DuD
Datenschutz und Datensicherheit

Biometric applications and the data protection legislation

The legal review and the proportionality test

Els Kindt

In the attempt to harmonise the application of European data protection legislation to biometric systems, the Art. 29 Data Protection Working Party adopted a working paper on biometrics. In this article, the risks mentioned in the working paper are summarised and some decisions of European Data Protection Authorities with respect to the implementation of biometrics are discussed. The author finds that especially the application of the proportionality principle still leads to contradictory decisions.

Mr. Els Kindt
LL.M

Legal researcher
Centre for Law and ICT, Catholic University of Leuven (Belgium)
www.icri.be

Her research focuses on the legal aspects of the processing of biometric data
els.kindt@law.kuleuven.be

Introduction

The emergence of the deployment of biometric technologies in the private sector requires a legal analysis as to the compatibility of these new techniques with the existing legal framework. The present contribution sets out some issues from the angle of data protection, with some references to human rights protection. The starting point is the opinion of the Working Party established by Article 29 of the Directive 95/46/EC on biometrics of 1 August 2003 (hereinafter 'opinion WP 80').[1] Since this opinion, however, there remain uncertainties as to the purposes and the criteria which make biometric data processing lawful and legitimate. This leads to sometimes contradictory positions of national data protection authorities on similar biometric implementations.

This contribution reminds of the important differences between the biometric functionalities and pleads for a consistent use of vocabulary in biometric matters. It continues with referring to some of the specific risks of biometrics which were mentioned in opinion WP 80 and points to some interpretation difficulties. It touches also upon some additional risks of the use of biometrics. The contribution concludes with describing briefly the purpose and proportionality principle, which is a leading principle in almost all decisions on the processing of biometric data, and the difficulties in applying this principle.

[1] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document on biometrics*, 1 August 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/ 2003/wp80_en.pdf.

1 The risks of biometric data processing

1.1 Verification v Identification

One shall recall that the use of biometric technologies imply that (in most instances) unique biological and/or behavioural characteristics of a person are collected and stored for the verification of a claim made by that person or the automated identification of that person. This description mentions the two main functionalities of biometrics which are very different not only in purpose, but also in the way these functions are effectuated : (1) the verification function which is a one to one comparison and which allows to check a claim made by a person (for example, 'I am holding the employee card which is issued to me and I am entitled to enter these premises') and (2) the identification function which is a one to many comparison and which allows to tell if the biometric characteristic is in the central database (to avoid double-dipping, e.g., of asylum seekers who have already applied in another country), or, if names are mentioned in that database, to tell to whom that biometric characteristic belongs.

It is essential to distinguish these two functionalities of biometrics from each other in the debate about possible risks. The verification function is mostly used to strengthen an authentication process, by something you 'are', in addition to something you 'have' and you 'know'. The verification function also permits that the biometric characteristic is stored locally, under the control of the individual. The risk that the biometric data are used to identify that

individual or are used for other purposes ('function creep', i.e. the risk that the data are used for secondary purposes which are not compatible with the purposes for which the data were initially collected) remains limited as compared to the use of biometric characteristics in the identification function, upon the condition that the biometric system is implemented appropriately. It is in our view the identification function of biometric data that poses the most concerns and that causes most risks (such as tracing or surveillance or identity theft) because the biometric data are no longer under the (physical) control of the person concerned. These concerns have become more real as several governments are starting up large scale central databases for passports and eID cards with mandatory biometric characteristics (e.g., the United Kingdom). These large scale database with the names and addresses of citizens (and often a lot more information) which will be linked with the biometric characteristics of a given person will allow governments but also the private parties which have access thereto to identify persons by simply submitting one of the registered biometric characteristics. Overall, the use of the identification function by private entities should be scrutinized. The question should be raised to what extent such private organisations have the right to control the identity of individuals.

A correct use of the biometric terminology is important for the debate. In Working Group 1 of Subcommittee 37 of the Joint Technical Committee 1 of the International Standardisation Organisation, work is being done on the harmonization of the terms that parties, whether users or developers, use in the field of biometrics.[2] The development of a vocabulary and common definitions for biometric systems is extremely important but also difficult because of the diverging understanding of common terms. For example, in the current draft document, it is stated that certain terminology is depreciated, in particular the terms 'positive identification' and 'authentication'.[3] 'Positive identification' refers in principle not to a one to many comparison, but to a one to one verification. 'Authentication' could refer to both.

1.2 The opinion of the Article 29 WP

Since the opinion of the Article 29 Data Protection Working Party on biometrics of 1 August 2003, an analysis of the privacy and data protection problems of biometrics will in principle refer to the issues that were identified in that document. The opinion came after substantial work was already done in the BioVision project (IST-2001-38236, which started in 2001 and ended mid 2003).[4] The issues which were put forward in opinion WP 80 remain valid as a starting point for further discussions of the legal aspects of biometrics.[5] In this contribution, we will not discuss this opinion at length. This is already done in other work, such as in the Fidis project.[6] Nevertheless, for a proper understanding, the main concerns stated by the Working Party in opinion WP 80 are at the end of this contribution represented again, in a brief schematic overview (see figure 1).

Two elements of the fore-mentioned opinion have our attention. The opinion WP 80 focuses primarily on biometric applications for verification purposes. The opinion WP 80 expressly states so.[7] The reason why the Working Party concentrates on verification, could probably be explained by the fact that back in 2003, the biometric techniques for identification were not yet fully developed; the working party refers to the size of the database and the type of biometrics as factors which at that time were still determining factors in rendering the identification function possible.[8] In the meantime, the techniques have further developed, and one should no longer doubt that the identification capabilities of biometrics have improved, at least to such extent that some governments believe that it is useful and possible to establish central national registers which contain in a central database biometric characteristics for identification purposes.[9] Another reason could be that the Working Party believes that the role of biometrics for the biometric systems industry should remain in principle limited to its deployment for verification purposes. The Working Party is not clear in that respect. In the discussion about the principle of purpose and proportionality, the Working Party discusses the example of the use of biometrics for access control purposes and hereby refers to the verification function.[10] On the other hand, the Working Party seems to describe in its opinion the risks of biometric data in general, whether used for identification or verification purposes, such as the sensitive information contained in biometric data, secret capture, the FAR and FRR and theft, which are risks for biometric data used for identification or verification. Other risks described, such as surveillance, incompatible re-use, the use as unique identifier and identification are dangers which in principle would only apply if the biometric data are used in a centralised way.

The position of the Working Party on whether biometrics should only be used by the industry for verification is not explicit and remains unclear. It would therefore be welcomed if the Working Party could clarify its position in that respect. The goal of the opinion WP 80 was to contribute to the effective and homogenous application of the data protection legislation upon biometric systems. Since the opinion is used by the national data protection authorities (hereinafter the 'DPAs') as containing guidelines for further interpretation of the data protection legislation, such clarification is desir-

[2] See JOINT TECHNICAL COMMITTEE ISO/IEC JTC 1, SUBCOMMITTEE SC 37, Technical Text of Standing Document 2, version 5 – Harmonized Biometric Vocabulary, 31 January 2006, a working document, available at http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-1480.pdf?nodeid=4954581& vernum=0 (hereinafter 'Draft Harmonized Biometric Vocabulary v. 2.5').

[3] See Draft Harmonized Biometric Vocabulary v. 2.5, at 16.

[4] See for this discussion in particular the three BioVision documents which are mentioned in the Literature list.

[5] Other interesting studies have been published in the meantime, some of which mentioned in the Literature list. For Germany, see also T. WEICHERT, „Staatliche Identifizierung durch Biometrie", *Datenschutz Nachrichten* 2004, vol. 2, (9) which gives a useful overview of German legal provisions relevant to the use of biometrics by the State.

[6] Fidis (Future of Identity in the Information Society) is a network of excellence (NoE) funded by the European Commission's Sixth Framework Program. See in particular M. GASSON, M. MEINTS, e.a. (eds.), *Fidis deliverable D.3.2.: A study on PKI and biometrics*, Fidis. Future of identity in the Information Society, 4 July 2005, 101-105, available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf.

[7] See *above*, footnote 1, at 3.

[8] See *above*, footnote 1, at 2 and the there mentioned footnote 3.

[9] See, for example, the United Kingdom, where the National Identity Register, that will be established under the Identity Cards Act 2006, will contain biometric data in a central database.

[10] See *above*, footnote 1, at 6.

able in view of the objectives of the Working Party.

The other element in the opinion that catches our attention is the reference to the proportionality. In opinion WP 80, the Working Party stated that the principle of purpose and proportionality is a decisive factor in the legal review of biometric systems by the DPAs. There is, however, legal uncertainty on how the purpose and proportionality principle must be applied to the processing of personal data in general and of biometric data in particular. This issue will be further discussed in section 2 below.

1.3 Other risks of the use of biometric data

Since the opinion WP 80 of 2003, there are some additional concerns which have been expressed or which should be taken care of. Because biometric technologies are evolving very fast, the Article 29 Data Protection Working Party has said that its opinion was only a 'working document' which it intended to revisit in the light of the experiences of data protection authorities and technological developments linked to biometric applications.[11]

One of the basic principles of the data protection legislation set forth in the Directive 95/46/EC relates to the data quality. The principle requires that the personal data must be '*accurate*, and, where necessary, *kept up to date*'; furthermore, 'every reasonable step must be taken to ensure that *data which are inaccurate* or incomplete, having regard to the purposes for which they were collected or for which they are further processed, *are erased or rectified*' (emphasis added).[12] This requirement with regard to the data quality poses a problem for specific forms of biometric data which relate to a human characteristic that changes over time, for example, if the individual grows older. The reference biometric data relating to hand geometry or face of younger persons, for example pupils of a school, may at a certain point not be of any good quality anymore, as the characteristics change and these changes are not reflected in the reference data. This problem has been recognized in relation with the use of the facial image of children for the use of identity documents in a study performed for the Ministry of the Interior in the Netherlands in 2005. The report stated that 'it is very likely that facial recognition of children of twelve years or younger, on the basis of a reference image that is some years old, is problematic. The reason is the significant changes in the proportions of the characteristic points in the face during growth. These changes take place after a complex process that is to a large extent determined by the sex and genetic background'. Furthermore, the report stated that the problem also exists for children older then twelve, and that additional research on this topic is needed. The data quality of the reference biometric data of young persons is therefore a concern, not only from a practical point of view, but also under the data protection legislation, which imposes requirements for the quality of the data, in particular that the data shall be accurate. Inaccurate data would lead to increased FAR and FRR and would render the whole biometric application unreliable. FAR and FRR also pose risks for the data subjects, by either having somebody else in your place identified for the service or by being wrongly rejected. This concern is especially relevant since biometric applications are now often promoted in schools or other environments involving children, for convenience and other purposes (for example the administration of meals).[13]

As described above, the personal data processed should be accurate. A fundamental element of biometric systems is the matching decision. Because of the inherent statistical nature of a biometric system, a decision of a biometric system merely gives a degree of correlation between the submitted biometric samples and the reference biometric data. Each type of biometric system has FRR and FAR to a higher or lower degree. It is the system designer or the operator (owner) who will set the acceptance threshold and error rate, often decided and adapted to the requirements of a specific application. In a low security application, e.g., the registration of meals of pupils, one could decide to reduce the FRR, which will have as effect an increased FAR. This trade off and the fact that the match is never a complete match (but only a probability) imply that the decisions that biometric systems make about an individual and the data relating thereto are never for 100 % correct or sure. One could question if this is in conformity with the requirements of the Directive that the data relating to individuals shall be accurate. Biometric systems fail per definition to fulfil this requirement. Individuals may always be subject to false decisions which affect them.

If biometrics are used by a private owner for access control purposes, e.g., to a place open to the public such as a dancing or soccer stadium, the public interest (securing (public) order) is often invoked, or the interests of the controller, outweighing the interests of the individuals.[14] The Directive 95/46/EC states that especially if the processing is based on these grounds, the data subjects should have the right to '*object at any time on compelling legitimate grounds relating to his particular situation'* to the processing, unless the national legislation states otherwise.[15] Legitimate grounds could be the contention that biometric data include sensitive data (see also *below*), difficulties to enrol, or also religious belief. The principle of the right of individuals to object to the processing of data is relevant in discussions about biometrics. Biometric systems will therefore probably never include all individuals to whom it might be directed (e.g., controlling access of passengers to specific zones in airports).

Other risks are indicated by further research stating that in almost all biometric raw data considerable additional information is included, in particular about health. Although one would expect that in case templates are used such additional information is considerably reduced, additional systematic research with respect to remaining additional information in templates is required in order to verify such assertion.[16]

The last issue that we would like to mention here is that additional research has proved that spoofing of biometric systems for misappropriation of biometric data is a realistic security threat. The consequences hereof can be very severe, because biometric characteristics can in principle not be

[11] See *above*, footnote 1, at 11.

[12] Article 6.1 (d) of the Directive 95/46/EC.

[13] See, for example, about the debate about the use of biometrics in schools in the United Kingdom, W. GROSSMAN, 'Is School fingerprinting out of bounds?', *Guardian*, 30 March 2006, available at http://technology.guardian.co.uk/weekly/story/0,,1742091,00.html.

[14] See Article 7 (e) and (f) of Directive 95/46/EC.

[15] Article 14 (a) of Directive 95/46/EC.

[16] For a quite comprehensive overview of health information that can be discovered in raw data, see KINDT, E. and MULLER, L. (eds.), *D.3.10. Biometrics in identity management*, Fidis, 2007 (in preparation).

changed, unless biometrics are used in a revocable way.[17]

2 The purpose and proportionality test

Biometric applications can not only be used in two different operating modes (identification v. verification), but also for a variety of purposes. As stated in section 1.2, the Working Party stated that the purpose and proportionality principle is a leading principle in the review of biometric systems. The Article 29 Data Protection Working Party hereby referred to Article 6 of the Directive 95/46/EC that requires that '(…) *personal data must be (a) processed fairly and lawfully, (b) collected for specified, explicit and legitimate purposes* (…)' *and that the data shall be 'adequate, relevant and not excessive* (..)'. The Working Party, however, gives little guidance in its opinion WP 80 on how the purpose and proportionality principle must be applied to biometrics. The general notion 'fairly' is undefined and broad. It could include that the data processing shall not intrude unreasonably upon the individual's privacy, autonomy and integrity[18] and shall be transparent.[19] 'Lawfully' is a notion that includes that the processing shall not be against the data protection legislation or any other legislation or legal principle. Under what conditions biometric data processing is 'lawful and fair', however, is not defined or stated in a coherent manner. It is even more difficult to know when the processing is proportionate with the risks. The Working Party discussed in its opinion the use of biometric data for access control purposes, and stated in this context that the way biometric data could be stored, i.e., in a central way or on an object exclusively under the control of the data subject, will determine to what extent the fundamental rights of individuals are at risk. The central storage of biometric data poses more risks, in particular for 'function creep' and the linking of information in several databases. At the same time, the Working Party seems to state that such central storage could be permitted for high security installations, provided it was checked before with the national DPAs. Other criteria which may be relevant to determine the proportionality are being touched upon, such as the kind of biometric (e.g., the outline of a hand as opposed to fingerprint), the fact that the data could be left unintentionally (e.g., fingerprint) and the way biometric data are digitalized. The criteria for deciding in a coherent manner upon the proportionality of the use of biometrics, however, remain unclear. These criteria are also not stated in the 95/46/EC Directive.

The DPAs confirm in their decisions the importance of the principles of purpose and proportionality as primary principles.[20] The DPAs and the courts review whether the use of biometric identification techniques is lawful and in proportion with the purposes of the application based upon Article 6 of the Directive 95/46/EC. The criteria that are used by the DPAs, however, vary. The DPAs do also not apply the requirements developed in their decisions in a uniform manner. Even more, the different national DPAs come to contradictory decisions or positions for similar biometric systems. An example is the use of biometrics for air travel : on 5 November 2003, the DPA of the Hellenic Republic renders a negative decision on the use of iris and fingerprint on a smart card for air passengers, while the 'Privium' programme, using iris on card for frequent travelers, is operational at the Schiphol airport in the Netherlands for about five years now. [21]

The proportionality principle seems to surface again in the balancing of interest test of Article 7 (f) of the Directive 95/46/EC which mentions in a limitative way the legitimate grounds on which a data processing is permitted. The last mentioned ground for processing personal data is if 'processing is *necessary* for the purposes of the *legitimate interests* pursued by the controller (…), *except where* such interests are *overridden* by the *interests for fundamental rights and freedoms* of the data subject which require protection under Article 1 (1)' (emphasis added). Article 1 (1) to which this provision refers, imposes an obligation upon the Member States to protect the fundamental rights and freedoms in relation with the processing of personal data, in particular the right to privacy. In the balancing of rights test, that finds its origin in common law systems, the proportionality requirement is emerging again. The proportionality principle in this context refers to a general principle of law that requires a fair balance and reasonable relationship between the means requested or used, including the severity and the duration of the means, and the objective sought. The principle has its origin in public law, where it protects individuals against state interference; in the context of the enforcement of fundamental human rights, and further to case law related therewith, interference with such rights is not permitted if it is not 'prescribed by law', for 'legitimate purposes' and to the extent that the interference is 'relevant' or 'necessary' and not 'excessive'. This proportionality principle seems now to be also used to decide upon interest of private parties which are in conflict.[22] The criteria for the application of the principle, already much debated in human rights cases in general, become also the focus of attention in the context of biometric data processing.

The proportionality principle is also related with the margin of appreciation doctrine. The risk is that to the extent that there is no clear answer as to which criteria need to be taken into account for determining whether a biometric processing is fair and proportionate, and which interest outbal-

[17] See also *above,* footnote16.

[18] See BYGRAVE, L. A., *Data Protection Law. Approaching its rationale, logic and limits*, in B. HUGENHOLTZ en e.a. (eds.), *Information Law Series*, The Hague, Kluwer Law International, 2002, 58.

[19] See also recital 38 of the 95/46/EC Directive which links the notion of fairness with transparency and information.

[20] The French DPA (CNIL) stated it as follows: '*C'est au regard de l'ensemble de ces considerations qu'il y a lieu pour la Commission d'apprécier, dans chaque cas, si le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données sont, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données ainsi constituées, adaptés et proportionnés à la finalité assignée au dispositif'* (Opinion N° 04-018 of 8 April 2004 of the CNIL on the request for an opinion by the Hospital of Hyères relating to the employment of a fingerprint verification application for the management of the employees' time and attendance (negative)).

[21] Another example is the opinion of 19 March 2001 of the Dutch DPA ('*Registratiekamer'*) relating to a biometric access system for visitors of catering and sports infrastructures, named VIS 2000, in which the DPA is willing to accept the use of such system, provided the controller implements its nine recommendations for the processing of the (biometric) data. The Belgian DPA ('*Commissie voor de Bescherming van de Persoonlijke Levenssfeer'*), however, mentioned in its annual report for 2005 that it rendered a negative opinion on a similar biometric access system. See also *above*, footnote 1, at 7, footnote 19.

[22] See, for example, Article 7 (f) of the Directive 95/46/EC, which also applies if the controller is a non-public entity.

ances the other, the margin of appreciation of the DPAs and the courts will further increase and the level of protection of the fundamental rights at risk will be different. The objective of the Working Party, however, was to limit diverging interpretations.

Further research is therefore necessary as to when the processing of biometric data is fair and lawful and to what extent the criteria touched upon by the Article 29 Data Protection Working Party and other criteria (such as the accuracy of the biometrics data) are able to determine whether the processing of biometric data is proportionate to the (legitimate) aim. This research may indicate that there are flaws in the present regulation of biometric data and that additional initiatives need to be taken in that respect.

3 Conclusion

This contribution recalled some risks which biometric data processing involves. In this debate, it is highly recommended to use a consistent vocabulary and the current work of the ISO JTC 1 SC 37 is for this reason of high relevance. Attention is also requested for the important purpose and proportionality principle which leads to sometimes contradictory decisions by the national DPAs in their legal review. The application of this principle may show the flaws in the present regulation of biometric data and indicate which initiatives need to be taken in that respect. Further research is therefore necessary with respect to the proportionality principle in combination with the way biometrics are implemented.

Privacy Risk	Storage	Qualifying factors	Data Protection principle	Suggested remedy in WP 80 to counter risk
Identification	Central storage	Size of database Type of biometrics used	Proportionality Art. 7	
Biometrics contain sensitive information (health, race)	Central (or local) storage		Prohibition to process sensitive data Art 8 Data minimisation Art. 7	No images Use of templates which exclude such information
Secret capture and/or surveillance	Central storage	Especially vulnerable are low-level intrusiveness biometrics (e.g., face, voice), but also fingerprint, …	Fair collection and processing Art. 6 (a)	Local storage under control of data subject
Incompatible re-use ('function creep')	Central storage		Special risks to rights and freedoms Art. 20	Prior checking with DPA
Theft	Central (or local) storage		Appropriate technical and organisational security measures Art. 17	Appropriate security measures Including impossibility to reconstruct image from template
Use as unique identifier for connecting databases	Central storage	Use by governments	Conditions to be determined Art. 8 § 7 Right to object Art. 14 (a)	Mathematical manipulations
FAR/FRR	Central or local storage	Type of biometrics used	Prohibition of automated decisions Art. 15	Re affirmation of outcome

Figure. 1: Overview of important risks as set out in opinion WP 80 Source : Fidis deliverable D.3.10 (in preparation)

Literature

ALBRECHT, A., *BioVision. Privacy Best Practices in Deployment of Biometric Systems*, BioVision, 28 August 2003, 49 p.

ALBRECHT, A. and WALSH, M. (eds.), *BioVision. Report on legal and privacy issues*, BioVision, 28 August 2003, 26 p.

ARTICLE 29 DATA PROTECTION WORKING PARTY , *Working document on biometrics*, 1 August 2003, 11 p.

CAVOUKIAN, A., Information and Privacy Commissioner, Ontario, September 1999, 62 p.

COUNCIL OF EUROPE, *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, February 2005, 26 p.

EUROPEAN BIOMETRICS PORTAL, *Biometrics in Europe. Trend Report*, 2006, 113 p.

EUROPEAN BIOMETRICS PORTAL, *Biometrics in Europe. Trend Report*, 2007, 39 p.

GASSON, M., MEINTS, M. e.a., (eds.), *Fidis deliverable D.3.2. : A study on PKI and biometrics*, Fidis. Future of identity in the Information Society, 4 July 2005, 138 p.

MAGHIROS, I. e.a. *Biometrics at the Frontiers : Assessing the Impact on Society*, in EUROPEAN COMMISSION, JOINT RESEARCH CENTRE and INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (eds.), *Technical Report Series*, 1 June 2005, 166 p.

MEINTS, M. and HANSEN, M. (eds.), *D3.6. Study on ID Documents*, Fidis, 2006, 160 p.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Biometric-based Technologies*, 28 April 2004, 66 p.

REJMAN-GREENE, M. (ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 October 2003, 202 p.

WEICHERT, T., „Staatliche Identifizierung durch Biometrie", *Datenschutz Nachrichten* 2004, vol.. 2, 9-19.