EU data protection legislation and case-law with regard to biometric applications

Ioannis Iglezakis
Assistant Professor
Faculty of Law, Aristotle University of Thessaloniki

Abstract

Biometric applications are increasingly used to provide enhanced security in verification and identification procedures. However, privacy concerns are raised from the processing of biometric features, which are deemed as personal data and in certain circumstances, as sensitive personal data. Their processing may infringe the privacy of the individual, as it provides more potential for control of the individual. Data Protection Authorities in the EU Member States have issued various decisions, prohibiting biometric applications in some occasions. Their decisions, however, lack consistency and are contradictory. Therefore, it should be examined if the legal review of biometric applications should be based on the application of existing legislation on data protection and particularly of the proportionality principle, or whether specific legal provisions should be introduced. It is stressed out that discrimination exists as regards biometric applications in the private sector and those in the public sector, since biometry has been introduced in passports and plans exist to introduce them also in identity cards. The processing of biometric data is regulated in some EU Member States data protection acts, which provide for the principles of proportionality and/or prior notification to the supervisory authority, while other laws define biometric data as sensitive data and thus, grant enhanced protection to data subjects.

Keywords: Biometry, biometric applications, authentication, verification, proportionality, data protection

Introduction

The privacy implications of biometric applications employed in the private sector have been examined in the recent years by EU Member States' Data Protection Authorities (DPAs) in many occasions[1]. The progress in the development of biometric technologies and their application for authentication/verification or identification required the intervention of supervisory authorities, taken into account the privacy concerns raised by biometric technology, which could compromise informational privacy[2].

The decisions taken by DPAs, however, seem to be ambiguous and lack consistency. In particular, there is no consensus which criteria make biometric data processing lawful and there are different interpretations on the application of the proportionality principle to biometrics. The Data Protection Working Party established by Article 29 of Directive

[1] It is notable that biometric applications and genetic technologies have in common that the object of processing are unique physiological characteristics of the individual; hence, such processing allows an intensive control of the individual, in case anonymization techniques are not used.

[2] In our modern information society, informational privacy is not conceived as the right to be let alone (Warren/Brandeis); it rather encompasses the claim for exercising control over one's own information (Westin, 1967).

95/46/EEC[3] delivered an opinion on biometrics on 1 August 2003 (WP 80, 2003), which did not had as an effect the harmonization of application of the EU data protection legislation to biometric systems (Liu, 2009, p. 327-238).

On the other hand, we are experiencing a proliferation of biometric systems in the public sector. Many states around the world, in order to combat identity fraud, included biometric data in passports, while other countries plan or have introduced biometric data (mainly fingerprints) in identity cards (Grijpink, 2006, p. 317). Currently, there is a burning debate about the implementation of biometrics in passports and ID cards due to problems of constitutional and data protection law, which are raised by it (Hornung, 2004; 2007).

These problems highlight the absence of clear rules on specific issues in the General Framework Data Protection Directive[4], but also the intricacy of the issues raised by modern technology with regard to data protection. Thus, the privacy issues raised must be addressed with adequate legislative and technical safeguards.

Description of biometric applications

Biometric systems are applications of biometric technologies that consist in the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity (Liu, 2009).[5] Such applications are employed for various tasks, in different areas and in the public as well as in the private sector.

Biometric features that are used for verification or identification have common characteristics. They are: a) universal, as they exist in all persons, b) unique, for they are distinctive to each person and c) permanent, since the property of the biometric feature remains permanent over time for every individual) (DPWP 2003, p. 3). Other properties of biometrics features are the following: a) collectibility: the biometric characteristic should be quantitatively measurable and easy to collect, b) performance: accuracy, speed and resource requirements should be satisfied, c) acceptability: indicates the extent to which a system is harmless and accepted by the intended users and d) circumvention: refers to the robustness of a system against fraudulent methods and attacks (Zorkadis and Donos, 2004, p. 127).

There are two main categories of biometric techniques, i.e. a) physical and physiological-based techniques which measure the physiological characteristics of a person and include fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, voice recognition, etc. and b) behavioral-based techniques, which measure the behavior of a person and include hand-written signature verification, keystroke analysis, gait

[3] OJ L 281 of 23/11/1995, p. 31.

[4] For an assessment of the EU Directive see, e.g., Robinson et al., 2009. In this study, it is pointed out that the Directive serves as a reference model for good practice and harmonizes data protection principles, which permit flexibility, while being technology neutral, but is characterized by weaknesses, such as that the link between the concept of personal data and real privacy risks is unclear, etc.

[5] Liu underlies that the term 'biometrics' is used to describe two different aspects of the technology, i.e. biometrics as characteristics, referring to measurable biological or behavioural aspects of the person that can be used for automated recognition and biometrics as process, referring to automated methods of recognizing an individual based on measurable biological and behavioural characteristics (Liu, 2009, p. 237).

analysis, etc. Yet, biometric systems exist that combine different biometric modalities of the use with other identification or authentication technologies.[6]

Apparently, biometric applications involve the use of unique biological and /or behavioral characteristics of a person, which are collected and stored for the verification of a claim, made by that person or for his/hers automated identification. The two basic functionalities of biometrics, which must be distinguished for the assessment of privacy risks, are: 1) the verification function, which is a one-to-one comparison, allowing an authentication check of a claim by a person, and 2) the identification function, which is a one-to-many comparison, allowing to verify that a biometric characteristic is in the central database or to identify to whom that biometric characteristic belongs (Kindt, 2007). Verification does not always require identification and also, it does not require that the biometric feature is stored in a central database, but it can be stored on a card in the possession of the user.

Biometric data can be processed after a biometric template is extracted from the biometric data (e.g. image of the fingerprint, picture of the iris, etc.). The biometric template, which is a structured reduction of a biometric image, is presented in digitalized form and is stored in a database. Alternatively, biometric processing takes place on the basis of raw biometric data (e.g. an image). The templates can be stored in the memory of a biometric device, in a central database or in plastic, optical or smart cards (DPWP 2003, p. 4).

Biometric data processing is used for the automated verification or identification purposes in order to provide secure access to physical (restricted areas, workplaces and other facilities) or virtual areas (to electronic systems or services) (DPWP 2003, p. 2). On one hand, it should be stressed out that biometric systems enhance privacy, as they are more secure and flexible than the traditional authentication procedures, e.g. those based on documents or codes that can be stolen, lost or forgotten. On the other hand, however, the processing of biometric data means enhanced control of the individual, compared with traditional authentication and identification procedures.

The risks of biometric data processing

The privacy risks of biometric applications are emphasized by privacy activists, whereas data protection authorities also adopt a negative stance towards biometry (see below). At first hand, there is an association of biometry with criminality, since biometrics was initially applied in the area of DNA and fingerprint testing. Fingerprint testing has been used previously by law enforcement agencies for the investigation of crimes and their collection was subject to legal constraints. As a result, their use for verification or identification purposes provokes fears of increased surveillance over citizens or users of biometric applications and loss of dignity, as means of criminal investigation such as fingerprint testing are applied for identification and verification of common citizens (DPWP 2003, p. 1; Cavoukian, 1999).

In our view, the advantages provided by biometrics should not be ignored and, therefore, the assessment of privacy risks should consider the particular circumstances of biometric data processing. The main factors which must be taken into account are the purpose of the system,

[6] So, to perform authentication, three different methods may be used jointly – based on something the individual knows (password, PIN), something he/she owns (token, smart card, etc.) and something he/she is (biometric feature). For instance one can be authenticated to use a computer by inserting a smart card, typing a password and presenting his/her fingerprint (DPWP 2003, p. 4).

i.e. if it is used for identification or verification, whether biometric data are stored centrally or locally and whether a system allows the re-use of biometric data for incompatible purposes. Furthermore, a proportionality test should be applied, taking into account all the above criteria and the particular details of the processing.

Privacy concerns are awakened primarily when biometrics, e.g., fingerprints, are used for identification purposes and are stored centrally. In this way, biometric processing allows a person to be tracked individually and be subject to monitoring, since biometric features act as unique identifiers that bring together disparate pieces of personal information about a data subject (Cavoukian, 1999). It is notable that nowadays the use of biometrics for identification takes place on a large scale in the public sector, since the adoption of EU Regulation No 2252/2004 imposing mandatory biometric features in passports and travel documents. In the EU, also several governments have introduced eID cards with biometric features and others are planning to introduce eID cards (Hornung, 2004).

Another reason for concern is the possibility offered by biometric applications that personal information from different sources be linked together to form detailed personal profiles about the individual. This infringes manifestly the right to informational privacy and therefore, measures should be taken to address this threat to privacy. Similarly, a risk to privacy emerges where the biometric data will be used for other purposes, i.e. for secondary purposes not compatible with the purposes for which the data were initially collected. This risk comes mainly forward when third parties have the ability to gain access to biometric data in identifiable form and bring them together with other information, without the consent of the data subject (Cavoukian, 1999).

The accuracy of data is an important factor for the assessment of biometric systems. In case biometric data are not accurate, this would lead to the false rejection of authorized persons and the false acceptance of unauthorized persons. Such instances jeopardize privacy, if a third person is identified in place of an authorized person or if the latter is being wrongly rejected (Kindt, 2007, p. 168).

Other privacy risks of biometric applications are also subject of research. Security threats may put at risk the functioning of biometric systems, such as the misappropriation of biometric data via spoofing. Additional information which is present in raw data may reveal sensitive information concerning health or revealing racial origin. It is thus suggested to destroy such unnecessary data (DPWP 2003, p. 7-8).

The legal review of biometric applications by European organizations' opinions, Data Protection Authorities of EU Member States and national case law

An analysis of data protection problems of biometrics was delivered by the Data Protection Working Party (DPWP) in 2003 (op. cit), which identified some fundamental issues, stressing out the importance of the proportionality principle. The Consultative Committee of the 108 Convention (Consultative Committee 2005, p. 18) and the European Data Supervisor (EDPS, 2006, s. 2.4) also provided comments on the application of this principle in the biometric context.

The Working Party underlines that the purpose and proportionality principles must be observed. The purpose for which biometric data are collected and processed must be firstly

determined. Furthermore, the principle of proportionality has to be respected. Article 6 of Directive 95/46/EC lays down, in more particular, that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. And also that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (DPWP 2003, p. 6).

The Working Party also identifies other aspects that have to be addressed (DPWP 2003, p. 8). It refers to the principle of fair collection of information and to the legitimacy of processing, emphasizing that the processing of biometric data must be based on one of the grounds of legitimacy provided for in Article 7 of the Directive and in case sensitive data are being processed, the processing must be in conformity with the provisions of Article 8 of the Directive. The Working Party, further, suggests submitting biometric systems to prior checking by data protection authorities if systems are to be used that present specific dangers. It also highlights the obligation of the controller to take technical and organizational measures to protect personal data and particularly, to implement such measures from the beginning of the processing, especially during the phase of "enrollment", where biometric data are transformed into templates or images. Particular care should be taken in order to avoid false rejection of authorized persons and false acceptance of unauthorized persons, which could create problems on many different levels.

In accordance with the proportionality principle, which takes the most important place between the other legal principles that apply in the case of biometrics, it should be examined whether the purpose can be achieved in a less intrusive manner. With other words, if there are several appropriate measures that can be taken, the measure chosen must be the most privacy-friendly with regard to the purpose of processing.

The principle of proportionality is explained with reference to certain circumstances of biometric processing. The Working Party has the view that biometric systems related to physical characteristics that do not leave traces (e.g. shape of the hand but not fingerprints) create fewer risks for privacy. This applies also for systems related to physical characteristics which leave traces but do not rely on the storage of data in the control device or in a central data base. The Working Party in its opinion highlights that central storage or unnecessary storage for authentication should be avoided. It is not clear, however, from the opinion of the Working Party how should identification applications be assessed. As the central storage of biometric features is unavoidable for identification, one cannot totally exclude the implementation of biometric systems for this purpose, but a strict application of the proportionality principle is considered necessary (DPWP 2003, p. 6 et seq.).

The Consultative Committee proposes the use of biometric templates instead of raw biometric images, which contain less sensitive information than the raw data. It is argued, however, that it is not realistic to avoid any possible link with sensitive data, as most biometric data unavoidably contain racial, health, physical characteristic information which could be sensitive data (Liu, 2009, p. 239).

The Working Party and the Consultative Committee add to those criteria the storage length of the necessary biometric data and stress that biometric data should not be stored longer than necessary (DPWP 2003, p. 8; Consultative Committee, p. 8). Finally, the European data protection supervisor underlines the sensitive nature of biometric data and calls for risk assessment before any biometric processing takes place. It evokes the requirements of the

European Convention for the Protection of Human Rights and Fundamental Freedoms and its case law, which must be taken into account (European Data Protection Supervisor, 2006, p. 3). In the legal review of biometric applications, DPAs of the EU Member States base their decisions on the proportionality principle, applying the aforementioned criteria. In more particular, they check whether biometric applications for identification and authorization purposes comply with the requirements of Article 6 of the EU Directive as transposed into their national law. However, the interpretation of the proportionality principle varies, even by the one and the same authority. For instance, the French CNIL refused to allow the use of fingerprints to admit children to a school restaurant, since it held that digital fingerprints would pose too many dangers for misuse and that it was excessive. However, it accepted the use of hand geometry for the same purpose in a school cafeteria, as it held that they would not leave traces and could not be misused for any other than the original purpose.[7] On the other hand, the UK DPA has accepted the use of fingerprints in similar circumstances, but it noted that certain precautions should be taken, such as the limitation of the purpose of processing, security measures and the destruction of data when it is no longer needed (Information Commissioner's Office, 2007).

The use of fingerprints at the workplace to control the presence of employees or verify compliance with working hours and, at the same time, prevent unauthorized conduct by employees, has been considered as infringing the proportionality by the Italian[8] and Greek[9] Data Protection Authorities, since it has been held that the purpose of processing can be attained by other, less privacy-intrusive systems, which do not impinge on privacy and do not involve an employee's body.

The Greek DPA has adopted a very restrictive approach to biometrics, which is in some extent contradictory. While it considered as lawful the processing of biometric data related to access control in security installations in the Athens Metro[10] and the Venizelos Airport[11], it did not allow a biometric system used to authenticate users to company sites and systems, as it held that the control of entry into the company's facilities could be achieved by less restrictive means, such as access cards without biometrics[12].

A general remark is that in the decisions of DPAs in the EU Member States the legality of processing plays a less significant role than proportionality. It is notable that the Greek DPA delivered a negative decision on the use of iris and fingerprint on a smart card for air passengers in the context of a European project on the verification of identity of air passengers, on a volunteer basis[13]. Although data subjects would participate in this experimental project with their consent, the DPA held that in accordance with the principle of proportionality, less intrusive measures could be used, such as the presentation of the passport together with the ticket and the boarding card. It is notable that a project for the identification of frequent travellers is operational at the Schirphol airport in the Netherlands, while in the UK the IRIS project offers to passengers who volunteer to undergo an iris scan in order to skip passport checks.

[7] CNIL, Deliberation 02-070 of 15.10.2002.
[8] See The Garante per la protezione dei dati personali, Provision of July 21, 2005.
[9] DPA, Decision of 20/3/2000.
[10] DPA, Decision No. 9/2003, online available at: www.dpa.gr.
[11] DPA, Decision No. 39/2004, online available at: www.dpa.gr.
[12] DPA, Decision No. 74/2009, online available at: www.dpa.gr.
[13] DPA, Decision No 52/2003, online available at: www.dpa.gr.

More recently, however, the Greek DPA changed its opinion and delivered an affirmative decision on the use of a biometric application in the airport of Macedonia, Greece.[14] It allowed the operation of an experimental project in the airport installations, in which users' authentication takes place with the encryption of fingerprints and the production of various biometric identities. The Authority took into account that biometric data are subject to pseudonymization in a way that the biometric identities could not reveal the original biometric data.

On the other hand, the use of biometric data in EU passports, which affects all citizens, was introduced as a mandatory requirement despite the privacy controversy relating to it. It should be noted that the EU Regulation No 2252/2004 was upheld by the ECJ in its decision of 18 December 2007.[15] The Court held that the measures provided for in this Regulation concerning the verification of the authenticity of passports are capable of guaranteeing and improving the effectiveness of checks on persons at external borders and therefore, it considered Regulation No 2252/2004 as a measure developing the provisions of the Schengen acquis.

Evidently, there is discrimination of biometric applications in the private sector as compared to applications in the public sector and thus, a discussion is necessary of possible legislative solutions.

Legislative provisions on the processing of biometric data in EU Member States

The EU Directive 95/46/EEC has no specific provision on the processing of biometrics and thus, it has to comply with the provisions of the Directive, in general. Some statutes of EU Member States contain, however, specific provisions applying to processing of biometric data, which will be further scrutinized.

1. The Norwegian Personal Data Act

The provision of Article 12 of Norwegian Personal Data Act 2000 states that:

> National identity numbers and other clear means of identification may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification. The Data Inspectorate may require a controller to use such means of identification as are mentioned in the first paragraph to ensure that the personal data are of adequate quality.

This provision regulates the use of personal numbers and other means of identification such as fingerprints and other biometric data. It basically provides that "accurate identification means" such as biometrics are being used when it is necessary. The requirement of necessity is understood as an expression of the proportionality principle, since in accordance with the interpretations of this provision, the use of biometrics is not necessary when other less intrusive alternatives are available for achieving the reasonable security purpose (Liu, 2009, p. 242).

[14] DPA, Decision No. 31/2010, online available at: www.dpa.gr.
[15] Case C-137/05 United Kingdom of Great Britain and Northern Ireland v Council of the European Union. European Court reports 2007 Page I-11593.

Therefore, this regulation is a specification of the proportionality principle and thus, its regulative value is that it enhances the visibility of this principle.

2. The Personal Data Protection Act of Slovenia

The Personal Data Protection Act of Slovenia provides more detailed provisions on biometric data processing. In Article 6 Nr. 21 biometric characteristics are defined in the following way:

> Biometric characteristics - are such physical, physiological and behavioural characteristics which all individuals have but which are unique and permanent for each individual specifically and which can be used to identify an individual, in particular by the use of fingerprint, recording of papillary ridges of the finger, iris scan, retinal scan, recording of facial characteristics, recording of an ear, DNA scan and characteristic gait.

Such a provision can only indicate, of course, biometric features and could not be conclusive. Furthermore, the act includes a specific chapter on biometrics (Chapter 3), which applies to processing in the public and private sector. The purpose of biometric processing is defined in article 78, which states that: "The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act".

On processing of biometric data in the public sector, article 79 provides the following:

> (1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.
>
> (2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

This provision specifies general principles of data protection, such as the principle of lawfulness, necessity and proportionality. In our opinion, it is untenable that the law states the particular reasons of identification and verification and it would sufficient to declare that processing should be carried out for legitimate reasons.

Regarding biometric application in the private sector Article 80 (1) states that:

> The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance.

This provision does not differ from the previous provision. It defines the purpose of processing more abstract and it allows the processing in the workplace, provided only that employees are informed thereof. Here again, it would be sufficient to state that the purpose of processing is necessary for the purpose of the legitimate interests pursued by the controller.

The provisions of paragraphs 2 – 5 introduce an obligation of prior checking of the processing (in case "the implementation of specific biometric measures in the private sector is not regulated by a statute"). The National Supervisory Body has to make a decision whether the introduction of biometrics complies with the act and the provision of paragraph 1. It also has to decide on the lawfulness of biometric systems controlling the presence at work of public employees.

3. Other laws

Other laws of EU Member States regulate the processing of biometric data as sensitive data or provide for procedural rules, namely the notification of processing to the supervisory authority.

The Italian Personal Data Protection Code[16] provides in section 37 for the notification of the processing of biometric data to the Supervisory Authority.[17] Section 55, which applies in data processing by the police, imposes the requirements of prior communication to the Authority and measures and precautions aimed at safeguarding data subjects to be complied with.

The Data protection act of Luxembourg[18] provides in Article 14 that prior authorisation by the supervisory authority (national committee) must take place for biometric processing, which is necessary for the control of the identity of a person.

The Slovakian Act[19] provides for regulation of biometric data processing in the framework of the regulation of sensitive data (special categories of personal data). It defines biometric data as data of the natural person based on which the person is clearly and unequivocally identifiable, e.g. fingerprint, palm print, analysis of DNA, DNA profile (section 4 (1) lit. n). Furthermore, it provides that:

> Biometrical data may only be processed under conditions stipulated by a special Act, provided that: a) it expressly results for the controller from the Act; or b) the data subject gave a written consent to the processing.

The processing of biometric data is subjected to the rules on sensitive data, in two laws; namely, in the Czech Personal Data Protection Act of 4 April 2000 (Article 4 lit. b) and the Estonian Act of 1 January 2008 defines as sensitive data in § 4 (2).

A possible legislative solution

The divergences in the application of the EU data protection legislation with regard to processing of biometric data and the uncertainty as regards the criteria and factors used to apply the proportionality principle lead to the conclusion that a specific provision should be introduced concerning the said processing. The regulation of biometrics should necessarily include firstly, a comprehensive definition of biometric characteristic, so that the field of

[16] Legislative Decreee no. 196 of 30 June 2003.
[17] Garante per la protezione dei dati personali; www.garanteprivacy.it
[18] Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l' égard du traitement des données à caractère personnel.
[19] Act No. 428/2002 Coll. On Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll.

application of the provision is clearly defined. Secondly, substantial rules must be introduced. In our opinion, the purpose and proportionality principles should be specified in the context of biometrics. The relevant provisions should include procedural rules, e.g. rules on prior checking etc., so that the supervisory authorities exercise control over biometric processing.

It should be noted that the purpose of the processing of biometric data is crucial and certainly it must be one that serves particular authentication/verification or identification needs. It is untenable to support the view that biometric application can only be accepted in special cases for access control to premises or facilities secrets file, as the Greek DPA stated in many decisions (see, e.g., No 245/9/20.3.2000 decision). The legality of the purpose has to be judged on the basis of the criteria for making data processing legitimate. Consent is an important criterion, but in order to satisfy the requirements of being freely given, specific and informed, data subjects must be fully aware of the risks entailed by biometric technology. Nevertheless, even if data subjects have consented to data processing, a proportionality test has to be applied.

The main difficulty with the application of the proportionality principle is that a case-by-case interpretation of this principle may lead into conflicting decisions of data protection authorities. Thus, to conclude whether a specific application is the most privacy friendly among others, certain circumstances have to be taken into account. Generally, superisory authorities take into account the type of biometrics, the method of collection, the type and length of storage and the security of the system. One cannot preclude certain types of biometrics and give preference to others. In particular, the use of fingerprints cannot be generally excluded and preference be given to hand geometry. A system using fingerprints can be allowed in certain circumstances, so for instance if security measures are taken and data are deleted when they are no longer needed.

Finally, already Article 20 of Directive 94/56/EEC oblige Member States to determine the processing operations which are likely to present specific risks to the rights and freedoms of data subjects and check that there operations are examined prior to the start thereof. It is evident that the processing of biometric data presents such risks and ought, therefore, to be subjected to prior checking. It is noteworthy that the DP Working Party suggests to submitting biometric systems to prior checking if they pose particular dangers, but it would not be clear for data controllers and data protection authorities when this is the case. Therefore, a general obligation to submit such processing to prior checking should be introduced.

It would be also advisable to submit biometric applications to privacy impact assessment. The same provisions that would provide for prior checking should provide that the controller must submit a privacy impact assessment, on the basis of which the supervisory authority could make a decision to allow or not the biometric processing under consideration.

REFERENCES

Article 29 Data Protection Working Party, Working Document on biometrics, 1 August 2003, (No. 12168/02/EN, WP 80), online available at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

Cavoukian, A. (1999). Privacy and biometrics, online available at:
http://www.ipc.on.ca/images/Resources/pri-biom.pdf

European Data Supervisor (2006). Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organization of the reception and processing of visa applications (COM (2006 269 final) – 2006/0088 (COD) (2006/C 321/14).

Grijpink, J. (2006). An assessment model for the use of biometrics, Computer Law and Security Report 22, pp. 316-319.

Hornung, G. (2004). Biometric Identity Cards: Technical, Legal, and Policy Issues, in: S. Paulua, N. Pohlmann and H. Reimer (Eds.), Securing Electronic Business Processes, pp. 47-57.

Hornung, G. (2007). The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards, SCRIPT-ed, vol. 4:3, online available at: <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/hornung.asp>

Information Commissioner's Office (2007). The use of biometrics in schools, online available at:
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf

Kindt, E. (2007). Biometric applications and the data protection legislation, Datenschutz and Datensicherheit 31 (2007) 3, pp. 166-170.

Liu, Y. (2009). The principle of proportionality in biometrics: Case studies from Norway, *Computer Law and Security Report 25*, pp. 237-250.

Robinson, N., Graux, H., Botterman and M., Valeri, L. (2009). Review of the European Data Protection Directive, Technical Report, Rand Europe, online available at:
http://www.rand.org/pubs/technical_reports/TR710/

The Consultative Committee established by the Council of Europe's Convention for the protection of individuals with regard to automatic processing of personal data of 1981 (2005). Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, online available at:
http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf

Warren, S. & Brandeis, L. (1890). The right to privacy, *Harvard Law Review (4)*, pp. 193-220.

Westin, A. (1967). Privacy and Freedom. Athenaum, New York.

Zorkadis,, V. & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective. Deriving privacy-enhancing requirements, Information Management & Computer Security vol. 12 No. 1, pp. 125-137.