A First Attempt at Regulating Biometric Data in the European Union

Els Kindt (KU Leuven)

INTRODUCTION

In 2004, the European Union ("Union") enacted legislation that obligated Member States ("MS") to store facial images and fingerprints in citizens' passports and travel documents.[1] Around the same time, the Union set up large-scale databases containing the biometric data of asylum and visa seekers and an information system for protecting the Schengen Area.[2] It wasn't long before this spilled over into public and private entities, which began using biometric data for crowd control, access control in the workplace, and monitoring in schools. While acknowledging that the use of biometric technology has many potential benefits, the Council of Europe warned that biometric data should be considered as "sensitive" data that presents risks, because it contains information about health and race, has the ability to identify people, can make it easier to link records, and is irrevocable.[3]

---

1 EU Regulation No 2252/2004, December 13, 2004.

2 Consider, for example, Eurodac, the Visa Information System (VIS), and the Schengen Information System (currently SIS II), which all emerged after 2000. Biometric data remains central to the Union's information systems, including the European Travel Information and Authorisation System (ETIAS), the Entry/Exit System (EES) (Regulation No 2017/2226), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN), as is clear from the recent interoperability framework (Regulation No 2019/817 and Regulation No2019/818).

3 See Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (Strasbourg: 2005), and the updated Progress Report of 2013, T-PD(2013)06, https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81. The Council of Europe adopted the European Convention on Human Rights in 1950, and the Convention No.108 on data protection in 1981, as revised in 2018 (Convention No. 108+). The Council of Europe consists of forty-seven Member States and is distinct from the European Union.

Despite the risks, the general data-protection framework and most national legislation did not contain specific provisions on biometric data use and processing,[4] and guidance remained limited while these technologies were being developed.[5] To address these gaps, some national supervisory data protection authorities (SAs) developed frameworks for biometric use.[6] As part of these frameworks, SAs have focused on the sensitive nature of the data, the risks of maintaining databases, and the possibility of "function creep."[7] The SAs also focused on whether the use of biometrics was proportionate to the legitimate aim sought to be achieved (i.e., the "proportionality principle"), leaving much room for discretionary policy considerations and unpredictable outcomes when applying the proportionality principle.[8]

It was against this backdrop that the Union introduced the General Data Protection Regulation 2016/679 (GDPR) in 2016. The regulation is directly applicable in Member States and includes provisions for both public and private biometric data processing. The Union also introduced Directive 2016/680 (Data Protection Law Enforcement Directive, or DP LED), which applies specifically to personal data processing for the prevention, detection, investigation, or prosecution of crime by law enforcement authorities (LEAs).

THE EU'S REGULATORY APPROACH TO BIOMETRIC DATA PROCESSING

Both the GDPR and DP LED provide, for the first time, a definition of biometric data: "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

4 See Directive 95/46 and Framework Decision 2008/977/JHA. "Processing" is understood very broadly, and is defined as "any operation or set of operations . . . whether or not by automated means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4(2), GDPR). Only a few Member States introduced specific legal provisions, e.g., France, Article 25 and 27 Act No. 78-17.

5 See e.g., the Article 29 WP, Working Document on Biometrics 2003 (WP 80), Opinion 2/2012 on facial recognition in online and mobile services (WP192), and Opinion 3/2012 on developments in biometric technologies (WP193).

6 This is done by advising, adopting opinions, and issuing guidelines, authorizations, restrictions, and bans. See, e.g., for France, Claire Gayel, "'The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations," *Computer Law & Security Review* 32, no. 3 (June 2016), 450–461, https://doi.org/10.1016/j.clsr.2016.01.013.

7 This can happen, for example, when an agency uses the data for something other than its original purpose (e.g., for law enforcement purposes). See also CNIL, "Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données," Communication central storage fingerprint, December 28, 2007, https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf.

8 The proportionality principle is an important principle in data-protection legislation. It requires that the processing is lawful and the data adequate and relevant and not excessive for the purpose specified. When interfering with human rights, the proportionality principle requires in addition a three-step test: that there is accessible and sufficiently certain law allowing the interference ("rule of law"); a legitimate aim; and *necessity in a democratic society*. For assessing the latter, one needs to determine whether (1) the interference answers a "pressing social need," (2) the argued reasons for deploying the interference are relevant and sufficient, and last but not least (3) whether all of this, in particular the interference (in our case the use of biometric technology), is in proportion with the legitimate aim pursued. As there remained confusion about the need for double review and because there was also lack of clarity about the three-pronged approach, this resulted in divergent and unpredictable outcomes when applying the proportionality principles and in broad "margins of appreciation." See also E. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Dordrecht: Springer, 2013), 403 et seq. and 621 et seq.

person, such as facial images or dactyloscopic [fingerprint] data."[9] A particularly noteworthy aspect is the "specific technical processing"[10] component, which effectively excludes "raw" data stored and retained in databases (e.g., of facial images captured on CCTV, voice recordings, or fingerprints),[11] or when published on a website or social network. The GDPR accounts also mention that the "processing of photographs should not systematically be considered to be processing of special categories of personal data..."[12] Video footage of an individual is also not considered biometric data as long as it has not been specifically technically processed in order to contribute to the identification of the individual.[13]

While the GDPR states that "processing of biometric data for the purposes of uniquely identifying" is prohibited,[14] there are many exceptions to this prohibition, including when the data "are manifestly made public" or if processing is "necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."[15] Because the exceptions remain vague (e.g., "substantial public interest'") and are numerous,[16] the GDPR still allows the processing of biometric data in many circumstances, including those where people give explicit consent.[17] Finally, the GDPR specifies that Member States may maintain or introduce further conditions or limitations.[18]

---

9 Article 4(14) GDPR and Article 3(13) Directive 2016/680. The technical process is likely to be understood as a biometric technical processing. The original definition in the EU Commission's GDPR proposal of January 25, 2012 COM(2012) 11 final and in the European Parliament's position in its first reading of April 13, 2014 was broader: "'biometric data' means any [personal data] relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data" (Article 4(11)). Experts view this definition as narrow and contrary to a general understanding of biometric data. For examples, see the ISO/IEC 2382-37 Information Technology—Vocabulary—Part 37: Biometrics (2017), where "biometric data" (3.3.6) includes both biometric samples (analog or digital representations of biometric characteristics), hence the initial or "raw" data, and the technically processed data thereof. See also EES, where biometric data is defined as including images: "'biometric data' means fingerprint data and facial image" (Regulation 2017/2226, article 3.1 (18)). On the biometric terminology and possible confusion, see also Catherine Jasserand, "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data," *EDPL* 2, no. 3 (2016): 297–311, https://doi.org/10.21552/EDPL/2016/3/6.

10 Added by the Council of the Union, composed of the heads of the Member States and governments. See Council doc. 15395/14, December 19, 2014, https://www.statewatch.org/media/documents/news/2014/dec/eu-council-dp-reg-15395-14.pdf. This modification was requested and added to the initially proposed definition and finally adopted. On the origin of this modification, see E. J. Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data," *Computer Law & Security Review* 34, no. 3 (June 2018):523–538, https://doi.org/10.1016/j.clsr.2017.11.004. This article also contains a graphic showing what counts as biometric data and not, and which legal provisions apply.

11 For example, the collection of facial images by governments to issue identity documents, and their storage in databases.

12 Rec. 51 GDPR. See also EDPB, *Guidelines 3/2019 on Processing of Personal Data through Video Devices, on Video Surveillance*, January 29, 2020, § 74 ("EDPB Guidelines 3/2019 on video devices").

13 Ibid.

14 Article 9.1 GDPR. The general prohibition was an amendment requested by the European parliament (EP) to the original proposal of the EU Commission. The processing of biometric data was hereby hence added to the list of special categories of data. EP first reading, T7-0212/2014, March 12, 2014. This followed the 2012 suggestions of the Council of Europe's Consultative Committee working on the modernization of Convention No. 108. Compare with Article 6.1 of Convention 108+ of the Council of Europe. The words "for purposes of uniquely identifying" were added later during the trilogue in 2016. See Council position, 05419/1/2016, April 8, 2016.

15 There are ten explicit exemptions. See Article 9.2 GDPR, "Processing of Special Categories of Personal Data," https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm.

16 The exception "personal data which are manifestly made public by the data subject'" is also much debated. See also, e.g., EDPB Guidelines 3/2019 on video devices, § 70.

17 For example, banks may rely on biometric data for financial account access if their customers explicitly agree.

18 Article 9.4 GDPR. For example, the Netherlands adopted a law allowing biometric data processing if necessary for "authentication or security purposes." Article 29 Dutch GDPR implementation Act of May 16, 2018. The Dutch SA however seems to apply this in a strict manner: see the decision of the Dutch SA (Autoriteit Persoonsgegevens), December 4, 2019, imposing a fine of 725,000 euros for unlawful fingerprinting of employees for access control (appeal pending), available at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_vingerafdrukken_personeel.pdf (in Dutch).

Under the DP LED, LEAs do not face a prohibition and may process biometric data to uniquely identify people where strictly necessary, subject to appropriate safeguards, and only in three situations: if authorized by law, to protect vital interests, or where the processing relates to data manifestly made public by the data subject.[19] While the DP LED has data processing restrictions only if there is "specific technical processing," LEAs may collect data (e.g., facial images or voice recordings) without biometric specific limitations imposed by the DP LED.

In cases where new technologies lead to processing that is "likely to result in a high risk" or in case of large-scale processing of special categories of personal data, the GDPR and DP LED require entities to conduct Data Protection Impact Assessments (DPIA). A DPIA is also required for systematic monitoring of a publicly accessible area on a large scale.[20] DPIAs mandate entities to conduct a comprehensive assessment of the risks of processing, as well as of the necessity and proportionality of the technology.[21] In some cases, private or public entities will have to ask the SA for prior consultation and authorization.[22] Furthermore, if the biometric data processing interferes with fundamental human rights and freedoms, including the right to privacy and the right to personal data protection, the fundamental rights framework shall be applied as well.[23]

The following sections outline the key learnings from these regulatory attempts, discuss their effectiveness, and highlight learnings for future regulation.

ASSESSMENT AND EFFECTS OF THE REGULATORY CHOICES

Impact of Definitional Choices

Since the GDPR and DP LED definitions of biometric data require "specific technical processing," the collection and storage of data like facial images or voice recordings do not receive more or stricter protection than any other personal data, such as the requirement of explicit consent or necessity and

19 See Article 10 Directive 2016/680. Note that in the two last situations, the need for an authorizing law doesn't seem to be required. For "data manifestly made public by the data subject," this is meant to cover social media.

20 Article 35 GDPR and Article 27 Directive 2016/680. This DPIA requirement was part of the original EU Commission's GDPR proposal of January 25, 2012 COM(2012) 11 final.

21 While the DPIA requirement adds important responsibility (and liability) for assessing the risks, necessity, and proportionality of biometric systems, post-GDPR experience already shows that such assessment is in general very difficult to conduct in practice. For the French SA's guidance, see CNIL, "The Open Source PIA Software Helps to Carry out Data Protection Impact Assessment" and its updates, June 25, 2019, https://www.cnil.fr/fr/node/23992.

22 See, e.g., CNIL (French SA), "Délibération no. 2019-001," January 10, 2019, https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf. The document discusses the processing of employee biometric data for access control to premises, devices, and apps at work, which requires such DPIA, Article 11.

23 See Kindt, *Privacy and Data Protection Issues*, 570 et seq; see also supra note 8 on the proportionality principle. The relevant fundamental rights of the European Convention on Human Rights and of the EU Charter that could be affected by biometric technology include, besides the right to privacy and data protection, the right to freedom of expression and of free movement, non-discrimination, and the right to assembly. In relation to LFR and LEAs, see FRA, "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, November 27, 2019, https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law. See also Pete Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," The Human Rights, Big Data and Technology Project, July 2019. National traditions interpreting these fundamental rights must also be taken into account, adding complexity to the matter.

the need for law as required under Article 9.2 GDPR. It is the use of the data, rather than its sensitive nature or its ability to enable identification, that determines when data becomes biometric.[24]

Because of the way the definition was written, the risks of biometric data collection are not covered. Data that should get special protection does not, because it is not currently being processed. This is particularly concerning because later use, particularly by law enforcement agencies, may be less transparent or restricted, and the data could be used without any notice to the individuals concerned or to the public.[25] Under the permissions granted under the GDPR and the DP LED, this implies that companies and government can collect large databases of images (e.g., similar to the information collected by Clearview), which might later be used for law enforcement purposes.[26]

Finally, the definition is not in line with the European Court of Human Rights case law, which has repeatedly stated that the practice of capturing, collecting, and storing unique human characteristics in databases interferes with the right to respect for private life.[27] Such interference was confirmed for facial images in *Gaughran v. The United Kingdom*, where the Court took facial recognition and facial mapping techniques into account, and "found that the retention of the applicant's DNA profile, fingerprints and photograph amounted to an interference with his private life."[28]

An appropriate definition should offer legal protections to unique human characteristics that are fit for identification purposes or could be used by automated processes, and regulation should also restrict the storage of this data in databases.[29] An alternative definition of biometric data could be: "all personal data (a) relating directly or indirectly to unique or distinctive biological or behavioural characteristics of human beings and (b) used or fit for use by automated means (c) for purposes of identification, identity verification, or verification of a claim of living natural persons."[30]

Lack of Clarity around Biometric "Prohibition" and Sweeping Exceptions

The law should take into account how different biometric systems function, and these functionalities should be regulated depending on how the data is processed. For example, while prohibitions on use and processing are outlined in the law, Article 9.1 GDPR does not distinguish between one-to-one (1:1) biometrics comparisons (i.e., verification), and one-to-many (1:n) comparisons (i.e., identification).[31]

---

24 The definition of biometric data does not include so-called "soft" biometrics, such as emotions, since they usually do not allow for identification or identity verification.

25 Article 23 GDPR allows Union or MS law to restrict the rights of data subjects, including the right to information, e.g., to protect public security. See also Article 13.3 Directive 2016/680.

26 For example, LEAs could use FR technology combined with social media profiles; or see the online dating investigation tool offered by Socialcatfish.com, which has commercialized social media and dating profile data.

27 ECtHR, *S. and Marper* 2008, § 86; ECtHR, *M.K. v France* 2013, § 26; see also Cons. const. (France) no. 2012-652, March 22, 2012 (*Loi protection de l'identité*), § 6.

28 ECtHR, *Gaughran v. The United Kingdom* 2020, §70.

29 This should come first and in addition to a prohibition to use for identification purposes, except for precise limited exceptions determined by law.

30 See also Kindt, 2013, *Privacy and Data Protection Issues* 144 et seq. and 851 et seq.

31 See and compare the wording of the prohibition with the definition of article 4(14) GDPR, which refers to the two functionalities ("which allow or confirm the unique identification"): article 9 GDPR forbids only "biometric data for the purpose of uniquely identifying," leaving it uncertain if this prohibition also includes processing for purposes of confirming identification (verification).

Meanwhile, the Council of Europe and SAs have stated that biometric verification contains less risk than biometric identification because no database is needed.[32]

On the other hand, one-to-many comparisons (i.e., identification) introduce additional risks, including the large-scale collection and storage of biometric information in databases, probability-based matching (which raises concerns about accuracy and false positives), and privacy-surveillance concerns. Because the GDPR and DP LED do not differentiate between the two functionalities, there is legal uncertainty for companies that want to invest in biometric verification technologies and privacy-enhancing methods.[33] Appropriate regulation should meaningfully address the relative risks of each functionality, discouraging or banning those that pose real risks, and potentially encouraging those that have the potential to offer real privacy and security protections.

Finally, the broad exceptions and overall vagueness of the law leaves the door open for specifically risky uses of biometric data like live facial recognition (LFR). The GDPR exceptions are general, and include language allowing biometric data processing for "reasons of substantial public interest" based on law. Because of the way this and other exceptions are worded, it remains unclear whether these serve as a legal basis that authorizes public or private entities to deploy LFR (e.g., at large stadium events).[34] The GDPR and DP LED alone will not resolve these questions, and additional specific EU and national laws are needed.[35]

CONCLUSION

The GDPR and DP LED approaches to defining biometric data exclude the collection of so-called "raw" data like facial images, yet protection is most important at the initial stage of the creation of biometric systems and infrastructures. The GDPR and DP LED also deviate from Europe's human rights case law and its own approach to data "processing," which is that data protection should start at the collection stage. A comprehensive legal framework should also aim to restrict

32 CoE, Progress Report 2013 (supra note 3), 58 (recommendation 7, as set out in the CoE report of 2005); Article 29 WP, WP 80 (supra note 5), 11 (Conclusion). One shall hence keep in mind that it is precisely the use of databases against a general public in public places (or in places accessible to the public, such as shops) and the identification functionality that pose the most risk, e.g., of surveillance or of unwanted identification. For example, verification could use local storage and strict safeguards that offer increased security for people trying to access phones or bank accounts, e.g., by local comparison of a facial image locally stored in a protected template form under the individual's control, e.g., on a smartphone, for controlling access to a payment application. Verification and identification have also been rightly distinguished by data protection authorities such as the French SA: see CNIL, "Communication central storage fingerprint," December 28, 2007, 5–6.

33 Such methods exist, in particular template-protection methods, permitting pseudonymous, revocable, and unlinkable biometric identifiers. See also CoE, Progress Report 2013 (supra note 3), 30–31 and Kindt, *Privacy and Data Protection Issues*, 801–807. Because of the data-protection-by-design obligation, such methods are very important.

34 See Danish SA, "Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion," May 24, 2019, https://www.datatilsynet.dk/tilsyn-og-afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion/.

35 Any interference with fundamental rights and freedoms requires a law that shall be sufficiently precise and certain (foreseeability) and accessible, in order to exclude arbitrariness. This is especially important for technology because "the technology available for use is continually becoming more sophisticated" (ECtHR, Kruslin, 1990, §33, on voice recording in criminal proceedings). In COVID-19 times, public controllers and LEAs may also be tempted to deploy LFR for controlling movement restrictions. Because of the risks posed for fundamental rights, the EU Commission recently launched a debate about possibly additional legislation for remote biometric identification: see EU Commission, White Paper on Artificial Intelligence: a European Approach to Excellence and Trust, February 19, 2020, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

any biometric data storage in databases, and should offer clear guidance as to any undesirable or forbidden biometric identification, unless allowed under strict legal conditions, and biometric verification solutions, under precise conditions. More precise laws around police collection and use of such data and policing techniques are needed, in addition to a strict interpretation of the necessity and proportionality tests as they apply to law enforcement use.

Apart from stronger legal and procedural safeguards under the GDPR and DP LED, and enhanced consideration of the fundamental rights' three-steps test, policymakers should adopt special regulation to strengthen and reinforce fundamental rights. These could include bans or moratoria against particular uses of biometric technology like LFR unless strictly necessary and proportionate for substantial public interests described in law. This is crucial, especially if LFR directly contradicts and affects the essence of fundamental rights, such as the right to peaceful assembly, which should not be left to case-by-case assessment.

As other states or countries look to the Union for guidance around regulating biometric data collection and use, this chapter has aimed to highlight the challenges posed by uncritically adopting the text of the GDPR and DP LED. For any future legislation, it will be important to recognize the risks and functionalities of biometric data systems, starting from the collection and storage of the data, not just during its processing or use, and to reconsider broadly worded exceptions that provide loopholes for companies, governments, and authorities to exploit.