Having Yes, Using No ? About the new legal regime for biometric data

E. J. Kindt

KU Leuven – Law Faculty – Citip – iMec
Sint-Michielsstraat 6
B-3000 Leuven
els.kindt @law.kuleuven.be

Universiteit Leiden - Law Faculty - eLaw Leiden
Kamerlingh Onnes
Steenschuur 25
NDL-2311ES Leiden

Post-doc legal researcher, KU Leuven – Citip

Associate professor, Universiteit Leiden – eLaw

Abstract: The rise of biometric data use in personal consumer objects and governmental (surveillance) applications is irreversible. This article analyses the latest attempt by the General Data Protection Regulation (EU) 2016/679 and the Directive (EU) 2016/680 to regulate biometric data use in the European Union. We argue that the new Regulation fails to provide clear rules and protection which is much needed out of respect of fundamental rights and freedoms by making an arteficial distinction between various categories of biometric data. This distinction neglects the case law of the European Court of Human Rights and serves the interests of large (governmental) databases. While we support regulating the use and the general prohibition in the GDPR of using biometric data for identification, we regret this limited subjective and use based approach. We argue that the collection, storage and retention of biometric images in databases should be tackled (objective approach). We further argue that based on the distinctions made in the GDPR, several categories of personal data relating to physical, physiological or behavioural characteristics are made to which different regimes apply. Member States are left to adopt or modify their more specific national rules which are eagerly awaited. We contend that the complex legal framework risks posing headaches to bona fidae companies deploying biometric data for multifactor authentication and that the new legal regime is not reaching its goal of finding a balance between the free movement of such data and protecting citizens. Law enforcement authorities also need clear guidance. It is questioned whether Directive (EU)2016/680 provides this.

Key words: Biometric data - data protection – new definition – unique identification – sensitive data - Regulation (EU) 2016/679 - GDPR – Directive (EU) 2016/680

Introduction

The launch of the iPhone X with face recognition deserves our attention in many respects . The 10th anniversary of the introduction of the now omnipresent smart phone was celebrated with the confirmation of the use of face recognition – as widely speculated – for unlocking the phone. It is in the first place irrefutable that for a wide spread population biometric data use becomes evident and the norm in all kinds of personalized objects which need security ànd convenience. This type of use therefore leads to a considerable *increased public acceptance* of collecting unique human characteristics in a context other than crime, for a large number of purposes.[1] In addition, and when looking closer, we should discern that precisely these types of biometric deployment will further

[1] The next step our information society is awaiting is the seamless carry-over of the login based on unique human characteristics to other 'Things', e.g., when one steps into her or his car or home, realizing the perfectly convenient body to machine communication.

increase important *collections* of biometric data.[2] At the same time, it remains unsure *where* these types of data are or will be stored, all depending on the 'playbook' of the architect of the system.[3] Laws have not provided clear guidance in the past. The question is whether this will change with the 'modernized' data protection legislation in the European Union.

The place of storage of biometric data is a relevant and critical factor. The storage place will to an important extent determine how such unique characteristics can be used: once the data is stored *in a database*[4], biometric technology permits anyone to conduct an analysis and *searches* by comparing biometric information[5] captured in real-time or collected in any other way *post factum* with the pre-existing enrolment database. In this way one can in an automated manner directly or indirectly identify a person, *i.e.*, to find out *who this person is,* based on physical, physiological or behavioural characteristics. As mentioned, the number of these biometric databases are growing, both in the hands of private and public entities. In other words, if someone has a face of a person and any database containing information about this individual and for example facial images, he or she could use this facial information to identify this individual and to take any action as desired. The central storage of biometric data allows for identification of individuals, in both private and public places, which definitely changes such spaces. But it also changes government, policing and intelligence activities. In a technocratic society, this given may presently only be known or understood by a limited group of experts, resulting in limited or no discussion about the collection or use of biometric data and about the powers and risks of the misuse of biometric technology. 'The greatest dangers to liberty lurk in insidious encroachment of men of zeal, well meaning but without understanding'.[6] While biometric technology surely can be supported and be effective for specific purposes such as crime investigation by competent authorities under clear legal conditions and independent oversight, any widespread use of such technology without or outside a clear legal framework should be worrying, but also the data collection of the biometric information *allowing* for such use. Once information is collected, such information will be used. This has been clearly proven already by the ever largest biometric collection and database Aadhaar in India, which was at its set up to be voluntarily and of which the objective was to provide citizen with a unique citizen ID. Soon thereafter, the collection became mandatory, for example to receive school meals or to open bank accounts, and access was provided to numerous non-governmental private sector entities for clearly

[2] Such important data collections have been induced already by other so-called Big Five tech companies (Alphabet, Amazon, Apple, Facebook and Microsoft) such as when improving social network services and users were invited in posting (profile) pictures.

[3] While Apple announced in 2013 at the release of the iPhone 5S, embedding fingerprint recognition (Touch ID) for unlocking the phone that the fingerprint would never leave the phone and would not be stored in the cloud, one needs to discern that the technology functions as a black box. In addition, and shortly thereafter, Apple filed patents for synchronizing Touch ID with other mobile devices and points of sale systems via iCloud whereby the (encrypted) fingerprints would actually be stored in the cloud. About these patents, see e.g., Ch. Zibreg, *Apple patents Touch ID iCloud sync, Apple Pay POS with embedded fingerprint sensor*, 15.1.2015, available at http://www.idownloadblog.com/2015/01/15/apple-patent-touchid-icloud/

[4] For example, a database with mug shots of the police, a national registry with the facial images (and possibly fingerprints) and other identity details of citizens to whom an eID, passport or drivers' license has been issued, an employee database with pictures, a membership list of a sports club and facial images, a list of missing persons, ….

[5] E.g., facial images from a CCTV system, facial images from simultaneous high quality video streams brought together on a platform or taken by a body worn camera, facial images from a social network platform or taken by a smart phone, real-times scanned faces of pedestrians, latent (found) fingerprints of an unidentified person, …

[6] Justice Brandeis, dissenting, in *Olmstead v United States*, 277 US 438 (1928), 277. This Supreme Court case concerned the question whether wiretapping technology allowing governments tapping public telephone conversations invaded privacy. The Supreme Court affirmed a privacy invasion by wiretapping public telephone conversations only forty (40) years later in *Katz vs. United States* of 1967.

different purposes.[7] This risk of collection and re-use was also at stake in the European Court of Justice cases *Schwarz* and *Willems* initiated by citizens who did not wish to part with their 'biometric data', which we discuss later. The collection of biometric data and the loss of anonymity poses risks to the exercise of fundamental rights, including but not limited to the rights to non-discrimination, freedom of expression, information and communication, freedom of assembly, due process and privacy and data protection and the entitlement to the presumption of innocence.[8] The Constitutional Court in France was in 2012 clear on the issue and stated that the keeping of a database with biometric identity information allowing identification interfered with the fundamental right to respect of privacy.[9]

The powers of biometric technology seems overall to be more a point of attention and debate in the United States. The Federal Trade Commission ('FTC') started in 2011 an investigation into the risks of the use of face recognition, after complaints over Facebook's use of facial recognition technology filed by four consumer protection organizations, led by the Electronic Privacy Information Center. Major stakeholders sat around the table in a conference 'Face Facts' at the end of 2011, and a report with recommendations was issued by the FTC shortly thereafter.[10] In the hearings and in the reports, it is clearly admitted that face recognition threatens anonymity. Another report of the Georgetown Law's Center on Privacy and Technology of 2016 revealed how law enforcement officials compare in several U.S. states the faces of suspects with photographs of (unsuspected) individuals based on the repository of their pictures in the driver's licenses and other databases or just taken from surveillance camera's or from pedestrians walking on the street. Such practices are allowing for a permanent virtual line-up, without any consent or warrant or limitation to serious crime.[11] Without clear regulation of the use of the technology, innocent people risk to be identified in political or religious speech activities, to be tracked and traced, to be controlled and manipulated, to be stigmatized or treated as suspects, or at least to have such feeling, which is precisely what the surveillance society is about.[12] Biometric identification technology considerably shifts the (power) relations between persons. While individuals more or less control non-automated identification by providing others with identifying information, and hence know to whom such information is or could become available, this changes with automated (biometric) identification technology enabling anyone to obtain much information about particular individuals without these individuals being necessarily informed of being recognized or identified 'just by their face' or other biometric

[7] Several individuals filed complaints against this biometric collection. In the meantime, the Supreme Court of India recognized the right to privacy as a fundamental right, which decision will further impact Aadhaar : Supreme Court of India, No 494 OF 2012, 24.8.2017, available at http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

[8] See also E. Kindt, *Privacy and Data Protection Issues of Biometric Applications.* A Comparative Legal Analysis, Dordrecht, Springer, 2013, pp. 297-306 ('Kindt, Biometric Applications 2013').

[9] Cons. const. (France) n°2012-652, 22 March 2012 (*Loi protection de l'identité*), § 6. The Court stated: '(…) la création d'un fichier d'identité biométrique (...) dont les caractéristiques rendent possible l'identification d'une personne à partir de ses empreintes digitales porte atteinte inconstitutionnelle au droit au respect de la vie privée'.

[10] See Federal Trade Commission, *Facing Facts. Best Practices for Common Uses of Facial Recognition Technologies*, October 2012, 30 p., available at http://ftc.gov/os/2012/10/121022facialtechrpt.pdf

[11] C. Garvie, A. Bedoya and J. Frankle, *The perpetual Line-up. Unregulated Police Recognition in America,* 18.10.2016, 119 p., Georgetown Law. Center on Privacy & Technology, available at https://www.perpetuallineup.org/ (Garvie e.a., Perpetual Line-up, 2016).

[12] The European Court of Justice pointed to this risk of stigmatization in *S. and Marper* (§ 122) (see *below*) and reminded of the risks of indiscriminate surveillance and its chilling effects for data being retained for a long period and subsequently used without information, which is such as "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". See ECJ, joined cases C-293-12 and C-594/12, *Digital Rights Ireland v. Minister for Communications* e.a., 8.04.2014, §37 ('ECJ, Digital Rights 2014').

characteristics. Such technology can be used by governments and autocracies to remain in power, to threaten and control any new beneficial but deviating individual opinions, beliefs and actions, and in the end, such a society does not allow for improvements and is condemned to deteriorate, to stagger and in the end, to die. And biometric data and technology deserves a better future.

In this article, we analyze the new legal regime applicable in the European Union to the collection and use of personal data relating to the physical, physiological or behavioural characteristics of a natural person. The Regulation (EU) 2016/679[13], directly applicable as of 25 May 2018 in all EU Member States, contains a new regime and a new definition of biometric data.[14] It contains an updated list of so-called special categories of personal data, commonly known as 'sensitive data' and mentions in this list a particular use of biometric data. Furthermore, if a processing, in particular when using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, there is a new obligation for the controllers to assess the impact and risks of such operations in a so-called data protection impact assessment and to take safeguards, and if needed, to consult with the supervisory authority and obtain authorisation. Member States will also have to implement Directive (EU) 2016/680 which contains some similar while different provisions relating to biometric data for law enforcement authorities. We analyze in a succinct way these new provisions and discuss to which extent the new regulatory framework reaches its objective of clear rules for all stakeholders, harmonized regulation and increased protection, in particular of the fundamental rights and freedoms as proclaimed.

1 New principles for biometric data use in the EU

1.1. The use of biometric data for identification is in principle prohibited under the GDPR

The Regulation (EU) 2016/679 has added to the list of 'sensitive' data a new category of special data: 'biometric data *processed* for the purpose of *uniquely identifying* a natural person'.[15] This list of 'sensitive' data traditionally mentions personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, … [16] and is now updated by the GDPR.

As a result and as a general principle, the processing of biometric data for the purpose of uniquely identifying a natural person, as the processing of all other special categories of personal data, is *forbidden*.[17] This prohibition to process these special categories of data exists because these types of data are considered sensitive by their nature, for example because they may unduly discriminate or stigmatize if processed.[18] This implies that all entities falling under the material scope of the GDPR, including public authorities, governments and private organizations, are in principle not allowed to

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *O.J.* L 119, 4.05.2016, pp. 1-88, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL ('Regulation (EU) 2016/679' or 'GDPR').
[14] Article 4 (14) GDPR.
[15] Art. 9.1 GDPR.
[16] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, pp. 31-50 ('Directive 95/46/EC'), art. 8(1) and art. 8(5), and as implemented in national data protection legislations.
[17] Art. 9.1 GDPR.
[18] Processing can be any operation or set of operations performed on personal data, including, whether or not by automated means, collecting, recording and storing. See Art. 4(2) GDPR.

process biometric data for 'unique identification'. For example, a shopping mall would in principle not be entitled to identify troublemakers by using a biometric comparison.[19] For law enforcement authorities, a separate regime applies, as we discuss below.

Several exemptions from the prohibition to process biometric data for uniquely identifying and the other special categories of data however exist, in total ten (10) and are described in detail.[20] It is likely that there will remain discussion about the principle and several of these exemptions, both on the level of the theory as in practical applications. For example, the first exemption is the 'explicit consent' of the data subject. Will the choice of going to or stepping into a place which is open to the public, be equal to a free, informed and specific explicit consent provided the required legal information about biometric identification is provided ? If the consent were to be asked in a clearly contractual context along general terms and conditions, article 7 GDPR provides more guidance.[21] Another exemption is if the processing is necessary 'for reasons of substantial public interest', provided there is a law which (i) is proportionate, (ii) respects the essence of data protection and (iii) provides for suitable and specific safeguards for fundamental rights and interests. But what is substantial public interest ? Which safeguards need to be implemented ?[22] And also, what means 'unique' identification ?[23] Another interesting question is whether one could argue that when the controller collects biometric data and stores such in a database (which is considered 'processing'), *knowing* that the storage in a database *permits identification* in the future, this fact of storing in a database could or should be considered processing of biometric data for the *purpose* of uniquely identifying ? And what if one collects the data and has the clear intention to use identification, but only in the near future, or maybe the far future ? Or a third party has such intention ? Any (intended) future use of the data should in our view be taken into account for ascertaining the applicable legal framework. If not, this would be contrary to the intention of the legislator for the granted protection. However, strictly speaking, the data, if mere images, are at that point however not yet biometric data as defined.[24] An intriguing exception relevant for biometric data processing is the exception and hence the permission to process biometric data for purposes of uniquely identifying where the data subject has manifestly made the data public. Would this exception allow for face recognition, even without explicit consent or law stating a substantial public interest ?

[19] The purpose of such processing could be, for example, to deny access.

[20] See Art. 9.2 GDPR.

[21] Art. 7(2) GDPR requires that the request for consent in the context of a written declaration is presented (i) in a manner which is clearly distinguishable from the other matters, (ii) in an intelligible and easily accessible form and (iii) using clear and plain language. Moreover, Art. 7(2) GDPR stresses that consent cannot be freely given and obtained if it is not separated from the provision of the services under a contract which does not require personal data processing.

[22] For previous guidelines on biometric data processing, including about safeguards, and which could still be useful, see also Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, 11 p. ('WP 29 Working Document on Biometrics 2003 (WP80)'), Article 29 Data Protection Working Party, *Opinion 3/2011 on developments in biometric technologies,* WP193, 27 April 2012, 34 p. and Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services*, WP192, 22 March 2012, 9 p.

[23] About this concept, see also (forthcoming) I. Schols, D. Meuwly, M. Dubelaar, J. Nietfeld and E. Kindt, *Legal aspects of the (re)use of biometric data for forensic research.* Interesting is also the note in the ISO Standard Vocabulary for biometrics 2017 to term 3.3.12 'biometric identification decision' that return of a candidate list is not considered a biometric identification decision.

[24] The collection and regulation on such collection in combination with an intended or unintended future use is hence presently unclear in the present framework. See and compare with the Protection of Freedoms Act 2012 in the United Kingdom, regulating biometric data use (by law enforcement (Chapter 1) and in schools (Chapter 2)) and which includes the intention in the definition of biometric information in Chapter 2 (see Chapter 2, § 28 (2)). About this Act, see also *below*.

One can say that there is more clarity on the level of the principle that the *use* of biometric technology for *identification* is a processing of a special category of personal data, which is overall *prohibited*. It means in our opinion that there is for example as a matter of principle a prohibition to use biometric comparison for identification or singling out based on so-called 'black lists', provided one of the exemptions could not be invoked. In any case, exemptions are possible and will have to be carefully reviewed and implemented.

In five of the ten exemptions of Article 9 (2) GDPR, additional Union or Member State *law*, providing safeguards for the fundamental rights and interests of the individuals concerned, is needed.[25] For the exemption by explicit consent, it is interesting to note that Union or Member state law may precisely limit - rather than allow- the cases where one could explicitly consent. This leaves Member States to carefully think about situations where biometric identification, based on consent, may not be desirable. We discuss this further below.

It is hence important to note that article 9 GDPR does *not consider all* processing of biometric data as defined (see below) as 'sensitive'. The list of 'sensitive data' mentions (only) biometric data *processed for the purpose of uniquely identifying* a natural person. This requires and implies the use of a database or list as mentioned above.

The processing for *verification purposes* hence does not fall under this general prohibition.[26] Decision makers, if non-experts, may not ascertain the (technical) difference between identification and verification or be able to understand in particular cases which functionality is used. In both cases, information is collected and compared, while the place of storage is far less understood or visible.

1.2 Law enforcement authorities and biometric data

The fore-mentioned general prohibition to process biometric data for uniquely identifying a natural person is *not* maintained in Directive (EU) 2016/680 (a) in the prevention and fight against crime or execution of penalties, or (b) when safeguarding against and preventing threats to public security, (c) provided the data are processed by so-called competent authorities.[27] Such authorities are allowed to process biometric data for unique identification under three *cumulative* conditions: (i) if 'strictly necessary', *and* (ii) if subject to appropriate safeguards for the rights and freedoms of the data

[25] See also our arguments in favor of law in E. Kindt, *Privacy and Data Protection Issues of Biometric Applications.* A Comparative Legal Analysis, Dordrecht, Springer, 2013, pp. 745-754 ('Kindt, Biometric Applications 2013').

[26] For the definition of these two functionalities, see also the (refreshed) ISO/IEC 2382-37:2017, Information technology – Vocabulary, Part 37: Biometrics ('ISO Standard Vocabulary for biometrics 2017'). The distinction between these two functionalities, whereby identification requires a list of data records, is of key importance for the discussion and regulation of biometric data processing.

[27] See 'competent authority' in Art. 3 (7) of the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *O.J.* L 119, 4.05.2016, pp. 89-131, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL (' Directive (EU) 2016/680' or 'Law Enforcement Directive'). Such authority is therein defined as either a public authority or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This Directive shall be implemented by Member States by 6 May 2018 and such national law applied by same date, or by 6.5.2023 for systems existing before 6.5.2016 and requiring disproportionate effort.

subject, *and* only (iii) (a) where authorized by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; *or* (c) where such processing relates to data which are manifestly made public by the data subject.[28]

It can be defended and understood that the general prohibition of the GDPR to process biometric data for unique identification should not apply for law enforcement authorities ('LEAs'). Using facial images, fingerprints, etc has always been important in policing and it is the task of the LEAs and it could be in the public interest that such images are used to prevent, detect and prosecute crime, upon the conditions that there is a clear legal framework and that any use, including the storage, is proportionate. Only when there is a clear legal framework, LEAs could be entitled to identify suspects, based on images contained in for example CCTV footage registering a crime and comparing these with databases of previously convicted criminals or arrested suspects. However, the European Court of Human Rights has clearly stated in *S. and Marper* that already the *retention* of fingerprints by LEAs amounts to an interference with the right to respect for private life.[29] In other words, it is of key importance to note that the European Court of Human Rights reiterated that the *mere retention and storage* of personal data by public authorities are to be regarded as having direct impact on the private life interests of an individual, *irrespective of whether subsequent use is made of the data.*[30] In another case involving the retention of fingerprints taken in the context of two investigations into alleged book theft and the request for the removal by the individual concerned, the same Court stressed in *M.K. v. France* that the protection of personal data is of fundamental importance to a person's enjoyment of her or his right to respect for private life, the more when such data undergo automatic processing and are used for police purposes. The Court concluded again that the retention amounted to disproportionate interference with the right to respect for private life because the French national *law failed* to ensure that *the data were relevant and not excessive* in relation to the purposes for which they were *stored*.[31] These two important cases show *the vulnerability of any retention of biometric data and its interference with fundamental rights.* National law shall hence carefully regulate *in a proportionate manner* the registration, the keeping and the use of well defined and such pre-existing biometric databases held by LEAs and used for such biometric identification tasks.[32] Such national law framing the storage of particular biometric data is presently however often

[28] Art. 10 Directive (EU) 2016/680.

[29] The Court stated that 'fingerprints objectively *contain unique information* about the individual concerned *allowing his or her identification with precision* in a wide range of circumstances. They are thus *capable of affecting his or her private life(…)*' and that 'the *retention* of fingerprints *constitutes an interference* with the right to respect for private life '(emphasis added). See ECtHR, *S. and Marper v. United Kingdom*, nos. 30562/04 and 30566/04, 4.12 2008, § 84 and § 86 ('ECtHR, S. and Marper 2008').

[30] The Court hereby referred to previous case law in *Leander v. Sweden* and *Amann v. Switzerland*. See ECtHR, S. and Marper 2008, §67 and §124. It is then further required to pay due regard to the specific context of the recording and retention, the nature of the records, the way of use and processing and the results obtained (§ 67).

[31] In this case, the data of a citizen was kept on a police database for 25 years. Because the prospects of success of a request to be removed was uncertain and therefore a 'deceptive guarantee', the Court found that this equated to a retention for an indeterminate period. The retention was hence not regarded as *necessary in a democratic society:* ECtHR, *M.K. v. France*, no.19522/09, 18.4.2013, §§ 44-46 ('ECtHR, M.K. 2013').

[32] For further criteria, see ECtHR, S. and Marper 2008, also discussed in Kindt, Biometric applications, 2013 and ECtHR, M.K. 2013. For example, the United Kingdom has in the meantime adapted its national legislation for the retention of DNA and fingerprints (see sections 1 to 25 of the Protection of Freedoms Act 2012). As a result, in the United Kingdom only individuals *convicted* will now have their fingerprint records and DNA profiles retained indefinitely.

lacking in Member States. One of the concerns here is hence that these databases continuously grow and biometric data, such as facial images, are retained ànd used without clear legal basis.[33]

Another important critical factor in our view is also the increased access by LEAs to biometric databases held by third parties, and the use for identification purposes for LEAs' tasks, while these databases were initially not set up for LEAs use.[34] We would call this a trend of 'the growing biometric crowd of suspects'. Since LEAs have obtained access to such databases of non-EU citizens, one should at least worry that the next step may be a political agreement and subsequent legislation allowing for access to databases of EU citizens, such as for example national identity biometric databases[35]. This would allow cyber policing relying on biometric databases by identifying individuals with the aid of global (non LEA) biometric databases held by third parties in the private or public sector. And what about the taking of images of the crowd and real-time scanning on the street ? This is problematic, as contrary to the use of databases of convicted criminals or arrested suspects, such access – but also the real-time recording of the images - would imply that all (EU) citizens are continuously but almost invisibly treated as being suspected, without individualized suspicion, with no warrant. As this could only be defended in exceptional circumstances such as life-threatening public emergencies backed by specific events, law and possibly court order, access and use in all other situations implies a constant (threat of) surveillance.

As mentioned, LEAs are entitled to process biometric data for uniquely identifying provided this is 'strictly necessary', with safeguards and based on law safe two exceptions. In this context, as already mentioned above, the question is particularly relevant what shall be understood under 'data manifestly made public' ? Are the facial images captured by surveillance cameras in public places, data 'manifestly made public by the data subject' ? Or is this exception about the use of images and footage posted on public social networks ? This is an important question. In case images taken by surveillance cameras in public places could be processed, even no law would be required, only 'strict necessity'[36] as well as safeguards. And what are these safeguards? If a public notice of camera surveillance would be available for these places, would this be sufficient to deploy intelligent camera's linked with lists of databases of 'wanted people' to compare continuously all the faces of all the individuals in a public place ? In other words, is police as a competent authority entitled to scan images of persons in public places and compare these for identification purposes with a suspect list ?[37] We believe that the continuous biometric comparison for identification purposes in a public

[33] See, e.g., in the United Kingdom and the High Court decision of 22.6.2012 criticizing the lack of legal basis for the retention of *facial images* in U.K. police databases: *RMC and FJ v Commissioner of Police for the Metropolis and Secretary of State for the Home Department* [2012] EWHC 1681, available at https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/Judgments/r-rmc-fj-metropolitan-police-commissioner-22062012.pdf See also X, *'UK Biometrics Commissioner criticizes review of retention and use of custody image's, in Biometric Technology Today,* ScienceDirect, April 2017, also available at http://www.sciencedirect.com/science/ article/pii/S0969476517300632?via%3Dihub

[34] E.g., access by LEAs to databases of non-EU citizens, such as asylumseekers (Eurodac) and visum applicants (VIS), while the initial biometric registration of these persons in databases was not related to any use for criminal investigations.

[35] This is precisely at stake in the discussion about the biometric databases in the framework of identity or travel documents. See in this context also *below* about *Schwarz* and *Willems* of the European Court of Justice.

[36] The strict necessity criterion seems to be derived from case law of the European Court of Justice about interference with articles 7 and 8 EU charter Fundamental Rights (see ECJ, Case C-92/09, *Volker und Markus Schecke v. Land Hessen, Eifert v. Land Hessen*, 9.11.2010, where it is used for one of the first times, and later repeated, including in e.g., ECJ, Digital Rights 2014.

[37] These practices seem to exist in some Member States. See, e.g., in the Netherlands, J. Schellevis, *Politie gaat verdachten opsporen met gezichtsherkenning,* Nederlandse publieke oproep, 16.12.2016, available at https://nos.nl/artikel/2148598-politie-gaat-verdachten-opsporen-met-gezichtsherkenning.html

place[38] would not align with the 'strictly necessity' criterion in most cases. However, in case of urgency related to and backed by a serious crime or terrorist event, one could defend that such comparison may for a limited time be 'strictly necessary' subject to appropriate safeguards, such as independent oversight and strict limitation of the purposes. These are however important questions which shall be debated when CCTV cameras become linked and equipped with new functionalities and the camera surveillance laws need to be updated.

We argue that the national legislator shall hence define *by law* clear conditions meeting the fundamental rights and freedoms checks for such biometric comparison and identification.

1.3. DPIA, prior consultation and prior authorization

- DPIA needed in case of the processing of a special category of personal data on a large scale

Regulation (EU) 2016/679 imposes in addition upon the controller an obligation for a data protection impact assessment (DPIA), *inter alia* when special categories of data are processed *on a large scale*.[39] As discussed above, if biometric data are used for uniquely identifying, such processing is considered the processing of a special category of personal data, and consequently, such processing, upon the condition that it is *on a large scale*, would, if permitted and hence based on one of the exemptions as briefly discussed above, have to be submitted to an assessment exercise, named DPIA (formerly also known as a PIA). This is in accordance with the global rationale of the GDPR that the controller is responsible and shall demonstrate compliance with the legislation as required by the new principle of being accountable for the processing.[40] The DPIA is herein an important tool.

Making an impact assessment under data protection is a new obligation under the GDPR and creates lots of concern and questions. For example, as of when would a biometric use for uniquely identifying be on a large scale ? To assess the scale, large scale processing operations would aim at processing 'a considerable amount of personal data at regional, national or supranational level' and which 'could affect a large number of data subjects'.[41] Further guidelines for such DPIA have been provided by the Article 29 Working Party.[42] Some national DPAs, such as in the United Kingdom and in France, have also provided more information and guidance on a DPIA in general, and in some case also specific for biometric data.[43]

---

[38] A further distinction could be made between 'positive' and 'negative' identification, although these terms are depreciated. In the first case, one tries to find out if an individual is in an affirmative way identified as being on a list (e.g., a list of suspects), while in the second case one checks if an individual is not on a list (or database). Both comparisons in public places, if continuously, are in our view not 'strictly necessity' in most cases.

[39] This is the second (explicit) scenario requiring a DPIA which expressly refers to the processing (a) on a large scale (b) of *special categories* of data of Article 9(1) or of Article 10. See Art. 35.3(b) GDPR.

[40] This is the 'accountability principle', and is explicitly mentioned as a general principle in Article 5 (2) GDPR.

[41] See Recital 91 GDPR. E.g., we could think of the case where a banking institution would offer and implement to a large clientele biometric login.

[42] See Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4.4.2017, WP 248, 21 p. ('WP 29 Guidelines on DPIA (WP248)'). The Article 29 Working Party will as of May 2018 be reformed in the European Data Protection Board ('EDPB').

[43] See, e.g., France, CNIL, *Délibération n°2016-187* of 30 June 2016 relating to the 'unique authorization' for access control to places, devices and computer applications in the workplace based on templates stored in a database (AU-053), 15 p., available at https://www.cnil.fr/sites/default/files/atoms/files/au-053.pdf , and *Grille*

The Directive (EU) 2016/680 also imposes an obligation for controllers for making a DPIA. The latter however does contain only a more general provision similar to Art. 35.1 GDPR (see also below).[44]

The DPIA shall always be done *before* the start of the processing. The GDPR prescribes further what such DPIA shall contain.[45] Where appropriate, the views of the data subjects shall also be sought.[46] The controller is responsible for the carrying-out of the DPIA to evaluate, in particular, 'the origin, nature, particularity and severity' of the risk. The outcome of the assessment shall then be taken into account for determining the appropriate measures to be taken to mitigate the risks in order to demonstrate that the processing of the personal data complies with the Regulation. The GDPR hereby takes up defined components of more general risk management processes, e.g., as known in ISO 31000 reviews. The international standard ISO/IEC 29134 will also provide for more guidelines on the methodology for such DPIA.[47]

Such DPIA for biometric data processing is an iterative process and each of the stages to be revisited multiple times before the DPIA can be completed. A DPIA is hence an important exercise which will require the necessary time, skills and insights in the biometric application, as well as the organizational and technical measures, but also in the legal requirements. The controller is further free to publish the DPIA or not.

- Prior consultation and prior authorization

Moreover, prior consultation with the supervisory authority (currently the data protection authority or 'DPA') will be needed in case the DPIA indicates that the processing *would result in a high risk in the absence of or which the controller cannot mitigate by appropriate measures '*in terms of available technology and costs of implementation'.[48] Hence, such prior consultation would only be required when *residual risks remain high*[49] and the data controller cannot find sufficient measures to cope with them. For available technology to cope with particular risks, one could think of for example the use of so-called 'protected biometric information' or 'protected templates'.[50]

A consultation with the DPA will also be needed if national law requires prior authorization for a task carried out in the public interest.[51] Some Member States, such as France, have specific national law requiring authorization and have developed for biometric applications a whole 'jurisprudence' in relation to such authorizations as well as have issued specific so-called unique authorizations which allow controllers to adhere to pre-defined strict conditions.

D'Analyse, 11 p., available at https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail

[44] Art. 27.1 Directive (EU) 2016/680.

[45] See Art. 35.7 GDPR and recitals 84 and 90 GDPR. See also WP 29 Guidelines on DPIA (WP248).

[46] These views could be sought through a variety of means. See WP 29 Guidelines on DPIA (WP248), p. 13.

[47] See ISO/IEC 29134, Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO).

[48] Recital 84 GDPR. See Art. 36 GDPR.

[49] An example of an unacceptable high residual risk given by the Art. 29 WP is where 'the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome, and/or when it seems obvious that the risk will occur.' In the biometric context, this could be where the data subject cannot change its biometric credentials in case of theft of its biometric identity details (WP 29 Guidelines on DPIA (WP248), p. 18).

[50] See also EDPS, Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs), p. 3, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf ; Kindt, Biometric Applications 2013, pp. 792-805.

[51] Art. 36 (5) GDPR.

2 A new definition of biometric data

2.1 The new definition

To fully understand the explanation above, one shall know however that the (mere) collection, storing and keeping of physical, physiological or behavioural characteristics of a natural person does not fall under any specific regulation or benefit from any specific protection, other than the general data protection regime under the GDPR, replacing the Directive 95/46/EC and implementing national laws, and the Directive (EU) 2016/680 for the processing activities of the 'competent authorities'.

Not all data and data processing relating to the physical, physiological or behavioural characteristics of a natural person which permit verification or identification of a natural person is considered biometric data under the GDPR and the Directive (EU) 2016/680. Merely collecting and keeping such data, without any specific biometric processing, do not fall under the fore-mentioned specific protection we discussed above (see also table 1 *below*).

This is due to the rather narrow concept and definition of biometric data in the GDPR and in the Directive (EU) 2016/680. Data are considered biometric data under the GDPR only if the data 'result from specific technical processing' 'relating to the physical, physiological or behavioural characteristics of a natural person', ' which allow or confirm the unique identification of that natural person'. Further, the examples of facial images and dactyloscopic data (fingerprints) are given in the same definition.[52] The definition in the GDPR and the Directive (EU) 2016/680 are identical.

We expect further discussion about this definition.[53] A database with facial images or fingerprints without biometric processing would hence *not* be considered a database with biometric data or a biometric database. The setting up or the keeping of such database is hence also not subject to specific protective rules for biometric data processing, as discussed above, other than the data protection rules which apply to all personal data, such as under the GDPR the need for one of the six legal bases for personal data processing, including consent, an information obligation, record keeping, etc. We contend however that precisely such databases are the pre-condition and allow for biometric identification, as explained above, and such databases are therefore a risk for the fundamental rights and freedoms of the data subjects. Therefore, the 'fitness' of data to be used by automated means for identification or identity verification purposes should in our view rather be taken into account when developing a legal protective framework for the use of biometric data.[54] This would be - what we call - an objective approach.

The mere collecting and storing of facial images, fingerprints or iris images, … is by the legislator hence not considered as biometric data or processing biometric data. Facial images only become biometric data under the GDPR and the Directive (EU) 2016/680 if they are used for biometric comparison, and more precisely, if they are the result of 'specific technical processing'. This is what we understand from the new legal definition. Hence, as soon as the images are prepared for a biometric comparison, e.g., starting with enhancing the images for biometric extraction of relevant

[52] Art. 4(14) GDPR. For a critical assessment of the changes introduced into the definition, see also C. A. Jasserand , 'Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data', *EDPL* 2016, pp. 297-311. See also C. A. 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', *IDPL* 2016, pp. 63-76.

[53] A detailed analysis of the new definition is not within the aim of this article.

[54] See also Kindt, Biometric Applications 2013, p., 149 and the proposed definition therein.

information, as well as any further processing, such as the processing of templates or transformation into binary strings, the data would become biometric data and the processing biometric processing. But even if such processing is a processing of biometric data, as mentioned, no additional rules other than the general data protection rules seem to apply, for example, if the data would not be used for identification but only be used for verification. This is very important to distinguish and to understand.

Governmental databases, collecting and keeping images of faces or fingerprints, for example collected for eID cards, do hence not fall under any specific biometric legislation if not used for identification purposes, other than the general data protection rules, as for all other personal data. There are hence no major restrictions or specific protection for such data collections. However, at the same time, such collections remain vulnerable for re-use, including biometric comparison and use for identification purposes.

2.2 Origin of the new definition

The component 'resulting from specific technical processing' is the most striking element in the new definition. This component was added following a political agreement in the text of the Council in its General Approach adopted on 15 June 2015. The GDPR itself does not provide much explanation on how to interpret this. For example, does the 'specific technical processing' refer to the technical processing by a biometric system ?[55]

The wording 'resulting from a specific technical processing' added in the text of the definition by the Council can be traced back to wording that was proposed by the Committee on Bioethics in its opinion adopted at its 1st meeting in 2012 at the occasion of the revision of the Convention 108 of the Council of Europe.[56] This Convention N° 108 adopted in 1981 was also the text on which the Directive 95/46 was based.

The Committee on Bioethics was assigned in 2012-2013 with intergovernmental work on the protection of human rights in the field of biomedicine, however, and in the context of the Convention N° 164 for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine.[57] In its opinion with proposals on the modernization of Convention N°108, the Committee made observations and reviewed the concepts of genetic data and biometric data as contained in the proposals of the EU Commission and 'whether or not they may be considered sensitive data' to 'ensuring a harmonized approach'. The Committee herein stated that 'many data classed as biometric according to the definition[58], such as photos or audio or

[55] There is no reference to a biometric system in the definition, but it is likely that this should be interpreted in this way.

[56] Committee on Bioethics, Opinion on the document of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) entitled 'Modernisation of Convention 108: new proposals', DH-BIO (2012) 12 final, Restricted, 21.6.2012, p.6 ('Bioethics Committee, DH-BIO (2012) 12 final').

[57] The Committee was set up as consultative committee supporting the Steering Committee on Bioethics, in particular to re-examine the Biomedicine Convention and to examine legal challenges raised by developments in the biomedical field. See for the terms of reference of their mission for 2012-2013, Committee on Bioethics (DH-BIO) Terms of Reference, DH-BIO/INFO (2012) 2, 4 p. available at http://www.coe.int/t/dg3/health bioethic/cdbi/DH-BIO_INF_2012_2_TOR_e.pdf

[58] Reference was made to the definition of biometric data in the proposal text of the EU Commission which was then 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'. 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 on the free movement of such data* (General Data Protection Regulation), COM(2012) 11

video recordings, are ordinary personal data, which in a large number of cases, will undergo ordinary processing (private exchanges of photos or videos, archiving or publication by a newspaper…)' (footnote added).[59] The Commission stated that this 'type of ordinary processing' did not seem to require the application of specific legal rules. But what is covered by ordinary processing ? It seems to make a distinction between ordinary photographs, audio and video recordings, as handled by private persons or newspapers not requiring in its views a specific protection and biometric processing of a biometric characteristic. Put in a different way, it stated that 'it would seem that in many cases what should be termed biometric is not the initial data, but rather the specific technical processing operations applied to these data and the resulting data'.[60] The Committee has hereby made a start of protection only as of a 'certain use': '(…) thus, where ordinary personal data are concerned, they would not be designated as sensitive in themselves; only a certain use of such data would be sensitive'.[61] Was the Committee familiar with the characteristics, functions and progress of biometric technology ? Biometric data is not the same as biomedical or genetic data. 'Ordinary personal data' such as photos or videos, do allow for far-reaching use, because of the progress in biometric technology and not always remains subject to just 'ordinary processing'. The 'private use' of photos uploaded on social networks offers the possibility to identify the individuals. Even a company as Google publicly acknowledged in 2010, by its CEO, at that time Eric Schmidt, the far reaching potential and consequences of mere pictures and the technology. Google did not want to push it at that time further by stating: 'Show us 14 photos of yourself and we can identify who you are. You think you don't have 14 photos of yourself on the internet? You've got Facebook photos!' and by saying that Google won't be connecting personal information to the real world via facial recognition which Google has available, which Schmidt said is '*just too creepy*' (emphasis added).[62] It is hence possible that the reasoning of the Committee was flawed by insufficient knowledge of biometric technology. The case law of the European Court of Human Rights, including its decision in *S. and Marper*, which stresses that the mere retention and keeping in a databases of biometric information does pose serious risks and constitutes an interference, seems also not to be taken into account. This may have far-reaching consequences.

Many other questions remain with the definition. For example, it is far from clear at which particular point in time any collected data become biometric data. And which characteristics are to be considered 'ordinary': while photographs of faces seem to be considered ordinary, does this also apply to photographs of fingerprints (fingerprint images) ? Further analyses is needed on these issues, while we assess hereunder already the impact thereof in a critical way. We argue that, in addition to highly uncertain answers to the two questions above, the distinction in the definition makes the data protection to data relating to the physical, physiological or behavioural characteristics of a natural person which allow identification (and which should therefore be considered in itself of a special category), limited and makes protection drifting further away from

final, Art. 4(11), 25.1.2012. Note that in this definition, reference was only made to the use for identification, and not for verification.

[59] Bioethics Committee, DH-BIO (2012) 12 final, p. 6.

[60] *Ibid.*

[61] *Ibid.*

[62] L. Gannes, *Eric Schmidt: Welcome to « Age of Augmented Humanity »,* 7.09.2010, available at http://gigaom.com/2010/09/07/eric-schmidt-welcome-to-the-age-of-augmented-humanity/

the moment of collection to the (uncontrollable) use of the data. This results in a 'theoretic and illusionary' protection.[63]

2.3. Evaluation

The European legislator made in our opinion an artificial distinction between personal data relating to biological or behavioural characteristics, such as images, which are the underlying prerequisites for any biometric process, and the personal data resulting from specific biometric technical processing operations, which are biometric data under the GDPR and the Directive (EU) 2016/680. The first kind of data are the initial data set from which any biometric comparison process could start provided it has sufficient quality, but are not considered as biometric data under the GDPR and the Directive (EU) 2016/680.

In other words, the legislator makes a distinction between 'having' and 'using', while one can see that it is a small step from 'having' to the 'using', whereby the data subject may not at all be further in control or receive any information about further use. The European legislator has furthermore also not taken the jurisprudence of the European Court of Human Rights into account, which *considers the retention and storage of biometric data as an interference with the fundamental rights*, *regardless of any subsequent use*.[64] While the specific context of any storage may remain important, the nature of the data *allow* for identification and are *fit*[65] for biometric comparison and identification with the increasing number of pre-enrolled biometric databases.

The new definition is also not in line with any other definition of biometric data, suggested for example by the Article 29 Working Party in its three opinions of more than a decade ago on biometric data processing. In its Working Document on biometrics of 2003, it states that '[t]his kind of data is of a special nature, as it relates to the behavioral and physiological characteristics of an individual and may allow his or her unique identification'.[66] The Working Party hereby refers in our opinion also to biometric sample (images). This definition of the Working Party has been repeated and was adopted in its Opinion 3/2012 as well. The Organization for Economic Co-Operation and Development (OECD) also mentions different definitions of 'biometrics' in its report on Biometric-based technologies of 2004.[67] Finally, it should be noted that the new definition in the GDPR is in our view also not in accordance with the understanding and definition of 'biometric data', as defined in term 3.3.6 in the ISO Standard Vocabulary 2017 for biometrics. The existence of these diverging definitions of biometric data risk to result in confusion and difficult debates.

[63] See also the wording in ECtHR, M.K. 2013, §44, being very critical for the 'theoretic and illusionary' right of removal of fingerprints provided in the French decree, as such right runs counter to the interests of the investigating services in maintaining a database with as much information as possible.

[64] See above, ECtHR, S. and Marper 2008 and ECtHR, M.K. 2013.

[65] Provided the data are of 'good quality'. Technology however is evolving in such way that images of less quality may become less an issue for biometric comparison than before.

[66] WP 29 Working Document on Biometrics 2003 (WP80), p. 2. See also and compare with Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP191, 23.03.2012, p. 10 (WP 29 Opinion on reform proposals 2012 (WP191)).The Article 29 Working Party therein suggested to 'focus on what types of data are to be considered biometric data instead of focusing on what they allow'. We do not agree however with this suggestion for the reasons explained in this article.

[67] OECD, Biometric-based technologies, 2004, p. 10-11. The OECD referred to definitions proposed by the International Biometric Group (IBG) and a definition of G. Roethenbaugh who defined a 'biometric' as 'a unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity' in G. Roethenbaugh, 'An introduction to Biometrics and General History', *Biometrics Explained,* 1998.

What is particularly annoying, is that even though an entity is not using collected photographs in a biometric process , e.g. a school who collected the facial images of its pupils, and hence is not under an obligation to make a specific assessment or to take safeguards according to the new legislative framework, *this collection is present and hence risks to also being used, whether or not by third parties*, albeit for different purposes than the initial collection.[68] Hence, an important aspect for governmental and non-governmental large databases, collecting and keeping images of faces or fingerprints, albeit for civil purposes, while the (original) controller does not or may not have any intention to use the collection for biometric identification purposes and hence is not subject to specific regulation under the present regime, is that such collection could always be searched, partially accessed, directly accessed and used by a third party for identification purposes, whether for a valid or invalid and illegal purpose. An additional question is who will be responsible *i.e.* be the controller who has to comply with Article 9 GDPR for the use in such case ? It may, in our opinion, only be this third party, adding the data collection to its realm of sources to effectuate biometric comparison and identification.

As the Article 29 Working party already clearly pointed out in 2005 in the context of the implementation of the ePassport Regulation, mandating Member States collecting the facial image and optionally fingerprint for securing such passport by storing it on the chip : 'Any central database would increase the risks of misuse and misappropriation. It would also intensify the dangers of abuse and function creep'.[69] The group of national DPAs hence expressed clearly reservations since more than 12 years about any centralized European or national database containing biometric data.

The European Court of Justice ('ECJ') had in the meantime in a few cases the possibility to shed its light on the risks of the collection and storage of biometric data in databases but seems to have not seized the opportunity to do so.[70] The ECJ stated in 2013 in *Schwarz* that the use and storage *on the chip* in the ePassport as required by article 4(3) of Regulation No 2252/2004 for purposes of verifying the authenticity of the document or the identity of the holder met the conditions for limitations to the fundamental right to data protection (Article 8 and 52(1) of the EU Charter).[71] The ECJ however

[68] Another example is the European Automated Fingerprint Identification System (Eurodac) as already mentioned, which is constantly evolving, and to which the European Commission now also want to add facial recognition, and to which also Frontex and Europol will have access (see EU Commission, Proposal Eurodac recast, 4.5.2016, Com(2016)272final, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016PC0272&from=EN For some recent national examples of (illegal) re-use of data collections, see in the Netherlands: Rb. Den Haag, Translink, 8.05.2017, ECLI:NL:RBDHA:2017:5165, available at https://www.recht.nl/rechtspraak/uitspraak?ecli=ECLI: NL:RBDHA:2017:5165 (appeal is pending). This case concerns the transfer by Translink, managing the registered mobility data of the OV-Chip card held by a large population in the Netherlands, to the Ministry of Education, to check possible fraud of students not living independently but claiming a subsidy.

[69] Article 29 Data Protection Working Party, Opinion 3/2005 on Implementing the 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, 30.9.2005, WP112, pp. 8-9.

[70] In two of these cases (*Schwarz* and *Willems*), individuals refused to have their biometric data recorded for obtaining an ePassport or an identity card because of lack of guarantees for re-use.

[71] ECJ, C-291/12, *Schwarz v. Bochum*, 17.10.2013 ('ECJ, Schwarz 2013'). We support this decision to the extent that Regulation No 2252/2004 indeed only mandates the local storage of biometric data under the control of the individual and for verification purposes. At the same time, precisely because of the Regulation, Member States seize the opportunity to keep, store, organize and proclaim other uses of the data as they are collected anyway. Although the Court recognized the 'risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation' (see §58), the Court limited itself by stating that the Regulation does not provide a legal basis for such centralized storage (§61).

missed its chance in *Willems,* by refusing to pronounce clearly the need for legal protection when governments are collecting and storing such data. It stated that the fore-mentioned Regulation does not require Member States to guarantee in their legislation that the data hence collected will not be stored, processed and used for other purposes.[72] At the same time, in the same decision, the Court pointed somewhat to the need of 'examination by the national courts of the compatibility of all national measures relating to the use and storage of biometric data with their national law and, if appropriate, with the European Convention on the Protection of Human Rights and Fundamental Freedoms (…)'.[73] The Court hence left much discretion to the Member States to review and decide on this important (political) issue.[74]

We contend that once biometric data are collected, the use thereof by any third party – for example LEAs - is hardly avoidable or controllable. Even the requirement for a specific law may not prevent this. This is also what the French DPA has warned for since long.[75] Unfortunately, also the GDPR missed the opportunity to tackle this issue by focusing only on a specific use and not on the collection and the establishment of biometric databases. While we support the prohibition to use biometric data for identification purposes and the explicit requirement for a DPIA in some cases, we argue that the legal protection and assessment should start right at the collection and storage of images containing unique characteristics fit for and allowing for identification or verification.

The distinction in the GDPR implies and makes that personal data such as captured images of biometric characteristics (e.g., facial images, fingerprint images, vein, etc) – although fit for and while allowing in many instances for a biometric comparison - are legally speaking no biometric data, if or as long they are not the result 'from a specific technical processing'. In other words, although capturing the image is the first step in a biometric comparison process and images relating to biometric characteristics remain a requirement for biometric comparison, and building a database the condition for identification, the legislator seems to have intended to exclude mere images, and even the building of a database with such images, from a specific biometric data protection. This is the case for public and private sector collection, as well as for the collection and use by competent authorities, such as law enforcement authorities.

The last word is not said yet. All by all, the definition makes in our opinion a very technical distinction, but with far reaching consequences.

The 'clarification' in recital 51 of the GDPR confirms that the collection and storage of photographs, for example of facial images, are not intended to be covered by the definition of biometric data and the processing thereof not considered to be biometric processing (as long as not processed through specific (biometric) technical means). This recital states that mere photographs are only covered by

[72] ECJ, C- 446/12 to C-449-12, *Willems e.a. v. Burgemeester van Nuth* e.a., 16.4.2015, p. 5 ('ECJ, Willems 2015'). The court followed herein a strict legalistic approach, while this case was an opportunity to clarify an already complex legal issue. For a critical note to this decision, see also T. Wisman, 'Willems: Giving Member States the Prints and Data Protection the Finger', Case Notes, *EDPL* 2015, pp. 245-248 and Foegle, J.-Ph., 'Sans doigt, ni loi : La CJUE donne son "feu vert" à la biosurveilance', *La Revue des droits de l'homme*, 2015, 22 p., available at https://revdh.revues.org/1394

[73] ECJ, Willems, 2015, p. 5.

[74] See also, and on the other hand, the European Court of Human Rights which came to the conclusion in *M.K. v France* that the retention of fingerprint relating to minor offences of a person suspected but not convicted, by the police and for 25 years fails to strike a fair balance between competing public and private interests, and was hence a disproportionate interference with Article 8 ECHR (right to respect for privacy): ECtHR, M.K. 2013, §§46-47. See also before its decision in *S. and Marper* 2008.

[75] See Kindt, Biometric applications 2013, p. 520 *et seq.*

the definition of biometric data if processed through a specific (biometric) technical means. Recital 51 states: '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. (…)'.

But what are these means and from which point in time are or become collected (analog or digital) photographs, for example of the face, biometric data ? And does this clarification apply to 'photographs' of all biometric characteristics ? It is in our opinion far from certain that this clarification would apply to all 'photographs', sometimes also termed as ' images' or as 'samples'[76] of biometric characteristics, such as for example an image of a fingerprint or of an iris.

Photographs, for example of children at schools, if collected and disclosed on websites of the school, or registered in an internal database of the school, are according to the new definition in the GDPR not biometric data as long as they are not processed by a biometric system. This 'clarification' certainly has as a consequence that already existing large collections of photographs but maybe also of fingerprints would not directly fall under the specific protection for biometric data, such as the requirement of making a DPIA, relying on specific legal grounds but also requiring prior consultation and even authorization. The same applies to photograph collected by governmental agencies for the issue of identity documents or travel documents: they are not to be considered biometric data as long as they are not processed by biometric means. This is problematic as the collection of the data is already made, possibly for other purposes, while this collection could serve later (unnoticed since no new collection has to be made) for (unwanted) biometric comparison, as we already mentioned. As these collections are often maintained by public authorities or agencies with a public task, this strict definition has as a consequence the keeping of such databases out of reach of specific biometric data protection, which may come in handy for these public authorities and agencies.

The same applies to the databases held by for example law enforcement authorities. This is concerning as precisely the *retention* in databases by such authorities has caused much issues, as illustrated by the court cases mentioned. Furthermore, it is interesting to note that the Directive 2016/680 does not contain a similar Recital 51. The consequences thereof should hence also be further assessed.

3 Result: At least four different categories of 'biometric data'

From the analysis above, it should become clear that data relating to the physical, physiological or behavioural characteristics of a natural person may fall in at least four different categories. In which category the data fall, will mainly be depending on the *use* that is made of such data. We summarize this *below*.

[76] A biometric sample is defined in the ISO Vocabulary as an 'analog or digital representation of biometric characteristics (…) prior to biometric feature extraction (…) ' (term 3.3.21 ISO Standard Vocabulary for biometrics 2017).

3.1 Four different categories of 'biometric data'

First, personal data relating to the physical, physiological or behavioural characteristics of a natural person are 'mere' or 'ordinary' personal data and are not considered biometric data. This is because of the strict (functional) definition of biometric data in Art. 4(14) GDPR. Hence, collecting and storing such 'ordinary' personal data, even thought it relates to (unique) human characteristics, is not subject to any specific protective biometric regime, and falls under the general privacy and GDPR data protection legislation. This requires the need for a (general) legal basis under Art. 6 GDPR for the lawfulness of the processing, general information obligations, etc. Emotional data, e.g., facial expressions (without retention of facial image characteristics) and behavioural data, if and in so far it may not be sufficiently distinctive to allow or confirm identification, would also fall in this category. But, more importantly, also personal data relating to physical, physiological or behavioural characteristics of a natural person, which allow for unique identification or confirmation of an identity, but are not used in a biometric comparison, e.g., images of a face, fall in this category and (maybe) also images of fingerprint, of iris, of vein, etc. This is hinted to by Recital 51 GDPR. These data are not to be considered biometric data.

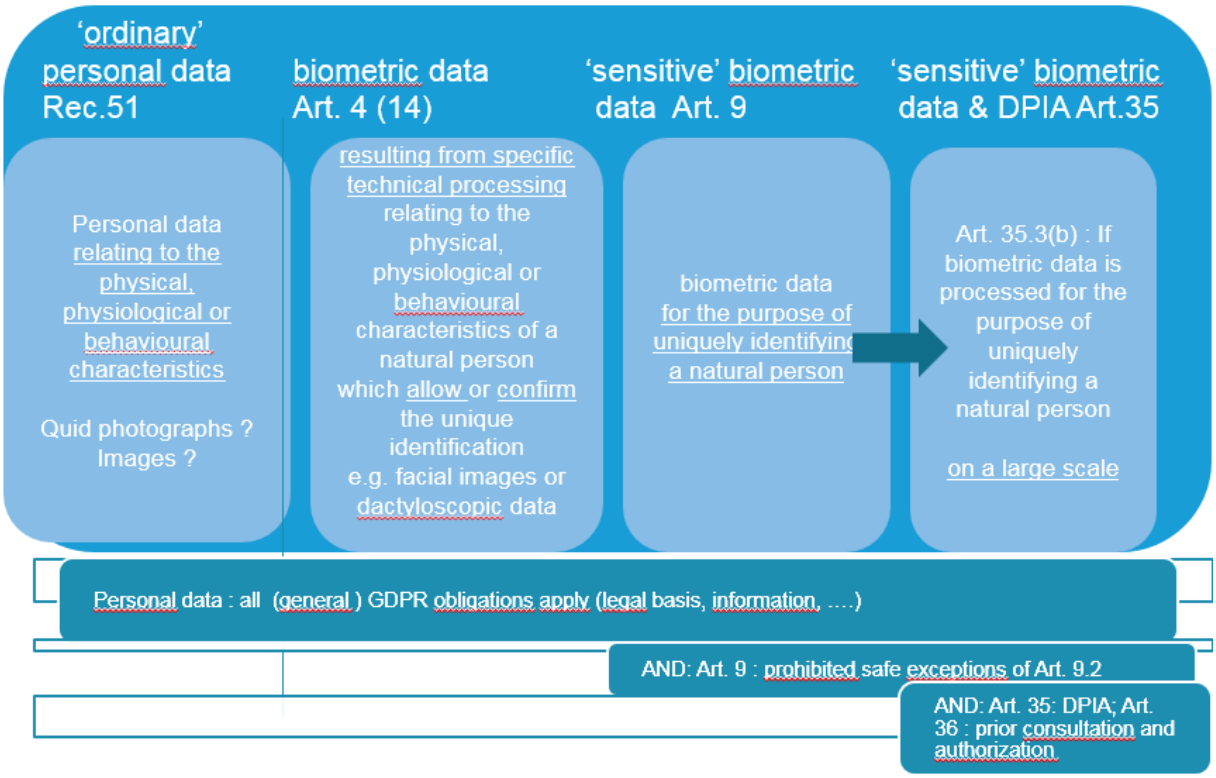
The second category contains the biometric data as defined, i.e., personal data *resulting from a specific technical processing* relating to physical, physiological or behavioural characteristics of a natural person, which allow or confirm unique identification. It is remarkable that there is no direct specific biometric legal regime applicable to this category, other than the general GDPR obligations. This category and biometric data in general is hence subject to the same legal regime as the 'ordinary' personal data.

The third category contains the biometric data processed for purposes of *uniquely identifying* a person. In this case, such use shall comply - in addition to all other data protection obligations - with Article 9 GDPR. Using biometric data in identification systems is in principle forbidden, unless exempted. This implies that if biometric data are processed by a biometric system for other purposes than identification, for example for verification, as the iPone X also claims to do, no specific biometric protective legal regime applies. Over all, verification systems, whereby only a 1:1 comparison is made based on biometric data as defined, seems at first sight to fall in the previous category 2 and to benefit from an easier regime. We substantiate *below* that this however may not be correct. We support an easier regime for the use of biometric data for verification purposes, as this poses less risks to fundamental rights. However, any use for verification should in our view be transparent to the data subjects and legislation should impose legal and technical guarantees, e.g. the data are not stored in a database. This could also include the requirement of a DPIA and setting out such guarantees in such DPIA. This is however not clear from the current legal texts.

Fourth, biometric data processed for purposes of uniquely identifying *on a large scale* fall yet in another category as they are subject to additional legal requirements. Biometric data in identification systems shall in this category comply - in addition to all other data protection obligations - with Article 9 GDPR and, in case this is on large scale, also with the Articles 35 and 36 GDPR.

The four categories of 'biometric data' and a succinct reference to the different and cumulative legal obligations are represented in the table 1 *below*.

Table 1 : 'Biometric data' in the GDPR, applicable provisions and obligations (c) E. Kindt



4 And : there is more…

4.1 Biometric data processing should always be reviewed as to whether a DPIA is required (Art. 35.1)?

Even if a DPIA would not be required based on Article 35.3(b) GDPR because (a) the biometric data is not used for identification purposes or (b) is not identification 'on a large scale', the use of biometric data, for example for verification purposes, could in our view nevertheless resort under the more general provision relating to the need for a DPIA as stated in Article 35.1 GDPR if such processing is likely to result in a high risk for the rights and freedoms. This is because biometric technology is a new technology and also because one should take the nature of the personal data used, the scope, context or purposes into account. We indicate this in table 2 with the arrow 1.

A DPIA would hence nevertheless be required although the GDPR is not explicit that for biometric data processing not qualifying under Article 9 GDPR (because it is not used for identification purposes), such a DPIA could nevertheless be required. This interpretation is in our view also suggested in the fore-mentioned Guidelines on DPIA.[77] This is in particular relevant for e.g. biometric verification systems. In other words, a DPIA may be required even if the processing of the biometric data would not fall in the third or fourth category of biometric data as explicitly mentioned in the GDPR and as

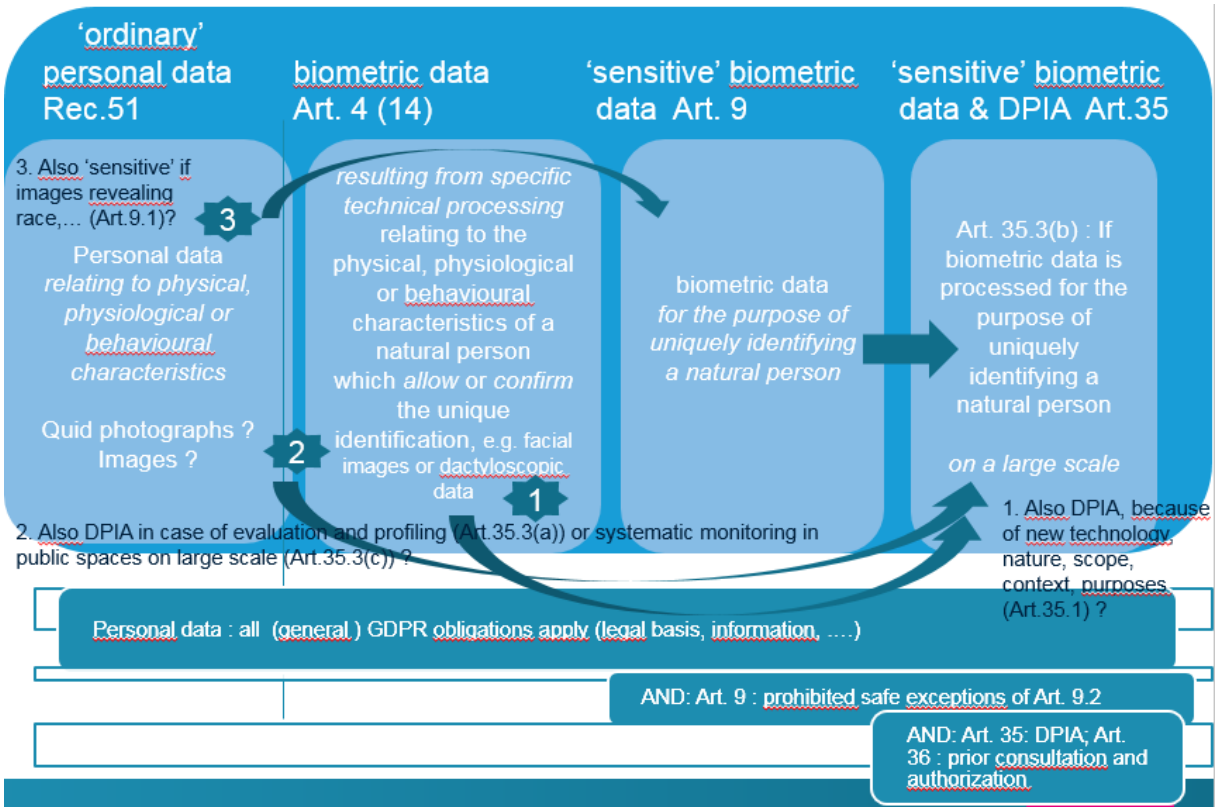
[77] See WP 29 Guidelines on DPIA (WP248), p. 9 and p. 10. The example where a DPIA is required is given therein: '8. Innovative use or applying technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, etc.' (p. 9).

we described above.[78] Moreover, and in addition, Member States may draw up lists of processing which require a DPIA (see also *below*).

4.2 Other 'biometric' data processing requiring a DPIA (Art. 35.3(a) and Art. 35.3(c)) ?

And this is not all. Even if a DPIA would not be required based on Article 35.3(b) GDPR because (a) the biometric data is not used for identification purposes or (b) is not identification 'on a large scale', one should note that Article 35.3(a) GDPR also requires a DPIA in case of 'systematic and extensive evaluation of personal aspects', based on processing, 'including profiling' and 'on which decisions are based that produce legal effects' or 'similarly significantly affect the natural person'[79]. In addition, Article 35.3(c) GDPR requires a DPIA 'in case of a *systematic monitoring* of a *publicly accessible area* on a large scale'. We indicate this in table 2 with the arrow 2.

Table 2 : Other data processing requiring a DPIA and data which could be 'sensitive' under the GDPR (c) E. Kindt



[78] An example of such processing for verification purposes likely to result in a high risk could in our view be when the biometric data used for the system, even if only used for verification, are stored in a database or in the cloud.

[79] E.g., When capturing emotions of individuals to monitor emotional status and/or to offer publicity. This provision 35.3(a) of the GDPR is further not mentioned in the Directive (EU) 2016/680, although this may be particularly relevant for LEAs in case of the use of biometric profiling. We defend that Art. 27.1 of the Directive (EU) 2016/680 could impose a DPIA in case of such use because of its general wording, even though the specific case of art. 35.3(a) GDPR is not applicable to LEAs and is not repeated in the Directive (EU) 2016/680 (see also above).

4.3. And there is still more : what about faces revealing racial or ethnic origin, sexual orientation, … ?

In addition, one could still argue that a facial image is personal data revealing racial or ethnic origin, health related information and even sexual orientation. Several (recent) national data protection legislations in the European Union refer to 'biometric data ' as sensitive and also (supreme) court decisions, e.g., in the Netherlands, have confirmed that facial images reveal racial information.[80] In this case, even though facial images as such would by the GDPR not be considered as biometric data to which a special regime applies, we argue that this does not prevent that *facial images could nevertheless fall in the special category of data*, to which the regime of Article 9 GDPR applies. We indicate this in table 2 with the arrow 3.

The GDPR however, does not clarify, confirm or rejects this interpretation of personal data relating to the physical, physiological or behavioural characteristics as being sensitive. This debate about whether some (or all) data relating to physical, physiological or behavioural characteristics of a natural person is to be considered 'sensitive' is going on already for a long time. Some defend that it is only if the data are *used* in this way and with the purpose that race or ethnic origin, etc. is used or revealed, that it is to be considered 'sensitive data'.[81] But because of the *nature itself* of the data, revealing race or ethnic origin, a medical condition, and even sexual orientation[82], effects based on for example race or ethnic origin are expected and therefore the data in our view should be treated as sensitive.[83] The GDPR has hence not solved these uncertainties. A correct legal interpretation remains hence a burden for controllers, while existing diverging interpretations in the Member States have not been cleared out in the new legal regime.

Finally, the mere storage of facial images in databases in our view contends risks because of the (future) identification potential as stated. If it is likely to result in a high risk, such DPIA would in our opinion also be required for the reasons stated. Therefore, for the reasons above, and from a practical point of view, a DPIA for biometric data processing will hence in many cases remain required, and should even for the storage of facial images be considered and reviewed. This remains a burden for the controller, while not having received more clear legal guidance on biometric data use.

[80] About these legislations and case law, see Kindt, Biometric Applications 2013, pp. 157-160.

[81] About the various interpretations in Member States as of when data are deemed sensitive, see Kindt, Biometric Applications 2013, pp. 126-139. The by some Member States defended interpretation and argument that only the *use* determines sensitivity seems to have become now also a criterion in the GDPR for when biometric data processing is considered 'sensitive'.

[82] See M. Kosinski, Y. Wang, *Deep Neural Networks are more accurate than Humans at detecting Sexual orientation from Facial Images,* 7.9.2017, available at https://www.gsb.stanford.edu/faculty-research/publications/deep-neural-networks-are-more-accurate-humans-detecting-sexual

[83] See Garvie e.a., Perpetual Line-up, 2016, pp .53-60. The report states that face recognition used by police will disproportionately affect African Americans, because of (i) trained algorithms on mug shots of more arrested African Americans and (ii) less accurate error rates for this group of people. Such effects should at least be recognized and neutralized.

5 Further conditions by national legislation

5.1 Further conditions by Member States for some special categories of data, including biometric data

Article 9.4 GDPR states that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data (sic) or data concerning health. This implies that it is likely that the processing of biometric data will be further regulated on national level. This was already the case before the GDPR. For example, the French Act of 1978, as modified, requires explicitly prior authorization by the National Data Protection Authority of biometric data processing and use which are 'necessary for identity control'.[84] It remains to be seen whether and to what extent the French Act and legislation will be modified or maintain its previous regime. The same question as to whether and how other national legislations will be adapted is valid in other countries.[85] National legislation regulating biometric data processing seems now continued by the GDPR. The aim of harmonization under the GDPR is therefore far from reached.

One shall note that this provision allowing for national regulation no longer makes a reference to the need for unique identification by the biometric data. The question hence raises whether it allows the national legislator for deviating and for a more strict national regulation for all biometric data (as defined or more broadly) and hence for more than only the biometric data considered sensitive ? As Article 9.4 GDPR is part of the regulation for special categories of personal data, one could argue that such national conditions could only relate to the use of biometric data for uniquely identifying persons. However, this remains unclear. National regulations for biometric data processing remain nevertheless likely.[86]

Because the Directive (EU) 2016/680 also states that profiling by competent authorities is in principle forbidden, unless authorized by law, such national laws for the use of biometric data for this purpose are also awaited.

5.2 Explicit consent for processing biometric data for the purpose of uniquely identifying may be restricted by Union or Member State Law

The exemption by explicit consent for processing biometric data for the purpose of uniquely identifying may be restricted by Union or Member State Law as well.

One could think here of more specific guidelines and regulations for the use of biometric data of employees in a labor context. While such data are in many cases increasingly used to secure applications or places, biometric verification, whereby the biometric data are locally stored, enabling

[84] Compliance with a so-called 'Unique Authorisation' for specific defined data processing activities is another possibility. See Art. 25, I 8° and II Act of 6 January 1978, as modified in 2004, available at https://www.cnil.fr/sites/default/files/typo/document/CNIL-78-17_definitive-annotee.pdf About the specific authorization regime in France for biometric data, see Kindt, Biometric Applications 2013, pp. 517-548, and also the very interesting analysis of the decisions of the CNIL in the period of 2004-2014 in C. Gayrel, 'The principle of proportionality applied to biometrics in France: Review of ten years of CNIL's deliberations', *CLSR* 2016, pp.450-461. Some new Unique Authorisations ('UA') have been adopted in the meantime, while some previous UAs were abolished.

[85] Other countries, such as the United Kingdom, Slovenia, the Slovak Republic, … also contain specific provisions on biometric data. These provisions will have to be reviewed for compatibility with the GDPR and the Directive 2016/680.

[86] Poland, for example, contains in its draft Act implementing the GDPR for various sectors a provision allowing employers to collect and process biometric data with the consent of their employees.

the employees to keep control over their data, is preferred from a privacy and data protection point of view. National law could specify this type of use as well as the required safeguards, while also stating that the prohibition of art. 9.1 GDPR may not be lifted by the explicit consent of the employee, even if there would be a choice for the employee.

Another example is whether national law could restrict private or public entities requesting explicit consent with biometric identification, such as shopping malls, clubs, swimming pools etc to identify and repel no longer desired visitors or customers.

5.3 National list of processing operations requiring DPIA

A third relevant area in which Union or national law may be specific and deviate from the uniform provisions of the GDPR, relates to the DPIA. Supervisory authorities may make lists of kinds of processing operations which need a DPIA or which do *not* require a DPIA.[87] Only in case the processing would relate to the offering of goods or services to data subjects in several Member States, or in case of the monitoring of the behavior of such data subjects, the consistency mechanism outlined in the GDPR will play in order to come to a harmonized view and even dispute resolution in case of diverging opinions in the Member States.[88]

Conclusion

This article describes how the new legal framework allows for the collection of biometric images under generally applicable provisions, including the storage in databases, and only regulates the specific use of such data.

Based on the definition of biometric data and distinctions made in the GDPR, we find that there are four different categories of personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow identity verification or identification. To each of these categories, different regimes apply, which we have explained in this article (see also Table 1). One shall also retain that personal data relating to physical, physiological or behavioural characteristics are *in se* by definition not automatically also biometric data under the GDPR. There should be a relation with and a result of a 'specific technical processing' and the data shall allow or confirm 'unique' identification. At the same time, and as mentioned, the collecting and storing of for example facial images does not fall under any enhanced specific biometric data protection regime.

According to the GDPR, the use of biometric data for identification is in principle prohibited (Art. 9.1). Article 9.2 GDPR however contains many exceptions to the prohibition of biometric data use for identification, including the explicit consent. We believe that Member States should discuss and take up their responsibility in limiting the use of consent for biometric identification, because of risks of exclusion, discrimination, undue process and other fundamental rights which cannot be limited by individual consent.

[87] Art. 35.4 and Art. 35.5 GDPR. The Belgian DPA, e.g., has issued a draft document CO-AR-2016-004 on PIA for a public consultation closed by 28.2.2017. In the Annex, it requires a PIA for the use of biometric technology for identification, without however stating that this should be on a large scale. See also *above*.
[88] Art. 35.6 GDPR and Art. 63 *et seq.* GDPR.

Controllers are left with an important responsibility under Article 35 GDPR to assess the impact of the biometric technology, and, if no sufficient safeguards are implemented, to discuss same with the DPA and even request prior authorization. Besides a mentioning of the need for such DPIA for the use of biometric data for uniquely identifying on a large scale in Article 35.2(b) , the more general provision of Article 35.1, and the other provisions of Article 35.2 requiring a DPIA may apply as well for particular biometric applications. The controller is hence confronted with a patchwork of complex regulation for biometric data use, while some issues are not fully solved. Such complex legal framework may hamper innovation.

This is at first sight not so much different from the regime under the Directive 95/46 and implemented national laws. As biometric data use can add convenience to less threatening applications in many scenarios, in particular if used for verification, legal protection could have been granted by tempering or even forbidding the storage in databases, and to encourage storage only on a secured object that remains under the control of the individual.

For law enforcement authorities, further national law is awaited implementing Directive 2016/680 which does not prohibit *per se* the use of biometric data for identification purposes. As mentioned, such national law shall meet the needs for and criteria of proportionate and strict necessary use of biometric data in a democratic society. This is certainly required for the retention and storage of such data, as the European Court of Fundamental Rights has already pointed to in several cases. More specific guidance for the use of biometric data in the Directive (EU) 2016/680 albeit based on case law would also have been useful for competent authorities.

To conclude, although we support the prohibition in the GDPR because identification contains major risks for fundamental rights and freedoms, whether by private actors or for law enforcement purposes, we regret that only the *use* of personal data relating to the physical, physiological or behavioural characteristics is tackled (subjective or use based approach) and not the collection and retention of such data in a *database* (the objective approach). It is precisely the collection of the data, which is somewhat apparent to the individual, and the storage in biometric databases that are the first step and allow for (hidden) identification. European case law has at several occasions pointed to the risks and interference with fundamental rights of the *retention* of such data in databases. If the European legislator aims to provide legal protection for 'biometric data', this should not start with the use, but as of the collection and storage of biometric data in databases which shall be specifically regulated.

This article has been made possible partly by received funding from the European Union's Horizon 2020 research and innovation programme in the context of the VICTORIA project under grant agreement no SEC-740754 and the VALCRI project under grant agreement no FP7-IP-608142. The author also thanks Damian Clifford of Citip and the anonymous reviewers for their reading and valuable comments. The viewpoints in this article are entirely those of the author and shall not be associated with any of the fore-mentioned projects, persons or entities. The author nor the Commission may be held responsible for any use that may be made of the information herein contained.