AI Act's ripple effect on biometric data: harmonising or fragmenting the regulation of biometric data

Sumer, B.; Menéndez Gonzalez, N.; Elbi, A.; Jasserand, C.; Czarnocki, J.; Kindt, E.J.; ... ; Stamhuis, E.

Chapter 8
AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data

Bilgesu Sumer, Natalia Menéndez González, Abdullah Elbi, Catherine Jasserand, Jan Czarnocki, and Els J. Kindt

Contents

Abstract The integration of biometric technologies into a myriad of sectors, from electronic authentication systems like FaceID to border control mechanisms, signifies a leap towards enhancing security and convenience. However, their integration poses a host of legal and ethical risks. The EU has introduced multiple regulations to address the widespread use of biometrics in both public and private domains. To begin with, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) introduced provisions targeting biometric data processing,

This chapter has received funding from H2020-MSCA-ITN-2019-860315 (PriMa), H2020-MSCA-ITN-2019-860813 (TReSPAsS), H2020-MSCA-IF-2019-895978 (DATAFACE), and H2020-883356 (iMars).

B. Sumer (✉) · E. J. Kindt
KU Leuven (KUL) Centre for IT and IP Law (CiTiP), Biometric Law Lab (BLL), Leuven, Belgium
e-mail: bilgesu.sumer@kuleuven.be

E. J. Kindt
e-mail: els.kindt@kuleuven.be

N. Menéndez González
European University Institute, Centre for a Digital Society, Leuven, Belgium
e-mail: natalia.menendez@eui.eu

A. Elbi · J. Czarnocki
KUL, CiTiP, BLL, Leuven, Belgium
e-mail: abdullah.elbi@kuleuven.be

K. Prifti et al. (eds.), *Digital Governance*, Information Technology and Law Series 39,
https://doi.org/10.1007/978-94-6265-639-0_8

while their definition of biometric data remains ambiguous. The Schengen Information System (SIS), the European Digital Identity (eIDAS) and the Payment Services Directive (PSDII) use other terminology to refer to biometric data. The latest development in biometric regulation is the introduction of the Artificial Intelligence Act (AIA), which establishes new definitions and requirements for processing biometric data. This contribution discusses the potential impact of the AIA on the regulation of biometric data, which is currently regulated by a scattered regulatory framework, causing diverging interpretations and legal uncertainty. Our study initially explains the current legal landscape that governs biometric data. Following this, we delve into the new definitions introduced during the negotiations in the adoption process of the AIA proposal. We eventually discuss the potential of the AIA to overcome the challenges posed by this emerging complex biometric law.

Keywords Biometric data · GDPR · AIA · LED · eIDAS · SIS · PSDII · Regulation

8.1 Introduction

Contemporary biometric applications typically deploy AI that is increasingly becoming omnipresent in a wide array of fields, from e-gates in border control to Face ID for digital identity. On the other hand, these powerful AI tools pose several risks as they can identify individuals based on their bodily information; hence, they can be used to discriminate individuals[1] and control populations.[2]

In recent years, the European Union (EU) legislators have reacted to the proliferation of AI-based biometric applications in public and private sectors with several regulatory instruments and proposals. For example, the GDPR, as the first general legal data protection framework that specifically regulates biometric data, incorporates several provisions governing biometric data processing.

However, the GDPR definition of Article 4(14) and several other GDPR references, such as Article 9(1) and Recital 51, caused diverging interpretations due to their ambiguity, leading to legal uncertainty. While technical definitions, such as those of the International Standards Organization (ISO), broadly define biometric

J. Czarnocki
e-mail: jan.czarnocki@kuleuven.be

C. Jasserand
University of Groningen, Groningen, The Netherlands
e-mail: c.a.jasserand@step-rug.nl

E. J. Kindt
Universiteit Leiden, eLaw, Leiden, The Netherlands

[1] George 2022, p. 3; Rose 2000, p. 321.

[2] Foucault 2008, p. 34; Gates 2011, p. 27.

data, the GDPR's protection seems narrower, possibly excluding biometric images such as photographs.[3] This delta between technical definitions in international standards and the definition of biometric data in the GDPR (and the Law Enforcement Directive (LED)) has been subject to discussions.[4]

More regulatory instruments that are *lex specialis*, refer to biometric data. For example, biometric data has long been used for identity verification and identification in border control and security at the EU borders in the Schengen Information System. Other sectoral regulations such as eIDAS 2.0. and PSDII also include provisions tacitly mentioning biometric data.

Against this background, the Commission also introduced the AIA proposal, which introduced new categories and definitions of biometric data. The importance of definitions in any regulation deserves particular attention as they do not only determine the legal meaning of the concepts but also the ways a term should be used in factual circumstances.[5] The definitions are particularly critical when it comes to AI-related matters, as the possibility of regulatory disconnection is relatively high due to the high pace of technological advances.[6]

The main purpose of this chapter is to discuss whether, by introducing these new categories, the AIA can harmonize the understanding and protection of biometric data, currently regulated by messy and somewhat inadequate provisions in different pieces of legislation.

For this purpose, Sect. 5.2 provides an overview of selected regulatory frameworks that are part of the efforts of the EU legislators in targeting the use of biometric data: the LED, the Payment Service Directive II (PSDII), the Schengen Information System II framework (SISII) and the European Digital Identity Regulation, i.e., eIDAS 2.0—that explicitly or implicitly govern AI-system biometric data. Following this descriptive section, we analyse divergent interpretations, gaps, areas of potential loopholes, and overlaps in these instruments.

Section 5.4 discusses the AIA and evaluates whether it can provide broader protection by harmonizing the current definitions or if it would create more confusion. Finally, we conclude that although the AIA seeks to enhance fundamental rights and data protection by introducing new definitions of biometric data, it may not effectively unify or clarify the concerns discussed below.

[3] Sumer 2022, p. 3.

[4] See for example: Kindt 2018; Jasserand 2016.

[5] Roznai 2014.

[6] As put by Brownsword and Goodwin: '*Indeed, one of the great regulatory ironies is that, where regulators (in an attempt to regulate, know where they stand) try their utmost to establish an initial set of standards that are clear, detailed and precise, the more likely it is that the regulation will lose connection with its technological target (leaving the regulation unclear as to their position)*' Brownsword and Goodwin 2012, p. 400.

8.2 Biometric Data in Regulatory Instruments

This section explains the legal concept of biometric data as personal data under several EU legal instruments, starting with the GDPR and LED and subsequently focusing on the sectoral legislations: eIDAS 2.0, PSD II, and SIS II. This preliminary inquiry demonstrates that there is no harmonised understanding of biometric data within the analysed framework.

8.2.1 Biometric Data as Personal Data

8.2.1.1 The General Data Protection Regulation

The GDPR replaced the former Data Protection Directive 95/46/EC, which contained no reference to biometric data; it was the first general EU regulation that included a definition of biometric data.[7] Article 4(14) defines biometric data as *personal data resulting from specific technical processing* relating to a natural *person's physical, physiological, or behavioral characteristics, which allow or confirm the unique identification* of that natural person, such as *facial images or dactyloscopic data.*

At the same time, Recital 51 further states *the processing of photographs* should not systematically be considered to be the processing of *special categories*, as they are covered by the definition of biometric data only when processed through a *special technical means* allowing *the unique identification* of a natural person. Hence, it seems that the GDPR distinguishes between 'mere' photographs (i.e., images for biometric recognition purposes) and photographs that are 'processed through special technical means' for the specific purpose of identification or verification. The GDPR seems to neglect the possibility that biometric images (before transformation) can also be sensitive data if their processing reveals sensitive information, such as ethnicity or health information.[8] The legal definition does not consider images of biometric characteristics, e.g., photographs, as sensitive data under Article 9. Thus, these images can be collected, centralised and processed for various legal reasons, including legitimate interests and marketing under Article 6.

Furthermore, there is uncertainty as to which biometric functionalities are prohibited by Article 9.1 GDPR, which states that (only) biometric data for *the purpose of uniquely identifying a natural person* shall be prohibited. A discrepancy between Art. 4(14) and Recital 51 in describing the functions/purposes should be observed, as the definition of biometric data under GDPR Article 4(14) seems incompatible with Recital 51. The definition makes a distinction between the functions of '*to confirm the unique identification*' (which contains the identity verification (1:1) function) and '*to allow the unique identification*' (which covers the biometric identification

[7] Regulation (EU) 2016/679 (GDPR); Kindt 2013.

[8] For a detailed discussion on this issue see: Sumer 2022, p. 3. See also, ECJ case on sensitive info inferences, August 2022.

(1:N) function). Some argue that both biometric verification and identification may be covered (and hence prohibited).[9] According to this view, biometric data associated with a specific person and utilised for biometric recognition (identification and verification) are considered sensitive.[10] Others interpret 'uniquely identifying' more narrowly as only referring to the identification functionality.[11] It should be noted that Recitals are, in principle, not legally binding. However, the exclusion of biometric verification from more stringent protection of Article 9(1) might pose risks to fundamental rights and freedoms. Recently, the EDBP clarified that both biometric identification and verification process sensitive personal data,[12] influencing some Data Protection Authorities (DPAs), like the AEPD (Agencia Española de Protección de Datos) (Spanish DPA), to treat biometric verification as processing special categories of data under the GDPR.[13]

8.2.1.2 The Law Enforcement Directive (LED)

The LED aims to protect citizens' fundamental right to data protection whenever criminal law enforcement authorities use personal data for law enforcement purposes.[14] It will, in particular, ensure that the personal data of victims, witnesses, and suspects of crime are duly protected, which will facilitate cross-border cooperation in the fight against crime and terrorism.[15]

Article 3(13) LED defines biometric data identically to the GDPR, and is also including a provision on special categories (Article 10), but there is no equivalence of Recital 51.[16] As explained below, some argue this might mean that the LED refers to and governs biometric images that have not been technically processed.[17] It is widely known that automated biometric systems used by police authorities, such as the Automated Fingerprint System (AFS), process images, e.g., photographs (and not templates). Therefore, one could argue that biometric images, such as photographs, may not be *a priori* excluded as falling under the category of biometric data under the LED, which diverges from the definition in the GDPR.

---

[9] Jasserand 2016 views 'allowing' and 'confirming' the unique identification as referring to the umbrella function of biometric recognition'. p. 309.

[10] Jasserand 2016, p. 309.

[11] Kuner et al. 2021, pp. 51–52 and Kindt 2018, p. 527 argue that Article 9(1) does not cover biometric verification. Also see, Clifford 2019, pp. 177–184; Tamas et al. 2021, p. 2.

[12] EDBP 2023, p. 10.

[13] AEPD, 2023, p. 13.

[14] Directive (EU) 2016/680 (Law Enforcement Directive or LED).

[15] https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#legislation [Accessed 3 March 2024].

[16] Also see: Jasserand 2019, p. 157.

[17] Other related legislations in the area of freedom, security and justice can also be considered related to the scope of the, 'LED' Davoli 2023, pp. 2–4.

8.2.2 Biometric Data in Other Sectoral Regulations

8.2.2.1 The eIDAS Regulation and the Amending Proposal (eIDAS 2.0)

The eIDAS Regulation (2014) governs trust in the context of online identity verification.[18] The European Commission, on June 3, 2021, proposed to amend the eIDAS Regulation with a view to updating it to a European Digital Identity Regulation.[19] Both the eIDAS Regulation and the Proposal do not explicitly define biometric data.

However, as in practice, biometrics are often used in AI-based authentication layers, e.g., for unlocking a device or securing access to premises. The eIDAS 2.0. proposal referred to authentication based on biometric data as an assurance factor in its Recitals. Recital 11 indicated that the stakeholders should consider the different levels of risk. It stated that processing biometric data to authenticate is one of the identification methods providing a high level of assurance and refers to the risks that the processing may entail for the rights and freedoms of individuals and the GDPR, hence acknowledging biometric data's 'sensitive nature'.[20]

During negotiations, the Committee on Industry, Research, and Energy (ITRE) suggested more stringent obligations for processing biometric data in the eIDAS 2.0 regulation.[21] Amendments to the Proposal clarified that using biometrics to identify and authenticate should not be a must for using the European Digital Identity Wallet[22] and that biometric data used in the context of eIDAS should not be stored without the user's explicit consent.[23] ITRE was explicitly in favour of limiting the use of biometric data to specific scenarios under Article 9 of the GDPR. Moreover, stakeholders that intend to process sensitive personal information, such as health or biometric data, as defined by Article 9 GDPR, would need prior approval from the competent authorities in the Member State in which they intend to provide their services. In addition, these stakeholders were supposed to comply with the legal bases in Article 6(1) GDPR.[24]

However, the text adopted by the Parliament excluded all these biometric data-specific provisions in the adopted position. It only referred to a concept of 'inherence' to regulate biometric data as a *strong user authentication* factor.[25] This broad concept is analysed in the following section under the PSDII.

[18] Regulation (EU) 2014/910 of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.

[19] Eidas 2.0. proposal, 2021.

[20] Eidas 2.0. proposal, 2021, Recital 11.

[21] ITRE 2021/0136, Recital 11, p. 16.

[22] The wallet is a piece of hardware and software that will store different types of personal data, including biometric data. Sumer and Schroers 2021.

[23] ITRE 2021/0136, Recital 11, p. 16.

[24] Eidas 2.0. proposal, 2021 Recital 11.

[25] European Parliament 2024, Article 3 (j) (51).

8.2.2.2 Payment Service Directive II (PSD II)

PSDII applies to payment services provided in the EU and addresses specific aspects of digital identity authentication regarding financial transactions. It allows for processing personal data for payment authentication and fraud prevention.[26] PSDII requires '*strong customer authentication',* which means an authentication based on the use of two or more elements categorised as:

- knowledge (something only the user knows, e.g., passwords);
- possession (something only the user possesses, e.g., devices);
- inherence (something the user is, e.g., biometric data).[27]

Biometric data is not explicitly defined in the PSDII but is indirectly referred to in the context of authentication like eIDAS particularly *strong customer authentication*, which includes the category of *inherence*: something a user is and relates to their physical or behavioural characteristics, as mentioned in the GDPR definition of biometric data.[28] However, the concept here goes beyond what the GDPR covers, as it might refer to any biometric characteristics that can be used for authentication, including such as e.g., keystrokes, walking patterns, or eye movements.

Moreover, PSDII defines sensitive payment data as '… *data, including personalised security credentials which can be used to carry out fraud* …'.[29] Therefore, sensitive data in the payment context include all data enabling user authentication, including biometric data. Such data processing must comply with the GDPR, as acknowledged in the Guidelines on the interplay of the Second Payment Service Directive and the GDPR by the European Data Protection Board (EDPB).[30]

8.2.2.3 Biometric Data in the Schengen Information System (SIS)

Biometric data processing is also considered a significant means to enhance security in the context of border control. This function can already be found in the first-generation Schengen Information System (SIS), a precursor EU-wide large-scale system established in 1995 to support the free movement within the Schengen Area.

---

[26] Directive (EU) 2015/2366.

[27] Strong customer authentication "means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data." Directive (EU) 2015/2366, Article 4(30).

[28] This interpretation is common in scientific literature and industry practice. Particularly see: Suleski and others, 2023; European Banking Authority 2020, On the requirements for "inherence" in strong customer authentication (SCA), https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5353 Accessed 13 February 2024.

[29] *Sensitive payment data* means data, including personalized security credentials which can be used to carry out fraud.' Directive (EU) 2015/2366, Article 4(32).

[30] EDPB 2020, p. 4.

SIS is Europe's most widely used and largest information-sharing security and border management system.[31] SIS consists of different legal instruments, such as the one that contributes to police[32] cooperation between Member States, the one ensuring security in external border control[33] by enabling competent authorities to enter and consult alerts on specific categories of wanted or missing persons and migrants in an irregular situation.[34] Each of the objectives mentioned above is regulated by different regulations. Following several revisions, the new second-generation SIS framework (SIS II) became fully operational as of March 2023.[35]

Due to the limitations of the first-generation search method based on biographical data (e.g., name, surname), the modernized SIS II heavily relies on biometric data processing by storing dactyloscopic data (i.e., fingerprints and palm prints), photographs, and facial images for person-related alerts. Additionally, DNA profiles can be entered under SIS II as a last resort to identify a person in the context of police and criminal justice cooperation.[36] Furthermore, Article 42 of the SIS II police cooperation lays down specific rules on biometric data processing. It requires complying with minimum quality standards for each biometric identifier before its storage in the SIS II.

In the context of SIS Regulations for police cooperation and border checks, biometric data encompasses *photographs, facial images, dactyloscopic data.* At the same time, DNA information is only referred to as biometric data under SIS II police cooperation.[37]

SIS II Return does not define biometric data and only refers to the personal data definition under the GDPR.[38] Besides, unlike the GDPR, the other two SIS Regulations do not include behavioural characteristics when defining biometric data.

Another point of divergence would be that they treat photographs and DNA information as biometric data. For the former, the SIS regulations distinguish photographs from facial images, specifying both of them as biometric data without addressing the nuances stressed in Recital 51 GDPR. For the latter, it is essential to note that DNA

[31] European Commission 2023, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en Accessed 3 March 2024.

[32] Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, (SIS II police cooperation).

[33] Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks| (SIS II border checks).

[34] Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals, (SIS II Return).

[35] For more details, see, EULISA 'Large-scale IT systems' available at: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Sis-Ii Accessed 3 March 2024.

[36] SIS II police cooperation, 2018/1862, Article 42 (3).

[37] SIS II police cooperation, 2018/1862 'biometric data' means personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, namely photographs, facial images, dactyloscopic data and DNA profiles' Article 3(12).

[38] SIS II for return, 2018/1860 Article3(11).

information would be covered within the scope of *genetic data* under the GDPR and LED rather than biometric data.[39] This distinction is crucial because, unlike biometric data, the processing of genetic data under the GDPR and LED does not hinge on the condition of processing '*for the purpose of uniquely identifying*' to be considered as special categories of personal data. Thus, against the diverging classification of DNA information as biometric data under SIS II police cooperation, its processing falls within the special categories of data processing within the scope of LED. Hence, its processing would fall under special categories of data processing regardless of the heated discussions on purpose-based biometric sensitive data processing, as discussed above.

8.3 Critics of Pre-AIA Regulations of Biometric Data

The definition of Article 4(14) GDPR, which is *lex generalis*, seems to deviate from and does not align with the (earlier) concepts and understanding of biometric data in specific legislation for specific domains, such as in SIS II regulations used in the border context. We mention some main points of attention hereunder.

First, the GDPR's definition of biometric data is not without debate and discussion. As mentioned, the definition encompasses four main constitutive elements as follows:

(i) personal data;
(ii) specific technical processing;
(iii) relating to the physical, physiological, or behavioural characteristics of a natural person;
(iv) which allows or confirms the 'unique identification' of that natural person.

In particular, *specific technical processing* and *unique identification* elements have been subject to critical scrutiny in academic literature. First of all, the phrase 'specific technical processing' is not defined. Therefore, it has created confusion about what 'technical processing' entails and under which circumstances biometric data falls in the sensitive data regime.

Scholars have pointed out that the GDPR allows for collecting and storing biometric data as images for other purposes, e.g., a list of employees or contact persons with facial images, without falling under the prohibition of Article 9 GDPR.[40] Such collection could arguably be based on the less strict data processing regime of Article 6 of the GDPR, which allows, for example, processing based on consent or legitimate interest. The option of processing the images of biometric characteristics based on Article 6 opens the door to a weakened level of protection for processing biometric data of people. Moreover, the GDPR's approach, in particular the prohibitions in Article 9(1) GDPR, relying on the criterion of the processing for identification

[39] Recital 34 and Article 4(13) GDPR 2016/697; Recital 23 and Article 3(12) 2016/680.
[40] Kindt 2018, p. 6; Sumer 2022, p. 3.

purposes as the trigger for the need for more protection, offers only partial protection, *i.e.,* against identification, and not against, e.g., function creep (e.g., use by law enforcement) after collection and, e.g., central storage. Considering the discussions in the literature, it is evident that the purpose criterion in the GDPR may not be regarded as ideal.

Secondly, the functional criteria for *uniquely identifying'* is one significant reflection of the GDPR's general risk-based approach. Identification of an individual is indeed a considerable risk. However, considering both technical definitions and the scope of the data protection legislation, delineating biometric data to only the biometric data that can uniquely identify an individual lacks the necessary comprehensiveness of the risks of processing such data. For example, behavioural biometric characteristics may not, in all circumstances, allow unique identification; however, they may reveal critical data, e.g., emotions and sensitive information such as ethnicity, that might be used to profile individuals. For example, facial data points are often used to identify human emotions without necessarily uniquely identifying individuals.

The other legislative frameworks and proposals use different technical terms interchangeably, such as authentication (eIDAS) and identification (GDPR), without further explanations, adding to the confusion. For example, eIDAS and PSDII regulate biometric verification (1:1). However, once collected, these biometric data could also be used for identification purposes. Although eIDAS and PSDII are *lex specialis*, they both refer to the GDPR provisions without providing their own definitions of biometric data. Therefore, the legal debates on how to read the GDPR's definition of biometric data remain relevant here.

Some of such divergences among the definitions of biometric data might be considered reasonable, especially between public/private and law enforcement-related regulations, i.e., LED and GDPR serve different purposes. Furthermore, the differences between the instruments pursuing a general purpose (GDPR/LED) and those that are meant to be adopted for a specific purpose, hence the *lex specialis* (border control, payments, or digital identity management) might be justifiable. In the latter, biometric data might be defined or is to be understood differently due to such specific purposes. For example, what is considered a biometric facial image in SIS II is not necessarily biometric data under the GDPR or LED. In SIS II, facial images are exemplified as biometric data and fall in the category of biometric data based on their quality to perform facial recognition. In the GDPR, facial images must be subject to 'specific technical processing' (to be transformed) to be considered biometric data.

As mentioned, the definition of biometric data varies even within the SIS II legal framework. On the one hand, SIS regulations conceive a broader understanding of biometric data, including photographs. On the other hand, a notable narrower scope excludes behavioural biometric data and limits the scope of biometric data to an exhaustive list mentioned in the definition. One could argue that, under the SIS II framework, the legislator favours and strengthens a context-dependent definition of biometric data by emphasizing the purpose of biometric data processing for police cooperation or border checks rather than adhering to the GDPR's primary definition.

8.4 Post-AIA Understanding of Biometric Data

This section provides an overview of definitions subject to negotiations during the AIA's official adoption process. In addition to the official AIA, we discuss the negotiation process, relying on the official texts available, which are mainly the Commission's Artificial Intelligence Act (AIA) proposal and the following adopted texts, i.e., the EU Parliament's draft report (2021) and amendments adopted by the European Parliament on June 14 2023 on the Proposal.

The EU Commission's AIA proposal[41] is part of its European AI Strategy, which aims to make the EU a world-class hub for AI and attempts to ensure that AI is human-centric and trustworthy.[42] The AIA proposes a risk-based approach to using, developing, and deploying AI systems based on four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk. This framework specifically identifies and regulates '*real-time*' and '*post*' remote biometric identification and categorisation by AI systems as forbidden or high-risk AI systems. Such systems are consequently subjected to the rigorous stipulations outlined in the AIA.

In addition to the Commission's proposition to regulate biometric identification, the discussions of the Proposal by the Council and the EU Parliament led to attempts to extend regulatory measures beyond this specific function. The Council proposed a new definition of biometric data in November 2022, removing the controversial *unique identification* prerequisite from the definition.

During the negotiations, more types of use of biometric data, such as for emotion recognition and biometric categorisation have been discussed, of which some are considered in particular domains at first as high-risk, including the amendment to Article 5(1), which addresses '*the placing on the market, putting into service or use of AI systems to infer emotions of a natural person in the areas of law enforcement, border management, in workplace and education institutions*'.[43] The Proposal in Recital 7 states: '*The notion of biometric data used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of [GDPR*].' In conformity with this, Article 3(33) provided an identical definition of biometric data as in the GDPR.

The European Parliament's compromised text, adopted on June 14, 2023, added the concept of 'biometrics-based' data and distinguished between biometric data as understood in the GDPR and biometrics-based data. According to this text, 'biometrics-based data are additional data *resulting from specific technical processing* relating to physical, physiological or behavioural signals of a natural person, such as facial expressions, movements, pulse frequency, voice, key strikes or gait, which *may or may not* allow or confirm the unique identification of a natural person'.[44] The biometric data is defined in the amended text in article 33a as 'data resulting

[41] European Commission 2021 AIA proposal.

[42] European Commission 2023, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, Accessed 28 February 2023.

[43] European Parliament 2023, Amendment 219, Article 5(1).

[44] European Parliament 2023, Amendment 21 (Recital 7).

from specific technical processing relating to physical, physiological or behavioural *signals* of a natural person' (italics added). While this is similar to the GDPR, 'signals' seem broader than 'characteristics', and the purpose of processing is not mentioned. The 'biometric-based data' category encompasses data used by biometrics-based systems, including 'emotion recognition systems' and 'biometric categorisation'. The latter two concepts or terms were also discussed and defined in the earlier versions of the AIA proposal; however, they were not included in the agreed draft, so we will not discuss them in detail here.[45]

Against this background, followed by a draft agreement AIA was adopted following lengthy negotiations. According to the unofficial draft agreement on the basis of the final AIA, the EU seems to have abandoned both the Commission's and Parliaments' view and introduced a different definition of biometric data—according to which the requirement for *allowing or confirming unique identification* is not considered a prerequisite for the qualification of biometric data. By recognising that *unique identification* may not always be the primary purpose of all use of biometric data, the AIA covers all personal data relating to the physical, physiological or behavioural characteristics from the human body if resulting from technical processing, broadening the scope of the protection offered by the GDPR and the LED.[46] The AIA seems to circumvent the problem by using the legal definition of (GDPR) to include new data types within the scope of biometric data. As mentioned, this is a critical development as not all biometric data are processed to identify an individual, yet they are still sensitive. The main reason for this sensitivity is that, in many AI applications, biometric data are processed to infer emotions (emotion recognition) or categorise people, i.e., biometric categorisation systems, according to shared biometric features revealing sensitive aspects, e.g., gender and ethnicity (Table 8.1).

Recital 14 AIA states that biometric data should be interpreted in light of Article 4(14) of the GDPR and such data can a*llow for the authentication, identification and categorisation of natural persons and for the recognition of emotions* of persons. Yet, the AIA introduces a subtle distinction between the notion of biometric data in the data protection instruments and in the AIA. These definitions are similar but different, as the AIA definition does not refer to the functional purpose of the GDPR.

It should be noted that the scope and the regulatory frameworks governing different biometric applications and functions need attention and a comprehensive approach. The AIA's definition of biometric data can be considered logical and more comprehensive for the protection of fundamental rights. Yet, it risks further confusion when

[45] European Parliament 2023, Amendment 23 to Recital 16 in AIA defines biometric categorisation as assigning natural persons to specific categories or inferring their characteristics and attributes such as gender, sex, age, hair colour, eye colour, tattoos, ethnic or social origin, health, mental or physical ability, behavioural or personality, traits language, religion, or membership of a national minority or sexual or political orientation on AIA and Article 3(39) to Article 3(1) 34: 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions, thoughts, states of mind or intentions of natural persons on the basis of their biometric data.

[46] Regulation (EU) 2024/1689 AIA.

Table 8.1 Transformation of biometric data definitions during the AIA negotiations. *Source*: EU AI Documents. (2024). The Artificial Intelligence Act. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Commission proposal	EP mandate	Council mandate	AIA
(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	(33) biometric data as defined in Article 4, point (14) of Regulation (EU) 2016/679 (33a) biometric-based data' means data resulting from specific technical processing relating to physical, physiological or behavioural signals of a natural person	(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data	3(34) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data

read together with the GDPR's definition of biometric data which may also be applicable to e.g., facial images collected by an AI system using these images for emotion recognition to which the AIA definition of biometric data would apply. While the AIA attempts to provide an additional layer of protection, it does not necessarily harmonise or bring more clarity to the issues discussed in the previous sections.

8.5 Conclusion

The GDPR's narrow and functional definition of biometric data has been subject to academic debates for its limited scope in protecting fundamental rights and creating legal uncertainty. At the same time, other legislation introduced above either replicate the GDPR's definition, deploys its own concepts or refer to the GDPR definition without further elaborating on it. Indeed, regulations such as the eIDAS and the PSDII include specific provisions and uses relating to biometric data, which deviate from the general concept and understanding of the GDPR's definition of biometric data. The reliance is precarious as the GDPR provides limited protection in this context. Consequently, this regulatory landscape for biometric data processing has resulted

in a diverse environment with potential discrepancies in the level of protection. The precise interplay between the GDPR and these evolving regulations, which are currently undergoing revision, also remains uncertain.

In response to this uncertainty, the AIA Proposal seeks to address some applications and AI systems on a case-by-case basis and for specific domains only. On top of this, it specifies various uses of identification systems by law enforcement by offering a more detailed definition of identification systems ('real-time' as opposed to 'post' identification). As such, the AIA is expected to play a pivotal role in regulating the risks for these specific biometric applications.

On the other hand, instead of bringing clarity, the AIA may create more confusion when read together with the GDPR's definition of biometric data. For policymakers, it is imperative to reassess and consolidate the definition and regulation of biometric data with clear guidance. We argue that enacting specific and designated legislation with a harmonized approach for defining biometric data is necessary.

References

Brownsword R, Goodwin, M (2012). Law and the Technologies of the Twenty-First Century. Cambridge University Press.

Bygrave LA (2010) The Body as Data? Biobank Regulation via the 'Back Door' of Data Protection Law. Law, Innovation and Technology, 2:1: 1–25.

Clifford D (2019) The Legal Limits to the Monetisation of Online Emotions KU Leuven PhD available at https://www.law.kuleuven.be/citip/en/research/phd-research/finalized/phd-damian-clifford Accessed February 13 2024.

Davoli A (2023) Judicial Cooperation in Criminal Matters. Fact Sheets on the European Union, pp 1-7 https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_4.2.6.pdf Accessed 13 February 2024.

EDPB (2020) Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR Version 2.0.

EDPB (2023), Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, April 26 2023, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en Accessed February 13 2024.

European Commission (2023) 'Data protection in the EU' (*European Commission website*) https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en Accessed February 13 2024.

European Parliament (2022) Draft Report on the Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (Com(2021)0281 – C9-0200/2021- 2021/0136 (COD)) Committee on Industry, Research and Energy.

Foucault M (2008) *The Birth of Biopolitics*, Palgrave Macmillan.

Gates KA (2011) Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York University Press, New York.

George ER (2022) Bias and Biometrics: Regulating Corporate Responsibility and New Technologies to Protect Rights. Notre Dame Journal Int'l & Comp. L. 12(2) Article 3.

Jasserand C (2016) Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data. Eur. Data Prot. L. Rev. 2 (3):297–311.

Jasserand C (2019) Reprocessing of Biometric Data for Law Enforcement Purposes: Individuals' Safeguards Caught at the Interface between the GDPR and the 'Police' Directive? (PhD Thesis) https://research.rug.nl/en/publications/reprocessing-of-biometric-data-for-law-enforcement-purposes-indiv Accessed February 13 2024.

Kindt EJ (2013) Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis, Dordrecht, Springer.

Kindt EJ (2018) Having yes, Using no? About the New Legal Regime for Biometric Data. Computer law & security review 34(3):523–538.

Kuner C et al. (2021) "The EU General Data Protection Regulation: A Commentary/Update of Selected Articles." Update of Selected Articles, May 4, 2021 https://doi.org/10.2139/ssrn.3839645 Accessed February 13 2024.

Kindt EJ (2022) 'Chapter 18. "Biometric data processing: Is the legislator keeping up or just keeping up appearances ?' in G. Gonzalez Fuster, R. Van Brakel and P. De Hert (eds.), *Privacy and Data Protection Law: Values, Norms and Global Politics*, Cheltenham U.K. and Massachusetts, U.S.A., Edward Elgar Publishing, Research Handbook.

Prabhakar S, Pankanti, S, Jain, AK (2003) Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy, pp.33–42.

Rose N (2000) 'Government and Control' (2000) 40 The British Journal of Criminology 321.

Roznai Y (2014) A Bird is Known by its Feathers'—On the Importance and Complexities of Definitions in Legislation. The Theory and Practice of Legislation, 2.2: 145–167.

Spanish Data Protection Authority (AEDP) AEPD, 'Guía sobre Tratamientos de Control de Presencia Mediante Sistemas Biométricos v. November 2023' (2023) https://www.aepd.es/documento/guia-control-presencia-biometrico.pdf Accessed 13 February 2024.

Suleski T et al. (2023) A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9.

Sumer B (2022) When do the Images of Biometric Characteristics Qualify as Special Categories of Data under the GDPR?: A Systemic Approach to Biometric Data Processing. 2022 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE.

Sumer B, Schroers J (2021). The new digital identity Regulation proposal and the EU data protection Regime. CiTiP Blog. https://www.law.kuleuven.be/citip/blog/the-new-digital-identity-regulation-proposal/ Accessed February 13 2024.

Tamas B et al. (2021) Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks. 2021 International Conference of the Biometrics Special Interest Group (BIOSIG). IEEE.

Legislations

Directive (EU) 2015/2366 of the European Parliament and of the Council of November 25 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

Directive (EU) 2016/680 of the European Parliament and of the Council of April 27 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 (hereinafter Law Enforcement Directive or LED).

Regulation (EU) 2014/910 of the European Parliament and of the Council of July 23 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 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).
Regulation (EU) 2018/1860 of the European Parliament and of the Council of November 28 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (Consolidated version).
Regulation (EU) 2018/1861 of the European Parliament and of the Council of November 28 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 (Consolidated version).
Regulation (EU) 2018/1862 of the European Parliament and of the Council of November 28 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 (Consolidated version).
Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Draft regulations and proposals

Council of the EU, The Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (hereinafter Draft AIA), 2021/016 (COD) - Analysis of the final compromise text with a view to agreement.
Draft European Parliament Legislative Resolution on the Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)), available at https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html Accessed February 13 2024.
European Parliament (2023) Amendments adopted by the European Parliament on June 14 2023 on the Proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
Position of the European Parliament adopted at first reading on February 29, 2024, with a view to the adoption of Regulation (EU) 2024 of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final (eIDAS 2.0 proposal).
Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts COM/2021/206 final.

Bilgesu Sumer is a doctoral researcher at KU Leuven (CiTiP) and a Biometric Law Lab (BLL) member. Her research focuses on the data protection implications of biometrics, AI, and blockchains.

Natalia Menéndez González is a Ph.D. candidate at the European University Institute, where she researches the proportionality within the use of Facial Recognition Technology. She is also a Research Assistant at the Centre for a Digital Society, a teaching assistant at the School of Transnational Governance, a co-founder of The DigiCon blog, a visiting researcher at the Biometrics Law Lab of the Center for IT and IP Law at the KU Leuven Faculty of Law and Criminology and former vice-chair of the Ph.D. students in AI Ethics research group. Her other research interests include AI Ethics, especially for Natural Language Processing, and the intersection between artificial intelligence and democracy.

Abdullah Elbi is a legal researcher at KU Leuven (CiTiP), and a member of Biometric Law Lab (BLL). His research focuses on fundamental rights implications of emerging technologies with particular interest in trustworthy artificial intelligence, biometrics, and voice assisstances. He has been involved in various EU and national level research Projects such as iMARS, FAITH, and SALT.

Catherine Jasserand is an assistant professor at the University of Groningen (Netherlands) within the STeP research group. She is an expert in law, AI, and biometrics. Between 2020 and 2023, she was part of the Biometric Law Lab (BLL) at KU Leuven as a Marie Skłodowska-Curie postdoctoral fellow. There, she investigated the impact of facial recognition technologies use in public spaces on the rights to privacy and data protection as part of the MSCA-IF project DATAFACE).

Jan Czarnocki is a Doctoral Researcher and Maria Skłodowska-Curie Fellow at the KU Leuven Centre for IT and IP Law in Belgium, and a member of the Biometric Law Lab (BLL). His work intersects the domains of law, philosophy, technology, and policy. Jan was also recognized as a Non-Resident Fellow at the Stanford Law School Transatlantic Technology Law Forum and an Affiliated Fellow at the Jagiellonian University Private Law of Data Project.

Els J. Kindt is an associate professor and senior research fellow with eLaw of Universiteit Leiden, the Netherlands, respectively the Centre for IT and IP Law (CITIP) of KU Leuven, Belgium. She has been an expert in law and biometrics for over 20 years. In 2020, she set up the Biometric Law Lab (BLL) for exchanging legal knowledge in this domain.