including use of AI systems) that cause or are likely to cause significant harm to others should already be on the alert and check twice in any case whether or not the activity is nevertheless permissible. Whether or not harm counts as 'significant' must be decided with a view to a number of factors, including, in the first place, the nature of the harm. In line with principles of tort law that are generally accepted by the national legal systems in the Member States, there is very little to no tolerance vis-à-vis practices that cause others personal injury or damage to property.[275] In the event of psychological harm, things are already more difficult, as psychological harm often depends on people's subjective feelings, which may differ vastly across the population, calling for a more 'objective test' for harm to be sufficiently significant (e.g. many people may currently feel that the mere availability of COVID 19-vaccination causes them psychological harm, as it puts them under pressure to get vaccinated – but that sort of harm cannot possibly count). Last but not least, infliction of pure economic loss can never lead to liability *per se* because, in economic relations, one party's gain is often the other party's loss, so there must be additional factors for remedies to be triggered.

The activity should not be considered permissible in any case where the purpose of the use is inconsistent with the way the affected natural person **contributed to drawing the inferences**. This would be the case, in particular, where the affected person was induced to contribute to the generation of relevant personal data for an entirely different purpose and could not reasonably (i.e. objectively) have been expected to contribute if the person had known or foreseen and understood the purpose of the use.[276]

Illustration 9: Personality profiles created with the help of a video game

> Company V operates an online video game. Natural persons such as G spend a significant part of their free time playing the game. When creating their user accounts and giving consent to data processing they were informed of the fact that V would pass user data on to third parties, and that V as well as those third parties would process the data for improving this game as well as developing similar digital products, and for personalising content, including offers that will be submitted to G in a contractual context, by way of user profiling.
>
> When clicking 'I agree', G did not anticipate that, while he would be playing the game, an AI system in the background would be analysing every single of his reactions to a broad variety of situations, meticulously measuring all sorts of behavioural traits, resulting in an extremely granular behavioural profile. Even less so did G anticipate that this would have an immense impact on the price offered to him for certain products in particular situations in the future (e.g. situations in which G tends to take quick and impulsive decisions), and that the contracts affected would include employment contracts, and that all this would cause immense harm with regard to his future career.

Source: Christiane Wendehorst

Whether or not consent to the processing of user data would, in circumstances such as the ones described in the Illustration, be considered valid under the GDPR, and whether or not the GDPR would ultimately capture inferences as such (both of which is ultimately for the CJEU to judge), the AIA should

[275] Expert Group on Liability and New Technologies (New Technologies Formation), ‚Liability for Artificial Intelligence and other emerging digital technologies' (European Commission 2019).

[276] See Principle 21 of the 'Principles for a Data Economy – Data Transactions and Data Rights' of the American Law Institute and European Law Institute, current version: Tentative Draft No. 2, 2021, available at https://ali.org/projects/show/data-economy/.

address the issue from the perspective of the AI system used. If, at the end of the day, a particular practice turns out to be illegal both under the GDPR and under the AIA, this is not a problem, but rather indicates a high degree of coherence of the acquis.

In a number of situations the problem will not so much be the fact that the affected person unwittingly contributed to the generation of data on the basis of which biometric inferences were drawn, but that, on the contrary, no personal data of the person affected have ever been collected that would, as such, justify drawing an inference of the relevant kind.[277] This is why Title IIa of the AIA should also prohibit biometric inferences where those inferences cause, or are likely to cause, significant harm (including non-economic harm) to a particular person and where that person **has not contributed** to the generation of relevant personal data in a way that would reasonably justify the inference.

Illustration 10: Biometric inferences drawn with regard to third parties

Company P that receives user data from company V in the previous Illustration uses this data not only for creating very granular personality profiles of natural persons actually playing the game, such as G. Rather, the creation of a personality profile for G also affects T, who is a third party sharing a number of characteristics (including age, profession, family situation, shopping habits, browsing history etc.) with G, because P draws inferences from G's behaviour to the behaviour of persons such as T, assuming that they will react in a given situation in very much the same manner as G. These assumptions are fed into recruitment software, which is why T is not hired for a job he would otherwise have been hired for.

As such, making assumptions on the basis of past experience can hardly be prohibited (and this is how science and technology generally evolve). However, where it is unreasonable to draw such a biometric inference in the light of the fact that no personal data of T have been collected and analysed that would justify a conclusion that T will react in a given situation in the same manner as G, the AIA should arguably put a halt to such use of an AI system.

Source: Christiane Wendehorst

The authors of this Study are well aware of the fact that suggesting provisions for biometric inferences will be a **very controversial** matter and that **a great deal of reflection** and discussion will be required to make sure provisions are not overreaching and do not stifle innovation and growth. However, she is of the opinion that the 'significant harm' test should be sufficient to keep effects within reasonable boundaries. This is why she recommends considering a provision along the lines of the following:

Article 5d
Biometric inferences

1. AI systems may not be used for drawing biometric inferences where such use

(a) causes, or can reasonably be expected to cause, significant harm, including non-economic harm, to the natural person concerned; and

(b) the use is inconsistent with the way that person contributed to drawing the inferences, in particular because

(i) that person was induced to contribute to the generation of relevant personal data for an entirely different purpose and could not reasonably

[277] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences' [2019] Columbia Business Law Review 494.

		have been expected to contribute if the person had known and understood the purpose of the use; or
	(ii)	**that person did not contribute to the generation of relevant personal data in a way that would reasonably allow such a biometric inference to be drawn.**
2.	**Paragraph 1(b)(i) does not apply where AI systems are used for purposes of law enforcement, migration, asylum or border control management in as far as purposes are proportionate to the aim pursued, respect the essence of the fundamental rights and interests affected and provide for suitable and specific measures to safeguard them.**	

6.8. Recommendations with regard to consent management

Last but not least, the authors of this study suggest considering a new provision on consent management. Again, this is a provision that might as well be inserted in the GDPR, but given that inserting a provision in the AIA would potentially cause much less disruption, and that this provision is particularly important in the context of biometrics-based data and biometric technologies, it is suggested to include the provision in Title IIa of the AIA.

In essence, the idea is that, in the light of the sensitivity of biometrics-based data and the fact that anyone who gets hold of them has enormous power over that individual, **automated consent management** should normally be provided for, allowing the affected persons themselves to effectively manage consent and to use independent tools or service providers[278] for consent management (such as data sharing service providers within the meaning of the Data Governance Act[279], or consent management services within the meaning of the German TTDSG[280]). Likewise, systems must be designed in a way that ensures automated transmission to all recipients of data, if any, and to automated reactions on the part of those recipients.

The authors of this Study well aware, though, that **effects of this are limited**, given that anyone can create biometric templates of others, e.g. from photos, video or voice recording or voice recordings freely available on the internet.

As it would be very challenging to provide for all the details in the AIA itself, and as consistency must be ensured with other areas of Union law, some of which are still in a flux (such as the E-Privacy-Regulation), it is suggested to leave the details to **delegated acts** of the European Commission.

The outlines of such a provision in the AIA could read as follows:

---

[278] See Christiane Wendehorst, 'Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III (Nomos 2017), 353; Data Ethics Commission of the Federal Government, 'Opinion of the Data Ethics Commission' (2019) available at <https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf> (last accessed 09 July 2021) 133; This goes beyond recent proposals by Giovanni Sartor, Francesca Lagioia and Federico Galli, 'Regulating Targeted and Behavioural Advertising in Digital Services' (2021 European Parliament), 103 to introduce an obligation not to prevent the use of such systems, Proposal 12.

[279] Article 9(1) Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.

[280] § 26 Proposal for Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutzgesetz).

Article 5e
Consent management

1. Where the use of biometric techniques under Articles 5a or 5b is based on the affected person's consent, the user of the system shall provide for automated consent management that fulfils, at least, the following requirements:

(a) the affected person must, at any time, have access to the consent management system and to all conditions under which consent is given, which must be easy to find, to comprehend and to use, and to which the affected person must be directed regularly in a way and at intervals that encourage active consent management;

(b) the affected person must be put in a position to use independent consent management tools or services;

(c) any modification or withdrawal of consent must be automatically transmitted to all recipients, if any, of biometrics-based data, which must have technical means in place to provide for automated erasure or other action required under applicable Union data protection law.

2. The Commission is empowered to adopt delegated acts in accordance with Article 73 to determine the detailed requirements of the systems referred to in paragraph (1) and, if necessary, exceptions from paragraph (1), which respect the essence of the provisions in paragraph (1).

REFERENCES

Acquisti A, Gross R and Stutzman F, 'Face Recognition and Privacy in the Age of Augmented Reality' (2014) 6 Journal of Privacy and Confidentiality

<https://journalprivacyconfidentiality.org/index.php/jpc/article/view/638>.

Adowaa Buolamwini J, 'Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers' (2017)

<https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf>.

Alon-Barkat S and Busuioc M, 'Decision-Makers Processing of AI Algorithmic Advice: Automation Bias versus Selective Adherence' (2021) abs/2103.02381 SSRN Electronic Journal

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794660>.

Alterman A, 'A Piece of Yourself: Ethical Issues in Biometric Identification' (2003) 5 Ethics and Information Technology 139.

Arya A and others, 'Integration of Biometric ID for the Effective Collection and Epidemiological Evaluation of Antibiotic Prescription in Tuberculosis and Other Diseases: A Medical Hypothesis' (2020) 21 Journal of Global Antimicrobial Resistance 439.

Asher-Schapiro A, 'What Is Behavioral Biometrics?' (Big Catch Blog)

<https://www.biocatch.com/blog/what-is-behavioral-biometrics>.

Association for Biometrics (AfB) and International Computer Security Association (ICSA), '1998 Glossary of Biometric Terms' (1998) 3 Information Security Technical Report 98.

Begault L, 'Automated Technologies and the Future of Fortress Europe' (*Amnesty International*, 2019)

<https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/>.

Bhuta N and others (eds), *Autonomous Weapons Systems* (Cambridge University Press 2016).

Biger-Levin A, 'Behavioral Biometrics vs Static Biometrics: Dynamic Fraud Detection Explained' (Big Catch Blog)

<https://www.biocatch.com/blog/behavioral-biometrics-vs-static-biometrics-fraud-detection>.

Bond C and DePaulo B, 'Accuracy of Deception Judgments' (2006) 10 Personality and Social Psychology Review 214.

Breebaart J and others, 'Biometric Template Protection' (2009) 33 Datenschutz und Datensicherheit - DuD 299.

Breland A, 'How White Engineers Built Racist Code – and Why It's Dangerous for Black People' (*the Guardian*, 2017)

<http://www.theguardian.com/technology/2017/dec/04/racist-facial-recognition-white-coders-black-people-police>.

Brey P, 'Ethical Aspects of Facial Recognition Systems in Public Places' (2004) 2 Comm & Ethics in Society 97.

Bygrave L, 'Article 22 Automated Individual Decision-Making, Including Profiling' in Christopher Kuner and others, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

Ćatović E and Adamović S, 'Application of Biometrics in Automotive Industry - Case Study Based on Iris Recognition' (International Scientific Conference on Information Technologies and Data related Research – Sinteza 2017).

Cappelli R and others, 'Fingerprint Image Reconstruction from Standard Templates' (2007) 29 IEEE Transactions on Pattern Analysis and Machine Intelligence 1489.

Chadwick R (ed), Encyclopedia of Applied Ethics (Elsevier Science 2012).

Connor N, 'Chinese School Uses Facial Recognition to Monitor Student Attention in Class' (*The Telegraph*, 2018) available at

<https://www.telegraph.co.uk/news/2018/05/17/chinese-school-uses-facial-recognition-monitor-student-attention/>.

Cooper J and Yon J, 'Ethical Issues in Biometrics' (2019) 30 Science Insights 63.

Data Ethics Commission of the (German) Federal Government, 'Opinion of the Data Ethics Commission' (2019)

<https://datenethikkommission.de/wp-content/uploads/DEK_Gutachtenengl_bf_200121.pdf>.

De Fauw J and others, 'Clinically Applicable Deep Learning for Diagnosis and Referral in Retinal Disease' (2018) 24 Nature Medicine 1342.

Dijk P van and others (eds), *Theory and Practice of the European Convention on Human Rights* (5th edn, Intersentia 2018).

Elkins A and others, 'Appraising the AVATAR for Automated Border Control' (2014)

<https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/002653/P9_RE(2019)002653(ANN3)_XL.pdf>.

European Data Protecion Supervisor, 'Opinion on the Second EU Smart Borders Package' (Opinion 06/2016).

European Group on Ethics in Science and New Technologies (EGE), 'Ethics of Security and Surveillance Technologies' (European Commission 2014).

European Group on Ethics in Science and Technology (EGE) 'Opinion on the Ethical Aspects of ICT Implants in the Human Body' (European Commission 2005).

European Parliamentary Research Service, 'The Fight Against Terrorism: The Cost of Non-Europe' (2018), 38.

European Parliamentary Research Service, 'The Ethics of Artificial Intelligence: Issues and Initiatives' (2020).

European Parliamentary Research Service, 'Artificial Intelligence at EU Borders: Overview of Applications and Key Issues' (2021).

Expert Group on Liability and New Technologies (New Technologies Formation), ‚Liability for Artificial Intelligence and other emerging digital technologies' (European Commission 2019).

Feldman Barrett L and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements' (2019) 20 Psychological Science in the Public Interest 1.

Floridi L, 'The European Legislation on AI: A Brief Analysis of Its Philosophical Approach' (2021) 34 Philosophy & Technology 215.

Fitzpatrick M 'Advertising Billboards Use Facial Recognition to Target Shoppers' (*GUARDIAN,* 2010)

<http://www.theguardian.com/media/pda/2010/sep/27/advertising-billboards-facial-recognition-japan>.

Gimbel E, 'How Biometric Technologies Improve Healthcare Operations' (*Technology Solutions That Drive Healthcare*, 2019)

<https://healthtechmagazine.net/article/2019/12/how-biometric-technologies-improve-healthcare-operations>.

Greer S, The Exceptions to Articles 8 to 11 of the European Convention on Human Rights (Council of Europe Publishing 1998).

González Fuster G, 'Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights' (European Parliament 2020).

Goyal M and others, 'Artificial Intelligence-Based Image Classification Methods for Diagnosis of Skin Cancer: Challenges and Opportunities' (2020) 127 Computers in Biology and Medicine 104065.

Graham S and Wood D, 'Digitizing Surveillance: Categorization, Space, Inequality' (2003) 23 Critical Social Policy 227.

Guelke J 'Surveillance: Ethical issues, legal limitations, and efficiency' (Surveille Deliverable D4.8 E, 2014), 9.

Gumpert G and Drucker SJ, 'Public Boundaries: Privacy and Surveillance in a Technological World' (2001) 49 Communication Quarterly 115.

Gutheil M and others, 'Interoperability of Justice and Home Affairs Information Systems' (European Parliament 2018).

Haselager P and others, 'A Note on Ethical Aspects of BCI' (2009) 22 Brain-Machine Interface 1352, 1352.

Henman P, 'Computer Technology – a Political Player in Social Policy Processes' (1997) 26 Journal of Social Policy 323.

Hildebrandt M and Gutwirth S (eds), Profiling the European Citizen (Springer 2008).

Hill K, 'The Secretive Company That Might End Privacy as We Know It' (NY Times 2020)

<https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

HLEG on AI, 'Ethics Guidelines for Trustworthy AI' (2019).

Hounslow D and Nozaki R, 'Japan - Data Protection Overview' (*DataGuidance*, 2020)

<https://www.dataguidance.com/notes/japan-data-protection-overview>.

Imaoka H and others, 'The Future of Biometrics Technology: From Face Recognition to related Applications' (2021) 10 APSIPA Transactions on Signal and Information Processing, 8.

Jain A, Dass S and Nandakuma K, 'Soft Biometric Traits for Personal Recognition Systems' in David Zhang and Anil Jain (eds), International Conference on Biometric Authentication (Springer 2004).

Jain A, Nandakumar K and Nagar A, 'Biometric Template Security' (2008) 2008 EURASIP J. Adv. Signal Process 1.

Kumar A and Zhang D (eds), *Ethics and Policy of Biometrics* (Springer 2010).

Kuner C and others, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

Lawson G and Stedmon A (eds), *Hostile Intent and Counter-Terrorism* (CRC Press 2017).

Liu YL, 'The Future of the Classroom? China's Experience of AI in Education' The AI Powered State: China's Approach to Public Sector Innovation [2020]

<https://www.nesta.org.uk/report/the-future-of-the-classroom/>.

Lucivero F and Tamburrini G, 'Ethical Monitoring of Brain-Machine Interfaces: A Note on Personal Identity and Autonomy' (2008) 22 AI & Society 449.

Martin P and others, 'Reviving Racial Medicine? The Use of Race/Ethnicity in Genetics and Biomedical Research, and the Implications for Science and Healthcare' (2007).

Marx G 'The Engineering of Social Control: The Search for the Silver Bullet' in Ruth Peterson and John Hagan (eds), *Crime and Inequality* (Stanford University Press 1995).

Mason J and others, 'An Investigation of Biometric Authentication in the Healthcare Environment' (2020) 8 Array 100042.

McStay A, 'Emotional AI and EdTech: Serving the Public Good?' (2020) 45 Learning, Media and Technology 270.

Mendoza I and Bygrave L, 'The Right Not to Be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer 2017).

Milano S, Taddeo M and Floridi L, 'Recommender Systems and Their Ethical Challenges' (2020) 35 AI & Society 957.

Miller T, *The Assault on Privacy* (Signet 1971).

Mittelstadt B and Floridi L, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22 Science and Engineering Ethics 303.

Mitra S and Gofman M (eds), *Biometrics in a Data Driven World: Trends, Technologies and Challenges* (CRC Press 2017).

Mordini E and Carlo Petrini, 'Ethical and Social Implications of Biometric Identification Technology' (2007) 43 Annali Dell'istituto Superiore di Sanita 5.

Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer 2012).

Morley J and others, 'The Ethics of AI in Health Care: A Mapping Review' (2020) 260 Social Science & Medicine 113172.

Nash J , 'EU Research Group Talks up Access Control, Biometrics in Healthcare (*Biometric Update*, 2020)

<https://www.biometricupdate.com/202009/eu-research-group-talks-up-access-control-biometrics-in-healthcare.

Nash J, 'Like a Nightmare Come True: Killer Robots Fighting Humanity's Wars' (*Biometric Update*, 2021)

<https://www.biometricupdate.com/202106/like-a-nightmare-come-true-killer-robots-fighting-humanitys-wars>.

Nast C, 'The Science behind the EU's Creepy New Border Tech Is Totally Flawed' (*Wired UK,* 2018)

<https://www.wired.co.uk/article/border-control-technology-biometrics>.

Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' (1998) 17 Law and Philosophy 559.

North-Samardzic A, 'Biometric Technology and Ethics: Beyond Security Applications' (2020) 167 Journal of Business Ethics 433.

Obaidat M, Traore I and Woungang I (eds), *Biometric-Based Physical and Cybersecurity Systems* (Springer 2019).

Palm E, 'Conflicting Interests in the Development of a Harmonized EU E-Passport' (2016) 31 Journal of Borderlands Studies 203.

Peers S and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Nomos 2014).

Phillips J and others, 'An Other-Race Effect for Face Recognition Algorithms' (2011) 8 ACM Transactions on Applied Perception, 1.

Plath K, DSGVO/BDSG (3rd edn 2018).

Ploeg I van der, 'Genetics, Biometrics and the Informatization of the Body.' (2007) 43 Annali dell'Istituto superiore di sanita 44.

Qiang X, 'President XI's Surveillance State' (2019) 30 Journal of Democracy 53.

Reece A and Danforth C, 'Instagram Photos Reveal Predictive Markers of Depression' (2017) 6 EPJ Data Science 15.

Royakkers L and others, 'Societal and Ethical Issues of Digitization' (2018) 20 Ethics and Information Technology 127.

Rubio I, 'Protección de Datos abre una investigación sobre las cámaras de vigilancia facial de Mercadona' (El Pais, 2020)

<https://elpais.com/tecnologia/2020-07-06/proteccion-de-datos-abre-una-investigacion-sobre-las-camaras-de-vigilancia-facial-de-mercadona.html>.

Rücker D and Kugler T (eds), *New European General Data Protection Regulation: A Practitioner's Guide* (Nomos 2017).

Sánchez-Monedero J and Dencik L, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' [2020] Information, Communication & Society 1.

Sartor G, Lagioia F and Galli F 'Regulating Targeted and Behavioural Advertising in Digital Services' (2021 European Parliament).

Shaw D, 'Asylum Applications: Home Office Urged to Use Lie Detectors' (*BBC News*, 2019)

<https://www.bbc.com/news/uk-46830373>.

Shifrin D and Tobin MB, 'Past, Present and Future: What's Happening with Illinois' and Other Biometric Privacy Laws' (The National Law Review, 2021) available at

https://www.natlawreview.com/article/past-present-and-future-what-s-happening-illinois-and-other-biometric-privacy-laws.

Smith M and Miller S, 'The Ethical Application of Biometric Facial Recognition Technology' [2021] AI & Society.

Sohnemann N and others, 'New Developments in Digital Services, Short-(2021), Medium-(2025) and Long-Term (2030) Perspectives and the Implications for the Digital Services Act' (European Parliament 2020).

Sud M and VanSandt CV, 'Identity Rights: A Structural Void in Inclusive Growth' (2015) 132 Journal of Business Ethics 589.

Sutrop M, 'Ethical Issues in Governing Biometric Technologies' in Ajay Kumar and David Zhang (eds), *Ethics and policy of biometrics* (Springer 2010).

Sutrop M and Laas-Mikko K, 'From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics' (2012) 29 Review of Policy Research 21.

Taub E, 'Sleepy Behind the Wheel? Some Cars Can Tell' (*NY Times*, 2017) available at

https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html.

Vavoula N, 'Police Information Exchange - The Future Developments Regarding Prüm and the API Directive' (2020 European Parliament).

Veale M and Borgesius FZ, Demystifying the Draft of the EU Artificial Intelligence Act (Pre-Print July 2021).

Vrij A and Granhag PA, 'Eliciting Cues to Deception and Truth: What Matters Are the Questions Asked' (2012) 1 Journal of Applied Research in Memory and Cognition 110.

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences' [2019] Columbia Business Law Review 494.

Williamson B and Eynon R, 'Historical Threads, Missing Links, and Future Directions in AI in Education' (2020) 45 Learning, Media and Technology 223.

Wojnowska-Radzińska J, 'Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) versus Data Protection – Is It Done in the Right Way?' (2020) 37 Review of European and Comparative Law 121.

Wolf P, 'Introducing Biometric Technology in Elections' (International Institute for Democracy and Electoral Assistance 2017).

Yeung P, 'Biometrics Ethics: Why Facial Recognition Still Has Racial Bias' (*Raconteur*, 2020) available at

https://www.raconteur.net/technology/biometrics-ethics-bias/ (last accessed 12 July 2021).

Završnik A, *Big Data, Crime and Social Control* (Routledge 2019), 196.

Zhang D and Anil Jain (eds), *International Conference on Biometric Authentication* (Springer 2004).

ANNEX: PROPOSED WORDING OF TITLE II AND TITLE IIA

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

[…]

(33) 'biometric data' means 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;

(33a) 'biometrics-based data' means personal data resulting from specific technical processing relating to physical, physiological or behavioural signals or characteristics of a natural person, such as facial expressions, movements, pulse frequency, voice, keystrokes or gait, which may or may not allow or confirm the unique identification of a natural person;

(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions**, thoughts** or intentions of natural persons on the basis of their ~~biometric~~**biometrics-based** data;

(35) 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories such as sex, age, hair colour, eye colour, tattoos, ethnic origin**, health, mental ability, personality traits** or sexual or political-orientation, on the basis of their ~~biometric~~**biometrics-based** data;

(35a) 'biometric inferences' mean conclusions with regard to permanent or long-term physical, physiological or behavioural characteristics of a natural person, on the basis of biometrics-based data or other personal data;

(36) 'remote biometric identification system' means an AI system 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 **the conscious cooperation of the persons to be identified** ~~prior knowledge of the user of the AI system whether the person will be present and can be identified~~ ;

(37) ''real-time' remote biometric identification system' means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification ~~all~~ occur **on a continuous or large-scale basis over a period of time and without limitation to a particular past incident (such as a crime recorded by a video camera)**~~; without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~

(38) 'post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;

(39) 'publicly accessible space' means any physical place accessible to the public, regardless of whether certain conditions for access may apply;

(40) 'law enforcement authority' means:

(a) any public authority competent 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; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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;

(41) 'law enforcement' means 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;

[…]

TITLE II

PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

Article 5

1. The following artificial intelligence practices shall be prohibited:

(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

(d) **the putting into service or use of an AI system for the comprehensive surveillance of natural persons in their private or work life to an extent or in a manner that causes or is likely to cause those persons or another person physical or psychological harm**; ~~the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives […]:~~

(e) the placing on the market, putting into service or use of an AI system for the specific technical processing of brain data in order to read or manipulate a person's thoughts against that person's will or in a manner that causes or is likely to cause that person or another person physical or psychological harm.

2. In addition to the prohibited AI practices referred to in paragraph (1), AI practices referred to in Annex Ia shall also be considered prohibited. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex Ia on the basis of a similar threat to fundamental rights and European values as posed by the practices listed in paragraph (1).

3. Paragraphs (1) and (2) are without prejudice to prohibitions that apply where an artificial intelligence practice violates other laws, including data protection law, non-discrimination law, consumer protection law, and competition law.

TITLE IIa

RESTRICTED ARTIFICIAL INTELLIGENCE APPLICATIONS

Article 5a
'Real-time' remote [biometric] identification

1. AI systems may be used for 'real time' remote biometric identification *[Opt.: or other 'real time' remote identification]* in publicly accessible spaces only when such surveillance is limited to what is strictly necessary for:

(a) the use for a specific purpose to which the persons identified have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;

(b) the use for purposes and under conditions referred to in Article 9 (2)(b) and (j) of Regulation (EU) 2016/679;

(c) the use for migration, asylum or border control management;

(d) the use ~~of 'real-time' remote biometric identification systems in publicly accessible spaces~~ for the purpose of law enforcement, ~~unless and~~ in 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 public security, in particular** 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.

2. The use of 'real-time' remote [biometric] identification systems in publicly accessible spaces for the purpose~~s of law enforcement for any of the objectives~~ referred to in paragraph 1 point**s c) and** d) 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.

In addition, the use of 'real-time' remote [biometric] identification systems in publicly accessible spaces ~~for the purpose of law enforcement~~ for any of the objectives referred to in paragraph 1 point**s c) and** d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

3. As regards paragraphs 1, point**s (c) and** (d) and 2, 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 the detailed rules of national law referred to in paragraph 4. 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.

The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point**s (c) and** (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.

4. A Member State may decide to provide 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~~ within the limits and under the conditions listed in paragraphs 1, point**s (c) and** (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point**s (c) and** (d), including which of the criminal offences referred to in point **(d)** (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

5. Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law and non-discrimination law, remain unaffected. In any case, only such personal data may be collected through remote biometric identification as are strictly necessary to achieve the purpose stated in paragraph (1), and must be erased as soon as they are no longer necessary in relation to this purpose.

Article 5b
Other use of biometric techniques

1. Biometric identification systems not covered by Article 5a, emotion recognition systems and biometric categorisation systems may be used only when such use is limited to what is strictly necessary for:

(a) the use for a specific purpose to which the affected persons have given their explicit consent within the meaning of Article 9 (2)(a) of Regulation (EU) 2016/679;

(b) the use for purposes and under conditions referred to in Article 9 (2)(b), (c), (h), (i) and (j) of Regulation (EU) 2016/679;

(c) the use for the purpose of law enforcement, migration, asylum or border control management in as far as purposes are proportionate to the aim pursued, respect the essence of the fundamental rights and interests affected and provide for suitable and specific measures to safeguard them.

2. Users of AI systems within the meaning of paragraph (1) shall inform of the operation of the system the natural persons exposed thereto unless this is inconsistent with the purpose within the meaning of paragraph (1) for which the system is used.

3. Further requirements or restrictions following from other Titles of this Act or from other laws, in particular data protection law, non-discrimination law and consumer protection law, remain unaffected.

Article 5c
Decisions based on biometric techniques

1. No action or decision which produces legal effects concerning the person exposed to biometric identification, emotion recognition or biometric categorisation, or which similarly significantly affects that person, is taken by the user on the basis of the output from the system unless this has been verified by means that are independent from the system and that provide a degree of reliability and accuracy appropriate to the significance of the action or decision.

2. Emotion recognition systems and biometric categorisation systems must, as such, not be used as legal evidence that the natural person concerned has in fact had the emotions, thoughts or intentions recognised by the system or belongs in fact to the category assigned by the system.

3. Further requirements or restrictions following from other Titles of this Act or from other laws remain unaffected.

Article 5d
Biometric inferences

1. AI systems may not be used for drawing biometric inferences where such use

(a) causes, or can reasonably be expected to cause, significant harm, including non-economic harm, to the natural person concerned; and

(b) the use is inconsistent with the way that person contributed to drawing the inferences, in particular because

(i) that person was induced to contribute to the generation of relevant personal data for an entirely different purpose and could not reasonably have been expected to contribute if the person had known and understood the purpose of the use; or

(ii) that person did not contribute to the generation of relevant personal data in a way that would reasonably allow such a biometric inference to be drawn.

2. Paragraph 1(b)(i) does not apply where AI systems are used for purposes of law enforcement, migration, asylum or border control management in as far as purposes are proportionate to the aim pursued, respect the essence of the fundamental rights and interests affected and provide for suitable and specific measures to safeguard them.

Article 5e
Consent management

1. Where the use of biometric techniques under Articles 5a or 5b is based on the affected person's consent, the user of the system shall provide for automated consent management that fulfils, at least, the following requirements:

(a) the affected person must, at any time, have access to the consent management system and to all conditions under which consent is given, which must be easy to find, to comprehend and to use, and to which the affected person must be directed regularly in a way and at intervals that encourage active consent management;

(b) the affected person must be put in a position to use independent consent management tools or services;

(c) any modification or withdrawal of consent must be automatically transmitted to all recipients, if any, of biometrics-based data, which must have technical means in place to provide for automated erasure or other action required under applicable Union data protection law.

2. The Commission is empowered to adopt delegated acts in accordance with Article 73 to determine the detailed requirements of the systems referred to in paragraph (1) and, if necessary, exceptions from paragraph (1), which respect the essence of the provisions in paragraph (1).

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI and PETI Committees, analyses the use of biometric techniques from an ethical and legal perspective. Biometric techniques raise a number of specific ethical issues, as an individual cannot easily change biometric features, and as these techniques tend to intrude into the human body and ultimately the human self. Further issues are more generally associated with large-scale surveillance, algorithmic decision making, or profiling. The study analyses different types of biometric techniques and draws conclusions for EU legislation.

PE 696.968
Print ISBN 978-92-846-8437-3| doi: 10.2861/65868| QA-02-21-976-EN-C
PDF ISBN 978-92-846-8436-6doi: 10.2861/982599QA-02-21-976-EN-N