Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data:

Which Changes Does the New Data Protection Framework Introduce?[*]

Abstract

For many years, the status of biometric data from a European data protection perspective generated a lot of discussions among European bodies and legal experts. Finally, after four years of lengthy negotiations, the European institutions have adopted a new data protection framework. For the first time, the concept of biometric data is introduced in a European legislative text. Beyond being defined, biometric data are also treated as sensitive data. The changes introduced by the new data protection framework and the issues they raise will be assessed in this article. In a first section, the article will introduce the topic and clarify some terminological aspects. In a second section, it will summarise the slow introduction of the notion of 'biometric data' into the European data protection landscape before the adoption of the Data Protection Reform Package. The next section will deconstruct the concept of biometric data with the help of the definition of personal data. It will then argue that the threshold of identification required for biometric data is higher than the one required for 'generic' personal data. In a fourth section, the article will assess the 'sensitive data' regime that is applicable to biometric data. It will also question the element of the context of the processing, which has been added as the condition that triggers the extra protection granted to sensitive data. The last section will conclude on the changes introduced by the new provisions.

I. Introduction

Payment processing companies, such as MasterCard, are working on developing technologies that use facial images and fingerprints to replace passwords in payment transactions.[1] Other payment companies seem to be working on yet more futuristic passwords, based on edible and embeddable biometric technologies. In April 2015, one of the executives of PayPal explained that such technologies were under development. [2] In an interview to the Wall Street Journal, he mentioned a shift in identification methods from the 'external body methods like fingerprints, towards internal body functions like

[*] Article published in the EDPL, volume 2, issue 3, September 2016, pages 297-311; for citation purposes, the published version should be used.

The author wishes to thank Prof. Jeanne Mifsud Bonnici and Prof. Laurence Gormley for their comments in an earlier draft, the peer reviewers for their very valuable reviews which helped improve the quality of the article and Christina Angelopoulos for her careful reading and editing suggestions. The views expressed in this article are solely those of the author. All remaining errors are the author's sole responsibility. This research was partly carried out under the European Union's Seventh Framework Programme for research, technological development and demonstration in the context of the INGRESS project (www.ingress-project.eu) under grant agreement no 312792.

[1] Alanna Petroff, 'MasterCard launching selfie payments' (*CNN, 22 February 2016*) <http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/>

[2] Jonathan LeBlanc, 'Kill All Passwords' (2015)<http://www.slideshare.net/jcleblanc/kill-all-passwords > accessed 30 May 2016.

heartbeat and vein recognition, where embedded and ingestible devices will allow 'natural body identification'.[3] While the company at stake denied developing such technologies and dissociated itself from the position of its employee, this example nevertheless illustrates the growing and widespread use of biometric data by private parties. Against this background and trends, the establishment of a legal definition and status of biometric data in the new EU data protection framework is welcome.

The concept of biometric data is absent from the European founding texts in the field of personal data protection, i.e. Convention 108[4] and the Data Protection Directive.[5] At the time of their respective adoption, the impact of biometric technologies on data protection rules was not widely discussed. The issue became a hot topic in the early 2000s. In 2003, the Article 29 Data Protection Working Party (the A29WP)[6] issued a *Working Document on biometrics,* in which it addressed the application of data protection rules to biometric systems.[7] Later on, it pursued its analysis in Opinion 3/3012 *on developments in biometric technologies.*[8] In parallel, the European Data Protection Supervisor (the EDPS)[9] discussed the legal status of biometric data from a data protection perspective in the context of the Passport Regulation (Council Regulation 2252/2004)[10] and also of border control instruments (in relation to the establishment of large-scale biometric databases, such as EURODAC, VIS or SIS).[11]

The entry into force of the Lisbon Treaty, in 2009, abolished the pillar structure[12] and changed the way data protection is approached at EU level. Prior to that Treaty, due to

[3] Amir Mizroch, 'PayPal wants you to inject your username and eat your password' (*the Wall Street Journal*, 17 April 2015) < http://blogs.wsj.com/digits/2015/04/17/paypal-wants-you-to-inject-your-username-and-eat-your-password/ > accessed 30 May 2016.

[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS, No. 108, 28 January 1981, Strasbourg (Convention 108).

[5] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/23 (Directive 95/46/EC or Data Protection Directive).

[6] The Article 29 Data Protection Working Party is an independent advisory body to the European Commission on data protection matters, composed of representatives of national data protection authorities, of the European institutions, and of the European Commission, <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> accessed 30 May 2016.

[7] A29WP, 'Working Document on Biometrics' (2003) WP 80.

[8] A29WP, 'Opinion 3/2012 on Developments in Biometric Technologies' (2012) 00720/12/EN WP193.

[9] Independent supervisory authority, which monitors the processing of personal data by the EU institutions and bodies, and advises on policies and legislative instruments that impact data protection, <https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS/Membersmission> accessed 30 May 2016.

[10] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L385 (Passport Regulation or Regulation No.2252/2004); see EDPS, 'Opinion on the proposal to amend Council Regulation No 2252/2004' (26 March 2008) OJ L C200/1.

[11] EURODAC is the EUROpean DACtyloscopic database, established in 2000 for the comparison of the fingerprints of asymum seekers; the Visa Information System allows the Member States of the Schengen area to exchange visa data (such as fingerprints) since 2004 and the Schengen Information System (SIS) was set up to support the exchange of information.

[12] Between 1993 and 2009, the EU was composed of three pillars: the three communities were gathered under the first pillar, Common Foreign & Security Policy under the second pillar, and Police and Judicial Cooperation under the third pillar.

the pillar structure, a patchwork of instruments regulated the processing of personal data in different sectors. The main instrument on data protection for internal market activities, falling under the 'first pillar', was the Data Protection Directive (Directive 95/46/EC).[13] In 'the third pillar' area of police and judicial cooperation, the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters was the main instrument on data protection.[14] Many sector-based regimes complemented these two instruments.[15] With the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights became binding, granting the status of fundamental right to the right to the protection of personal data, as set in Article 8 of the Charter. In addition, the Treaty of Lisbon introduced a new legal basis, Article 16 of the Treaty on the Functioning of the European Union. That Article gives general competence to the EU institutions to legislate on data protection matters across all sectors. Between 2009 and 2011, the European Commission launched two public consultations on the future of data protection regime.[16] Among the issues discussed was the introduction of the concept of biometric data within the data protection framework. In January 2012, the European Commission proposed a comprehensive data protection framework, the Data Protection Reform Package, regulating all sectors including police and judicial cooperation in criminal matters. The Data Protection Reform Package is composed of a proposal for a General Data Protection Regulation (known as the GDPR and replacing the Data Protection Directive)[17] and a proposal for a Directive on data protection rules applicable to law enforcement activities (replacing the Council Framework Decision 2008/977/JHA).[18] After four years of intensive and lengthy discussions, the new Data

[13] Directive 95/46/EC (n 5).

[14] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L350/60 (Council Framework Decision 2008/977/JHA).

[15] eg Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316/1 (repealed by European Parliament and Council Regulation (EU) No 603/2013 of 26 June 2013); Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L213/5; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205/63.

[16] The European Commission launched two public consultations. The first one, in 2009, concerned the future legal framework for the fundamental right to protection of personal data in the European Union. This consultation resulted into a Communication by the European Commission, 'A comprehensive approach on personal data protection in the European Union, published on 4 November 2010 (COM (2010)609 final)). The European Commission consulted a second time stakeholders on the proposals made in the Communication. http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm accessed 30 May 2016.

[17] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data (General Data Protection Regulation), COM (2012) 11 final.

[18] European Commission, Proposal for a Directive of the European Parliament and of the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final; the new Directive does not have any official acronym and is referred to as 'the Directive on law enforcement' in this article.

Protection framework was officially adopted in April 2016.[19] In both the GDPR and the Directive on law enforcement, [20] the concept of biometric data is defined and added to the list of sensitive data.

This article will address the legal status of biometric data from an EU data protection perspective and assess the impact of the adoption of the Data Protection Reform rules on their status. It will review the provisions contained in the Data Protection Directive and compare them with those of the GDPR. The provisions of the Data Protection Directive will remain applicable until the entry into force of the Data Protection Reform Package.[21] The article primarily focuses on the provisions of the GDPR. However references to the new data protection framework as a whole might also be made. References to Convention 108 and its draft revision will also be made as a point of comparison, in particular in relation to the qualification of biometric data as sensitive data. [22]

The article builds on existing legal literature pertaining to the status and qualification of biometric data from a data protection perspective. It will analyse, among others, the contributions by Prins, Grijpink, Yue Liu and Kindt.[23] Since the topic is highly technical, references to the scientific literature and terminology used in the biometric field will be made. In particular, the definitions adopted in the International Standard ISO/IEC 2382-37: 2012 on a Harmonized Biometric Vocabulary will be mentioned.[24] It should be noted that, even though the process of standardization is not complete yet, the International Standard can nevertheless be used as a reference. It has already been quoted, in particular, by the Italian Data Protection Authority (Il Garante) in its Guidelines on

[19]Adoption of the General Data Protection Regulation and of the Directive on law enforcement on 14 April 2016, See <http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era> accessed 30 May 2016.

[20] European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and of the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1; European Parliament and Council Directive 2016/680 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 L119/89 (Directive 2016/680).

[21] The Regulation will apply from 25 May 2018 while Member States should have transposed into national law the provisions of the Directive by 6 May 2018; see art. 99 GDPR and art 63 Directive 2016/680.

[22] Convention 108 (n 4); Draft Explanatory Report to the modernised version of Convention 108, working document of 2 June 2016, see <http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Draft%20Explanatory%20report_En.pdf> accessed 30 May 2016.

[23] See Corien Prins, 'Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies' (1998) 14(3) Computer Law and Security Report 159-165; Jan Grijpink, 'Privacy Law: Biometrics and Privacy' (2001) 17(3) Computer Law & Security Review 154-160; Yue Liu, 'Identifying Legal Concerns in the Biometric Context' (2008), 3(1) Journal of International Commercial Law and Technology 45-54; and Els Kindt, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis* (Springer, 2013).

[24] ISO/IEC 2382-37: 2012 (E)—Information Technology—Vocabulary—Part 37: Biometrics http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55194 accessed 30 May 2016.

Biometric Recognition and Graphometric Signature.[25] Biometric characteristics from which biometric data are extracted are physical or behavioural attributes. These attributes (such as face, fingerprints, voice or gait) show some distinctive and repeatable features (i.e. patterns) that can be measured and compared so as to recognise an individual. Biometric recognition is the general term used to cover the functions of a biometric system based on biometric data. These functions can be split between 'biometric identification', where the identity of an unknown individual is (or is not) established, and 'identity verification', where that individual's identity does not need to be established, but only verified. To perform biometric recognition, biometric characteristics are transformed into data under different formats: a sample (such as the image of a fingerprint, a facial image) and a template (a reduced form of the sample translated into codes, numbers).[26] The technical terms are further explained in the body of the article.

Although this article relies on scientific literature and terminology, it is not written by a scientific expert and it will not assess the quality of the scientific papers to which it refers. The article uses them as descriptive elements.

The article is structured as follows. The next section, Section II, describes the slow introduction of the notion of biometric data in the data protection field at the European level before the adoption of the Data Protection Reform Package. Section III deconstructs the concept of biometric data as defined in the GDPR. To this end, the section describes each component of the definition and assesses in particular the role played by the function of identification. On this issue, the article distinguishes the meaning of identification from a data protection perspective from that from a biometric recognition perspective. Section IV is dedicated to the status of biometric data as sensitive data. It also discusses the relevance of the purpose of processing as a condition for applying the regime of sensitive data to biometric data. The last section concludes on the changes that the GDPR introduces for the legal qualification and status of biometric data from a data protection perspective at EU level, as well as on the remaining uncertainties.

[25] See Garante (2014), Annex A to the Garante's Order of 12 November 2014, 3, see http://194.242.234.211/documents/10160/0/GUIDELINES+ON+BIOMETRIC+RECOGNITION accessed 30 May 2016.

[26] For an overview of biometric recognition, see for instance Yi Chen and Jean Christophe Fondeur "Biometric Algorithms', in Stan Z Li & Anil K Jain (eds), *Encyclopedia of Biometrics* (Springer, 2015), 156-161.

II. The Slow Introduction of the Notion of Biometric Data in the EU Data Protection Field[27]

This section retraces the progressive recognition of biometric data as a category of personal data at EU level prior to the adoption of the Data Protection Reform Package.

The concept of biometric data cannot be found in Convention 108 [28] nor in the Data Protection Directive, [29] the two European founding texts in the field of personal data protection.[30] This is logical, since at the time of their respective adoption, in 1981 and 1995, the impact of biometric technologies on data protection at European level was not widely discussed. It was not until the early 2000s that the European bodies started to discuss the topic.[31] The first documents and reports on the topic show their hesitations as to the exact status and definition of biometric data.

In 2003, the A29WP issued *a working document on biometrics* in which it addressed the application of data protection rules to biometric systems. While discussing the application of the Data Protection Directive to biometric data, it assessed their status from a personal data perspective. Its early findings on the nature of biometric data are unclear. On one side, it acknowledged that biometric data are by nature personal data, since they always relate to an individual who is 'generally identifiable'.[32] But on the other side, it considered that biometric data are not always personal data. It referred, in particular, to biometric templates, which might not constitute personal data if they 'are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject.'[33] As observed by Kindt, the A29WP did not provide any clear criteria to distinguish cases where biometric data (in particular under the form of biometric template) are personal data from the cases where they are not. In the subsequent Opinion on *developments in biometric technologies*, Opinion 3/2012, the Working Party did not provide further explanations. It merely repeated that 'in most cases biometric data are personal data' without further analysis on the definition or on the formats of biometric data.[34]

When reviewing the various opinions and reports on data protection and biometric data, what is striking is the absence of a definition for the notion 'biometric data'. A

[27] This section is based on the findings of a previous article, see Catherine Jasserand, 'Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': an Investigation into the Meanings of the Terms from a European data protection and a Scientific Perspective' (2016) 6(1) International Data Privacy Law 63-76.

[28] Convention 108 (n 4).

[29] Directive 95/46/EC (n 5).

[30] The OECD guidelines on the protection of privacy and transborder flows of personal data (updated in 2013) are also as a non-binding source, see http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm accessed 30 May 2016.

[31] In literature, some authors have addressed the issue earlier, e.g. Prins (n 23).

[32] A29WP, WP 80 (n 7) 10.

[33] Ibid footnote 11, 5.

[34] A29WP, Opinion 3/2012, WP 193 (n 8) 7.

definition of the term emerged quite late in the discussions on biometric data and technologies.[35] In particular, the A29WP investigated the status of biometric data from a data protection perspective even before defining the notion. It was only in 2007 that the Working Party gave a definition to the concept in Opinion 4/2007 on the *concept of personal data*. In that Opinion, biometric data are approached from a scientific perspective and defined as 'biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.' [36] In that same opinion, the A29WP argued that biometric data have a dual nature: they are both a piece of information about an individual and constitute a (unique) link between that individual and his or her biometric characteristics. This definition was quoted several times by the EDPS[37] and the A29WP itself.[38] However, that definition does not link 'biometric data' to 'personal data'. It is interesting to note that the definition of biometric data originally contained in the proposals for a Data Protection Reform Package also had no link to personal data.[39]

In their opinions and reports, the European bodies have indistinctly used the terms 'biometric data' and 'biometrics'. However, a systematic analysis of the two notions reveals that 'biometric data' is both a technical and a legal notion, whereas 'biometrics' is only a technical notion.[40] In any case, the two are not synonymous. The term 'biometrics' has been borrowed from the biometric recognition field. As such, in a data protection context, it should only be used in the way defined by the biometric community, i.e. as an 'automatic recognition method' based on biometric characteristics.[41] The term 'biometric data', on its side, covers the technical transformation of biometric characteristics into formats that can be used for biometric recognition. The technical definition does not require a link to a specific individual.[42] By contrast, in a data protection context, this link is crucial to determine whether the technical 'biometric data' constitute personal data. The next section deconstructs the legal concept of 'biometric data' introduced in the Data Protection Reform Package.

[35] For a complete overview of the definitions proposed by the European bodies, see Jasserand (n 27).

[36] A29WP, 'Opinion 4/2007 on the concept of personal data' (20 June 2007) 01248/07/EN WP 136, 8.

[37] EDPS, 'Opinion on a Research Project Funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' (1 February 2011) (hereinafter Opinion on Turbine Project).

[38] A29WP, Opinion 3/2012, WP 193 (n 8).

[39] European Commission, Proposal for the General Data Protection Regulation (n 16), art 4(11) that reads as follows: '*data* resulting from…' (emphasis added).

[40] See Jasserand (n 27).

[41] ISO/IEC 2382-37 (n 24), Term 37.01.03.

[42] ISO/IEC 2382-37 (n 24), Note below term 37.03.06 that reads as 'biometric data need not to be attributable to a specific individual.'

III. Deconstruction of the Legal Concept of Biometric Data

Until the adoption of the Data Protection Reform Package, there was no express provision on the concept of biometric data nor specific rules to regulate the processing of biometric data in European data protection instruments. Article 4(14) GDPR now defines 'biometric data' as:

> 'Personal data' resulting from a 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

The concept can be further analysed through its different components.

1. Personal Data

'Biometric data' are first of all personal data. This means that, before legally qualifying as 'biometric', this type of data needs to comply with the criteria applicable to the general category of personal data.

The definition of personal data in Article 4(1) GDPR is very similar to the original definition contained in Article 2(a) of the Data Protection Directive.[43] The notion is indeed defined in identical terms, as 'any information relating to an identified or identifiable natural person ('data subject').' The difference between the two lies in the description of what an 'identifiable person' is. Article 4(1) GDPR contains a broader list of possible identifying factors (including genetic identity) and adds examples of identifiers (such as name, identification number, location data and online identifier). The definition does, however, not refer to the notion of a biometric identity or biometric identifier.

The threshold according to which the identification of an individual is determined remains low: the individual does not need to be identified, but only made identifiable. Like in Article 2(a) of the Data Protection Directive, the adjective 'identified' is undefined.[44] As interpreted by the A29WP in Opinion 4/2007, 'identified' should be understood as meaning to be 'singled out' or 'distinguished' from a group of people.[45] Identifying someone in a data protection context therefore does not require establishing his or her identity.

[43] art 2(a) of the Data Protection Directive (n 5) reads as follows: 'Personal data shall mean any information relating to an identified or identifiable natural person "data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one more factors specific to the physical, physiological, mental, economic, cultural or social identity.'

[44] See also analysis made by Waltraut Kotschy, 'Article 2, Directive 95/46/EC', *Concise of European IT law*, in Büllesbach, Gijrath, Poullet & Prins (eds), (Kluwer Law International 2010) 35.

[45] A29WP, Opinion 4/2007, WP 136 (n 36) 12-13.

'Identifiable' is different from 'identified', as the former refers to an individual who has not been identified yet, but who can be, through the combination of other information. Recital 26 GDPR reiterates the test of 'identifiability', originally contained in the Data Protection Directive.[46] That test relates to "all the means likely reasonably to be used" to identify an individual. Recital 26 GDPR also sets a list of factors to be taken into account to assess the identifiability of an individual. That list is based on factors suggested by the A29WP in Opinion 4/2007.[47] Among those factors are those relating to 'available technology at the time of processing and technological development.'[48]

2. Resulting from a Specific Technical Processing

Like the Data Protection Directive, the General Data Protection Regulation regulates the processing of personal data.[49] The processing of personal data is defined in Article 4(2) GDPR as follows:

> Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The regulatory definition of biometric data contains a reference to technical processing. It does not specify what should be understood by 'specific technical processing', except to state that the purpose of that processing should be to uniquely identify an individual. In order to understand the technical processing to which biometric characteristics are subjected and their transformation into data, the following paragraphs explain the technical stages of biometric recognition and the biometric templates resulting from them.

a. Technical Steps of Biometric Recognition

The first stage of the processing is the enrolment of the biometric characteristics in a biometric system. The biometric characteristics are 'captured' under the form of an

[46] Recital 26 of the Data Protection Directive reads as follows: 'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (…).'

[47] A29WP, Opinion 4/2007, WP 136 (n 36) 15.

[48] Recital 26 GDPR reads as follows: 'To determine whether a person is identifiable, account should be taken to all the means reasonably likely to be used, such as singling out, either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonably likely to be used to identify an individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.'

[49] See material scope, art 3(1) of the Data Protection Directive and art 2(1) GDPR.

image, such as a fingerprint image. The format resulting from this phase is called a biometric sample.[50]

In a second stage, the information contained in a sample is extracted, reduced, and transformed into labels or numbers via an algorithm.[51] This phase is called feature extraction.[52]Only the 'the salient discriminatory information that is essential for recognizing the person' will be kept.[53] The extracted features are kept in a biometric template under the form of a 'mathematical representation of the original [biometric] characteristic.'[54] The reference template is then stored for comparison.[55]
In a third stage, a biometric sample (such as a fingertip) presented at a sensor will be compared with a previously recorded template (such as the template of a fingerprint). In some cases the comparison will be established with another biometric sample instead of a template. Comparison between samples is however less common.[56]

From these different technical steps and the transformation of biometric characteristics into biometric information, several processing operations, as defined in Article 4(2) GDPR, can be identified:[57] in a first phase (enrolment), data are collected; during the second phase (feature extraction), data are organised, structured, adapted and stored; the final phase of comparison entails specifically the retrieval, consultation, use and disclosure of the data.

b. ***Biometric Formats Resulting from the Technical Processing***

Two formats result from the technical processing: the biometric sample and the biometric template. As already described, a sample is the image of a biometric characteristic, whereas a template is a reduced and encoded form of information contained in a sample. Some authors, as well as the A29WP, wrongly use the phrase 'raw (biometric) data' to designate a biometric sample.[58] Raw (biometric) data are, for example, a fingerprint, fingertip, iris, voice, etc. In the absence of any technical processing through which the raw data are obtained, these fall outside the scope of

[50] ISO/IEC 2382-37 (n 24), Term 37.03.21, Definition of biometric sample as: 'analog or digital representation of biometric characteristics prior to biometric feature extraction.'

[51] This is a very simplified presentation of the formats. For further technical details, see Kindt (n 23) 43-47.

[52] ISO/IEC 2382-37 (n 24), Term 37.03.21.

[53] e.g. Davide Maltoni, Dario Maio, Anil Jain, and Salil Prabhakar, *Handbook of Fingerprint Recognition* (Springer 2003) 26.

[54] Emm Wollacott, 'Protection when Tech Gets Rather Personal', in *Biometrics and Identity Management,* Le Raconteur (30 April 2015) 10.

[55] *Encyclopedia of Biometrics* (n 26), 'Biometric Template', 152; *Encyclopedia of Biometrics* (n 26), Andy Adler and Stephan Schuckers, 'Biometric Vulnerabilities, Overview', 164.

[56] Kindt (n 23).

[57] art 4(2) GDPR, the processing of personal data is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such a collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

[58] See criticisms by Kindt in Kindt (n 23), footnote 100, p.43 and footnote 39, p.98.

biometric data. The term 'raw data' should only be used as a synonym of biometric characteristics.

Under the regime of the Data Protection Directive, the issue of biometric formats played an important role in the debate on the legal qualification of 'biometric data'. Not much doubt was expressed on the status of biometric samples, which were considered personal data.[59] In contrast, the status of biometric templates has generated more discussion. The position of the legal literature has also changed over time, taking into account the state of the art in biometric recognition. In early discussions on the nature of biometric templates from a data protection perspective, it was believed that biometric templates could not be 'translated back' into the biometric samples from which they originated. This was the position defended by Prins and Grijpink.[60] Grijpink even argued that biometric templates were anonymous data. Since Prins' and Grijpink's papers were first published, the scientists Adler,[61] Bromba,[62] Ross, Shah,[63] Cain and Jain[64] have demonstrated that biometric templates are in fact partially reversible and could possibly regenerate information contained in biometric samples. In recent legal studies on the legal status of biometric data, authors have concluded that biometric templates are reversible, at least partially, and may not be considered as anonymous data anymore. [65]

The new data protection framework does not refer to biometric formats. This is logical, since the legislative instruments are technology-neutral and the legal definitions should not be tied to any specific format. In any case, the notion of 'information' contained in the definition of personal data and as interpreted by the A29WP,[66] covers any type of form and format.[67] As a result, if discussions on the formats do not have their place in the Data Protection Reform Package, the European Data Protection Board[68] could

[59] Liu (n 23) 45-54 ; Paul De Hert, 'Biometrics : Legal Issues and Implications', Background Paper for the Institute of Prospective Technological Studies, DG JRC- Sevilla European Commission (2005) 13.
[60] Respectively Prins (n 23), Grijpink (n 23).
[61] Andy Adler, 'Can Sample Images be Regenerated from Biometric Templates?' (Biometrics Conference, 22-23 September 2003) http://www.sce.carleton.ca/faculty/adler/publications/2003/adler-2003-biometrics-conf-regenerate-templates.pdf accessed 30 May 2016.
[62] Manfred Bromba, 'On the Reconstruction of Biometric Raw Data from Template Data' (2006) http://www.bromba.com/knowhow/temppriv.htm accessed 30 May 2016.
[63] Arun Ross, Jidnya Shah, and Anil Jain, 'From Template to Image: Reconstructing Fingerprints from Minutiae Points' (2007) 29(4) IEEE Transactions on Patterns Analysis and Machine Intelligence 544-560.
In a very detailed paper the authors show which information a 'minutiae template' can reveal about a fingerprint sample. They conclude that 'the reconstructed image can be used to generate synthetic prints that can be used to compromise the security of a biometric system. If other information (…) are available in the template, then, perhaps, the original fingerprint can be reconstructed in its *entirety*.'
[64] Kai Cao and Anil Jain, 'Learning Fingerprint Reconstruction: from Minutiae to Image' (2015) 10(1) IEEE Transactions on Information Forensics and Security 104-117.
Cao and Jain pursue the research on the possibility to reconstruct a fingerprint image from a template and conclude that the reconstructed image is very close to the original sample, even if too perfect to fool a fingerprint expert.
[65] See Liu (n 23) and Kindt (n 23).
[66] A29WP, Opinion 4/2007 (n 36) 6.
[67] Ibid 7-8.
[68] Established by art 68 GDPR.

provide guidance to stakeholders and national data protection authorities on the legal qualification of biometric formats.

3. Relating to the Physical, Physiological or Behavioural Characteristics of a Natural Person

This criterion relates to the definition of biometric characteristics. It acknowledges the broad spectrum of measurable human characteristics that can be used for biometric recognition: this covers physical and physiological attributes (such as a fingerprint, face or iris), as well as behavioural attributes (such as voice, gait or signature).[69] The difference between physiological and physical characteristics is not very clear. Many experts in biometric recognition only refer to two types of characteristics: either physical and behavioural characteristics, or physiological and behavioural characteristics.[70] They provide the same examples for physical and physiological ones: fingerprints, face, palm geometry.

4. Allowing or Confirming the Unique Identification of that Individual

This criterion is a key element in the legal qualification of biometric data. It describes the purposes of use of the biometric characteristics, from which biometric data are extracted. It also sets the threshold for identification applicable to biometric data as a category of personal data. It builds on an understanding of the difference of meaning between biometric identification and identification in a data protection context.

a. The Different Meanings of Identification

For the biometric community, identification has a very specific and narrow meaning. It refers to the process of establishing the identity of an individual by comparing a biometric sample with previously stored biometric templates that exist across different databases.[71] This is the 'one-to-many' matching.[72] Identity in a biometric context does not require establishing the civil or legal identity of an individual, but determining that a sample and a previously recorded template originate from the same person. Identity is established, when a match is found between a biometric characteristic and a biometric template.

Biometric identification is generally opposed to identity verification (or biometric verification). Identity verification is often called 'authentication', but this is an incorrect usage of the term according to the biometric community.[73] As observed by Kindt, authentication is used as a synonym of verification, identification and biometric

[69] See eg, Anil Jain and Arun Ross, 'An Introduction to Biometric Recognition' (2004) 14(1) IEEE transactions on circuits and systems for video technology.

[70] See ibid; see also *Encyclopedia of Biometrics* (n 26), definition of Behavioural Biometrics, 62.

[71] ISO/IEC 2382-37 (n 24), Term 37.08.03, defining biometric identification as 'process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual.'

[72] A29WP, Opinion 3/2012 (n 8) 5.

[73] ISO/IEC 2382-37 (n 24), Term 37.08.03.

recognition.[74] But because one cannot deduce the functionality to which it refers,[75] the term 'authentication' should be avoided. This is important for terminological precision, since Recital 51 GDPR mentions the term 'authentication' in opposition to 'unique identification'. This issue is further developed in the next sub-section. Verification is the process of verifying if an individual is who she or he claims to be.[76] The purpose is therefore not to establish the identity of an individual, but solely to verify it. The comparison process in that case is known as 'one-to-one' matching.[77] The biometric sample of an individual is only compared with the biometric information contained in one device, such as a smart card, an ID card, a passport, or in a single database.

Until the introduction of the concept of 'biometric data' within the scope of the data protection legislation, there was no reason to distinguish the general meaning of identification from its specific meaning in a biometric context. With the adoption of the new data protection framework, there is such a need. As described in sub-section 1, identification in a data protection context (meaning 'singling out') has a broader meaning than biometric identification (meaning 'establishing somebody's identity'). However, it can be argued that the function of identification through personal data encompasses the biometric identification function.

b. Functions of Biometric Data ("Allowing or Confirming")

Biometric characteristics are thus used to perform biometric identification or identity verification. These two functions seem to be present in the definition of biometric data through the verbs "allowing" and "confirming". Although these two verbs do not reflect the terminology used by biometric experts to describe the uses of biometric characteristics, one can infer that "allowing" refers to establishing the identity of an individual (biometric identification), whereas "confirming" refers to verifying his or her identity (identity verification). It is regrettable that the legal definition is not more rigorous and does not take into account the precise terminology used in the context of biometric recognition. As criticised by Stalla-Bourdillon, the legal definitions contained in the GDPR do not reflect technological practices.[78] In her study, Kindt has also emphasized the importance of using the correct technical terminology to understand the discussions about biometric data.[79]

[74] Kindt (n 23).

[75] Ibid 42

[76] ISO/IEC 2382-37 (n 24), Term 37.08.02, defining biometric verification as: 'process of confirming a biometric claim through biometric comparison.'

[77] A29WP, Opinion 3/2012 (n 8) 6.

[78] Sophie Stalla-Bourdillon, 'the GDPR and the biggest mess of all: why accurate legal definitions really matter…", blogpost on Peep Beep, 12 April 2016 https://peepbeep.wordpress.com/2016/04/12/the-gdpr-and-the-biggest-mess-of-all-why-accurate-legal-definitions-really-matter/ accessed 30 May 2016.

[79] Kindt (n 23) 42.

On a positive note, one should observe that the current legal definition of 'biometric data' is much improved in comparison to the one originally proposed by the European Commission. The definition contained in the proposals of the Data Protection Reform Package only mentioned the function of 'biometric identification' and omitted that of 'identity verification'.[80]

c. ***Unique Identification***

The phrase 'unique identification' raises some terminological issues. Should it be understood as setting up the threshold of identification to be met by biometric data as personal data? Or should it be understood as referring to the 'biometric identification' function of biometric data? The wording of Recital 51 casts doubt on the exact meaning of this criterion.

Biometric data are defined as a legal category of personal data. It is therefore logical to look at the term 'unique identification' through the lens of the definition of personal data. From that perspective, 'unique identification' refers to the meaning of identification in a data protection context. As defined in Article 4(1) GDPR, data are personal if they relate to an identified or identifiable individual. The threshold of identification is low, since an individual only needs to be identifiable. But that threshold is much higher for biometric data. As suggested by Kotschy in her interpretation of Article 2(a) of the Data Protection Directive, 'unique identification' is the 'highest degree of identification.'[81] As a consequence, biometric data must relate to an identified individual to legally qualify as biometric data. The adjective 'unique' is not defined. It could mean that biometric data have such particularities that they can 'unambiguously' identify an individual. They can, in particular, link an individual to his or her body. But it would not be accurate to say that, for this reason, biometric data are unique to each individual and allow their unique identification. From a scientific perspective, the 'uniqueness' of biometric characteristics is an assumption that forensic experts have challenged.[82] It has indeed never been scientifically demonstrated that two individuals do not have the same fingerprints.[83] In addition, the results on which the identification is performed are relative. Biometric recognition is indeed based on measurements and probabilities of similarities (or dissimilarities). The results obtained from the

[80] European Commission, Proposal for the GDPR (n 17), art 4(11) reads as follows: 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data.'

[81] Kotschy (n 44) 35.

[82] For example, Mark Page, Jane Taylor and Matt Blenking, 'Uniqueness in the Forensic Identification Sciences: Fact or Fiction ?' (2011) 206 (1-3) Forensic Science International 12-18.
David Kaye, 'Questioning a Courtroom Proof of the Uniqueness of Fingerprints' (2003) 71 (3) International Statistical Review 521- 533.
Michael Saks, 'Forensic Identification : From a Faith-Based 'Science' to a Scientific Science' (2010) 201 (1-3) Forensic Science International 14-17.

[83] Simon Cole, 'Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents' (2006), 28(1) Law & Policy 109-135.

comparison of biometric data are subject to errors, in particular to false identification.[84] As such, biometric data cannot have the same function as a (static) unique identification number. The EDPS has advised against the use of biometric data as unique identifiers, because of the probabilistic nature of biometric technologies.[85]

Following that interpretation, an individual would only be identified if his or her biometric characteristics match previously recorded biometric data. In a case of a non-match, the individual remains unidentified. However, he or she could still be identifiable, i.e. he or she could be identified by a different entity than the data controller.[86] This is the case when biometric data can be matched with other data kept in a database different from the one consulted for comparison, especially in a scenario of identity verification. In that case, the individual would be identifiable. However, those 'biometric' data relating to an identifiable individual would not legally qualify as 'biometric data'. They would however be personal data, provided they fulfil the other conditions applicable to personal data in general.

But a second meaning could be attributed to the term 'unique identification'. One can wonder if 'unique identification' should not be interpreted as referring to the 'biometric identification' function of biometric data. In Recital 51 GDPR, 'unique identification' is used in opposition to 'authentication', while clarifying the conditions under which pictures qualify as 'biometric data.'[87] Recital 51 provides that:

> The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

The term 'authentication' is not clarified. However, it would be reasonable to consider that the EU institutions have used it as a synonym for 'verification'. In Opinion 3/2012 on developments of biometric technologies, the A29WP used verification and authentication as synonyms. In that Opinion, the A29WP defined the function of 'identity verification' as 'biometric verification/authentication'.[88] As mentioned earlier, the use of 'authentication' to refer to the functionalities of biometric systems is not accurate.

[84] For example, BioPrivacy, International Biometric Group, which developed Best Practices, see FAQs 'Are Biometrics Unique Identifiers ?', http://www.bioprivacy.org accessed 30 May 2016.

[85] EDPS, 'Comments on the Communication of the Commission on interoperability of European databases' (10 March 2006); EDPS, 'Opinion on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime' (19 December 2007) OJ C89/1 (2008/C 89/01).

[86] Recital 26 GDPR.

[87] Recital 51 GDPR reads as follows:'…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 through a specific technical means allowing the unique identification or authentication of a natural person.'

[88] A29WP, Opinion 3/2012 (n 8) 6.

However, if in Recital 51 GDPR, authentication means ‘identity verification’, should ‘unique identification’ be understood as referring to ‘biometric identification’? This interpretation would be inconsistent with the legal definition of biometric data. In addition, since the notion of biometric data is approached from a legal perspective in the GDPR, the term ‘unique identification’ should logically refer to the threshold of identification of biometric data (being personal data) and not to their ‘biometric identification’ function. One could still note the inconsistency of wording (and then meaning) between Recital 51 GDPR and Article 4(14) GDPR.

5. Facial Images and Dactyloscopic Data as Examples

Biometric characteristics are not themselves considered to be biometric data. Only the personal data ‘resulting’ from their processing qualify as biometric data. Thus, it is not the face of an individual, but the images of his or her face (pictures) that would be classified as biometric data. Likewise, it is not his or her fingertip, but a fingerprint image that will be classified as biometric data. This is a logical conclusion since ‘biometric data’ as legally defined are first of all ‘personal data’. To be protected under the data protection rules, personal data need to be, at least, part of a filing system or processed by automatic means.[89] The biometric characteristics themselves cannot be processed. Only the data generated from those characteristics can.

The legal definition of ‘biometric data’ gives two examples of those data: facial images and dactyloscopic data. Concerning facial images, not all the photographs will qualify as ‘biometric data’, but only the ones that ‘allow the unique identification or authenticate’ an individual will.[90]. To determine whether a facial image is fit for biometric recognition, different factors or parameters should be taken into account, such as light, exposure, location or the resolution of the camera.[91] These parameters are logically not detailed in the GDPR, as they are linked to the technological developments in face recognition.

As for dactyloscopic data, the GDPR contains no reference or definition. Another legislative instrument on the cross-border exchange of DNA profiles and fingerprints to fight terrorism and crime, the Prüm Decision, provides a definition. Dactyloscopic data in the GDPR could be understood as defined in Article 2(i) of the Prüm Decision, i.e. as covering ‘fingerprint images, images of fingerprint latents, palm prints, palm prints latents and templates of such images.’[92]

[89] art 2(1) GDPR ; art 3(1) of the Data Protection Directive.

[90] Recital 51 GDPR.

[91] Face recognition is based on individual’s distinctive facial characteristics, for guidance on face recognition; see for example EDPS, ‘Video Surveillance Guidelines’ (17 March 2010); A29WP ‘Opinion 02/2012 on facial recognition in online and mobile services’ (2012) 00727/12/EN WP 192.

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

The analysis of the different components of the legal concept of 'biometric data' reveals that only personal data resulting from a special processing of biometric characteristics and relating to an identified individual will qualify as 'biometric personal data'. When those data uniquely identify an individual, they will benefit from the protection granted to sensitive data. This special regime is the issue addressed in the next section.

IV. The Regime for Sensitive Data Applicable to the Processing of Biometric Data

Sensitive data (designated under the term 'special categories of data')[93] are a category of personal data that necessitate a higher degree of protection because of the consequences that their misuse would have on individuals.[94] The consequences are considered so damageable that their processing is prohibited unless an exception applies. The regime of sensitive data is defined in Article 8 of the Data Protection Directive.[95] This provision contains an exhaustive list of sensitive data, which are 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'

The Data Protection Reform Package has added biometric data to the list of sensitive data. According to Article 9(1) GDPR, the processing of biometric data 'for the purpose of uniquely identifying a natural person' is prohibited, unless one of the exceptions set out in Article 9(2) GDPR applies. Before the adoption of the Data Protection Reform Package, the debate around the nature of biometric data from a data protection perspective revolved around their content (i.e. whether they could reveal sensitive information) and their qualification (whether they could be considered themselves as sensitive data). This section analyses the different issues and assesses the new condition added to trigger the protection granted to sensitive data.

1. Debate before the adoption of the Data Protection Reform Package

For many years, the main issue about the sensitive nature of biometric data concerned their capacity to reveal sensitive data in the sense of Article 8 of the Data Protection Directive. Among the listed sensitive data, 'data concerning health' or 'revealing racial or ethnic origin' are of particular interest when it relates to the content of biometric data. Several scientific studies on fingerprints have indeed shown that biometric data could reveal this type of sensitive data. Medical research has in particular demonstrated that

[93] art 8 of the Data Protection Directive, art 9 GDPR.

[94] A29WP, 'Advise Paper on Special Categories of Data ('Sensitive Data')', Ref. Ares (2011) 444105 (20 April 2011).

[95] art 8 (1) of the Data Protection Directive reads as follows: 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex-life.' Art 8 (2) of the Data Protection Directive provides for some exceptions to the general prohibition of processing.

the pattern of fingerprint's ridges can indicate a risk of illnesses (such as diabetes).[96] Recent studies have also found that fingerprint patterns encode information about an individual's ancestral background (ethnicity). [97]

The A29WP and the EDPS have also expressed their opinion on the topic. In Opinion 3/2012, the A29WP considered that 'some biometric data', such as facial images could reveal sensitive data relating to health condition or ethnic/racial origin, but in that Opinion the Working Party did not qualify biometric data as sensitive data. [98] As for the EDPS, in several opinions relating to the processing of biometric data for passports and travel documents, it viewed biometric data as being 'highly' [99] or 'inherently sensitive,'[100] because of their characteristics and not because of the sensitive information they could reveal. Based on those opinions, the Advocate General Mengozzi in Case C-291/12 on the validity of the Passport Regulation (Council Regulation 2252/ 2004) stated that biometric data are sensitive data by nature. [101] On this specific point, the European Court of Justice did not follow his opinion. The Court, however, ruled that 'biometric data' are personal data because 'they objectively contain unique information about individuals which allows those individuals to be identified with precision.' [102]

On the formats of biometric data, the A29WP has not said much, although, in 2003, it did state that it considered that images are more susceptible to reveal sensitive data than the templates themselves.[103] Its analysis was based on the beliefs that a biometric image could not be regenerated from a biometric template.[104] In Opinion 3/2012, the Working Party did not amend its position, although by that time it was known that biometric templates could be partially reversible. Having said this, it is not sure from a scientific point of view that sensitive information can be derived from biometric templates. According to the state of the art in biometric recognition, a biometric image can partially be reconstructed from a biometric template.[105] From that reconstructed image, and in

[96] In particular Henry S Kahn et al. 'A Fingerprint Marker from Early Gestation Associated with Diabetes in Middle Age: the Dutch Hunger Winter Families Study' (2009) 38(1) International Journal of Epidemiology 101-109.

[97] Nichole A Fournier and Ann H Ross, 'Sex, Ancestral, and Pattern Type Variation of Fingerprint Minutiae: a Forensic Perspective on Anthropological Dermatoglyphics' (2015) American Journal of Physical Anthropology, online access 23 September 2015.

[98]A29WP, WP 80 (n 7) 10.

[99] EDPS, 'Opinion of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas' (COM (2004) 835 final), Section 3.4.2 Specific Nature of Biometrics, OJ L181/13.

[100] EDPS, Opinion of 19 October 2005 on the three SIS II proposals, Section 4.1 Biometrics, OJ C 181/13.

[101] C-291/12, *Michael Schwarz v Stadt Bochum* [2013], EU:C:2013:401, Opinion of Advocate General Mengozzi, para. 52.

[102] C-291/12, *Michael Schwarz v Stadt Bochum* [2013], EU: C:2013: 670.

[103] A29WP, WP 80 (n 7) 10.

[104] ibid, ' Whether a processing contains sensitive data is a question of appreciation linked with the specific biometric characteristic used and the biometric application itself. It is more likely to be the case if biometric data in the form of images are processed, since in principle the raw data [understood here as image] may not be reconstructed from the template.'

[105] Cao and Jain (n 64).

the absence of research on this issue,[106] it is however not certain that sensitive information can be identified.

In legal literature, the analysis by Yue Lui on the specific nature of biometric data provides some interesting insights. Based on a decision of the Norwegian Data Protection Authority on the use of CCTV in buses, Yue Lui explains that some view biometric data as 'carriers' of personal data and not as 'sensitive data' themselves. However, they become sensitive in case they are 'processed with the intention or consequence of generating sensitive information, such as health, genetic or racial information.'[107] Thus, it is the context of the use of biometric data that would condition the application of the regime of sensitive data. At the same time, Yue Lui states that she is not convinced by this reasoning. She explains that the status of biometric data should not be linked to the sensitive data they can reveal, but to their own characteristics. According to Yue Lui, because biometric data can be used as 'relatively unique and universal 'key data' for getting all kinds of personal information,'[108] they should be considered "as 'sensitive personal data' in general."

2. Purpose of Use as a New Condition to Apply the Regime of Sensitive Data

Discussions on the specific nature of biometric data were revived during the public consultations that preceded the launch of the proposals of the new data protection framework. Between 2009 and 2011, the European Commission consulted national authorities and stakeholders on the future of the data protection regime.[109] Several of these mentioned the issue of the specific nature of biometric data and suggested adding them to the list of sensitive data.[110] However, in the proposals on the Data Protection Reform Package, the European Commission only added 'genetic data' to the list. [111] It was instead the European Parliament that added them to the list of sensitive data when it voted on the proposals. [112] In the adopted texts, biometric data have been upgraded to the category of sensitive data, under the condition that they 'uniquely identify' an

[106] To the best of this author's knowledge.

[107] Yue Lui, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics* (Routledge 2012) 120

[108] Ibid 121

[109] European Commission (n 16).

[110] eg answers from Datatilsynet, the Norwegian Data Protection Authority http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/datatilsynet_en.pdf accessed 30 May 2016; or from Privacy International http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf accessed 30 May 2016.

[111] European Commission (n 17), Article 9(1) of the Proposed GDPR reads as follows: 'the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.'

[112] European Parliament, legislative resolution on the proposal for a GDPR (COM (2012) 0011-C7-0025/2012-2012/0011(COD)), 14 March 2014, art 9(1) of the amended proposal of GDPR reads as follows: 'the processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures shall be prohibited.'

individual. It is therefore the purpose of the processing ('unique identification') that will trigger the regime applicable to sensitive data.

As explained in the previous section, 'unique identification' is also used as a criterion to qualify specific personal data as 'biometric data.' Contrary to the other types of personal data listed in the category of sensitive data, 'biometric data' are not treated as sensitive by nature, but become sensitive as the result of their use.

a- Purpose of Biometric Data Processing

It is therefore the purpose of biometric data processing that determines the application of the regime of sensitive data. The purpose is defined as 'uniquely identifying an individual.' As per the analysis made in the previous section, biometric data resulting from both biometric identification (establishment of the identity) and identity verification should qualify as sensitive data, provided they relate to an identified individual. Still, a doubt persists because of the ambiguous wording of Recital 51 GDPR.[113] If 'allowing the unique identification' refers to the biometric identification function and 'allowing the authentication' means 'identity verification,' biometric data used for identity verification (such as passport/ID verification) would be excluded from the scope of sensitive data. But, as already observed, Recital 51 is inconsistent with Article 4(14) GDPR that defines the legal concept of biometric data. The definition distinguishes the function of 'allowing the unique identification' (which covers the biometric identification function) from that of 'confirming the unique identification' (which covers the identity verification function). Unique identification is then understood as the identity of an individual. Following the definition, biometric data used for biometric recognition (identification and verification) and linked to an identified individual benefit from the status of sensitive data.

It is difficult to reconstruct the intention of the EU legislator: the notion of 'biometric data' was not included in the list of sensitive data contained in the proposals of the Data Protection Reform Package. Likewise, not much can be found in the discussions on the proposals either. The criterion of the purpose of the processing was indeed added very late in the trilogue negotiations on the Data Protection Reform Package:[114] neither the resolutions on the proposals adopted by the European Parliament nor the political agreements reached by the Council mentioned the criterion. It can however be found in the draft version of modernisation of Convention 108.[115] The draft Convention is completed with a Draft Explanatory Report. The 2013 Draft mentions that 'solely the

[113] Recital 51 GDPR (n 87).

[114] The political agreements reached by the Council on the text of the General Data Protection Regulation in June 2015 and on the text of the Directive on data protection for law enforcement purposes did not mention biometric data in the list of sensitive data.

[115] Council of Europe, Consultative Committee of Convention 108 for the protection of Individuals with regard to automatic processing of personal data (ETS No. 108), Propositions of modernization adopted by the 29th Plenary meeting (T-PD(2012)4Rev4) (2012). The modernisation process started in 2011 and is still ongoing.

processing which will lead to the unique identification of an individual' is 'to be considered as sensitive.'[116] The Draft also contains the example of photographs, reproduced in Recital 51 GDPR, and provides the conditions under which pictures should constitute biometric data. The trilogue at the EU level seems to have aligned the texts of the Data Protection Reform Package with the draft revision of Convention 108.

b- __Sensitive Data by Reason of their Nature__

It is questionable whether biometric data should not have been treated 'sensitive data' by reason of their nature and not because of their purpose of use. In the original proposals of the Data Protection Reform Package, the European Commission did not add biometric data to the list of sensitive data, but only genetic data.[117] It justified the addition of 'genetic data' by reference to the ruling of the European Court of Human Rights (ECtHR) in *S & Marper v UK.*[118] In that case, relating to the retention of DNA samples, fingerprints and cellular samples of persons suspected but never convicted, the Court ruled on the sensitive nature of DNA information. It found that their sensitivity was linked to their characteristics – i.e. the possibility that DNA information could reveal ethnic origin[119] and family genetic makeup.[120] The ECtHR did not follow the same approach and reasoning for fingerprints, as the Court considered 'common ground that fingerprints do not contain as much information as either cellular samples or DNA profiles.'[121] The judgement was rendered in 2008 when fingerprint recognition technologies were less developed. Since that time, some scientific studies have shown that sensitive information, such as ethnicity[122] and illnesses [123] can possibly be derived from fingerprints. It can be argued that, if the ECtHR were to examine the issue now, the Court ought to take into account the state of the art in fingerprint recognition and question whether 'biometric data' should not be treated as sensitive data because of their nature.[124]

[116] Council of Europe, Bureau of the Consultative Committee of Convention 108, 'Draft Explanatory Report of the Modernized Version of Convention 108', T-PD-BUR(2013)3ENrev, para. 56.

[117] European Commission, proposal for the GDPR (n 17) and proposal for the Directive on law enforcement (n 18).

[118] *S and Marper v United Kingdom* [2008] ECHR 1581; European Commission, 'Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', Brussels, 25 January 2012, SEC (2012), 55.

[119] *S and Marper v UK,* para 76.

[120] ibid para 103.

[121] ibid para 78.

[122] A29WP, Opinion 02/2012 (n 91); Fournier et al. (n 97).

[123] Kahn et al. (n 96).

[124] It could also be argued that biometric data and genetic share several similarities from a data protection perspective: they both rely on permanent physiological characteristics for individual recognition and they can both reveal sensitive information. In addition, several national data protection laws (Slovenia, Slovakia) already include genetic data in the broader category of biometric data. Some authors (eg Kindt) support such a distinction on the ground that genetic data cannot be used for automatic recognition. But scientific research in the field (Jain) anticipates that 'in the near-future' DNA-profile matching might be done in real-time or at least within a few minutes.

The regime of sensitive data contained in the GDPR is quite similar to the one set in the Data Protection Directive. The general rule is the prohibition of processing sensitive data unless one of the exceptions listed in Article 9(2) GDPR applies.[125] The grounds for processing sensitive data are broadly similar to those under the Data Protection Directive, with some additions made in the area of health. In application of Article 9(4) GDPR, Member States have the possibility to adopt other conditions or stricter rules to allow their processing.[126]

V. Conclusions

The long-awaited provisions of the new data protection framework bring some certainties on the status of biometric data. They define the concept of biometric data taking into account the technical processing through which biometric characteristics are transformed into data. Equally importantly, the new provisions also grant the status of sensitive data to biometric data. But those certainties might only be illusory.

The legal definition of biometric data from a data protection perspective sets the conditions under which personal data can qualify as 'biometric data' and not the conditions under which 'biometric data' become personal data. The concept of biometric data is defined as a type of personal data. The definition combines the technical criteria of biometric data (e.g. the technical processing of biometric characteristics) with legal criteria applicable to personal data (e.g. the function of 'unique identification). However, the definition lacks preciseness when it addresses the functions of 'biometric recognition'. The terminology used by the biometric community to describe these functions, i.e. biometric identification and identity verification, is not re-used in the legal definition of biometric data. Instead, one should deduce that the verbs 'allowing' and 'confirming' respectively refer to the functions of 'biometric identification' and 'identity verification'. As for the criterion of 'unique identification', it sets the threshold of identification applicable to biometric data. Contrary to 'generic' personal data, biometric data must relate to an identified individual. The other 'biometric data', i.e. those that relate to an identifiable individual, do not legally qualify as biometric data, but can still be considered as personal data if they fulfil the other criteria applicable to personal data. The new data protection framework creates a new legal category of biometric data, which could be qualified of 'biometric personal data' to reflect their nature as personal data.

[125] art 9(2) GDPR provides for ten exceptions including explicit consent, legal obligations of the controller in the field of employment or social security and protection of the vital interests of the data subjects or of another individual.

[126] art 9(4) GDPR reads as follows: 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.'

The new provisions also add the category of biometric data to the list of sensitive data, but not by virtue of their nature. In the new regime, the purpose of processing (that is, to uniquely identify an individual) determines the application of the regime of protection. This condition is connected to the threshold of identification applicable to biometric data. However, taking into account the state of the art in biometric technologies, it is debatable whether biometric data should rather have been treated as sensitive by nature.