Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 12522
16 February 2011

The need for a global consideration of the human rights implications of biometrics

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Holger HAIBACH, Germany, Group of the European People's Party (EPP/CD)

Summary

In the aftermath of the events of 11 September 2001, the issue of security, and consequently that of the identification and verification of individuals, has become a priority at global level. The use of biometrics is becoming more and more frequent. The Committee on Legal Affairs and Human Rights is increasingly concerned about the rapid and uncontrolled development of biometric technologies. It stresses the need to strike an appropriate balance between security and the protection of human rights and fundamental freedoms, especially the right to privacy.

Given that at European level the legal framework regarding the use of biometric data remains vague, Council of Europe member states should take further measures to improve it. In particular, they should adopt specific legislation in this area, produce a standardised definition of "biometric data", put in place supervisory bodies and promote multidisciplinary research.

The Committee of Ministers could, amongst other things, revise the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in order to adapt it to the challenges stemming from the development of biometric technologies.

1. 2011 - March Standing Committee

Contents **Page**

A. Draft resolution[2]

1. In the aftermath of the events of 11 September 2001, security issues have become a priority at the global level. They have led to an ongoing search for secure and reliable methods of identification and verification of the intrinsic aspects of a human being through the use of biometrics. The rapid development of biometric technology offers a possible solution to various security concerns, but it also puts at stake several human rights, such as the right to respect for private life, the right to a fair trial and the presumption of innocence, the freedom of movement and the prohibition of discrimination, as enshrined in the European Convention on Human Rights (ETS No. 5).

2. The Parliamentary Assembly notes that there is a need to properly balance security and the protection of human rights and fundamental freedoms, including the right to privacy. The broad technical scope of biometrics, its rapid development and member states' willingness to make use of it for multiple purposes may not yet be appropriately reflected in member states' legislation in order to safeguard human rights. Once a new technology has found its way into everyday life, it becomes more difficult to implement or even adopt a proper legal framework. Member states should therefore deal with the legal issues relating to biometrics without delay.

3. At the European level, the existing legal framework remains vague, as there is no generally accepted definition of "biometric data". Thus the Assembly strongly believes that the Council of Europe itself should take steps to ensure that this legal framework is enhanced and modernised.

4. The Assembly therefore calls upon member states to:

4.1. adopt specific legislation on the use of biometric technologies to protect individuals from abuses of rights enshrined in the European Convention on Human Rights and other instruments on human rights protection, in particular to:

4.1.1. elaborate a standardised definition of "biometric data";

4.1.2. revise the existing regulations concerning general protection of personal data by adjusting them to current applications of enhanced biometrical technologies;

4.2. keep their legislation under review in order to meet the challenges stemming from the further development of biometric technologies, including so-called "second generation" biometrics;

4.3. promote proportionality in dealing with biometric data, in particular by:

4.3.1. limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice;

4.3.2. providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification;

4.3.3. working with template data instead of raw biometric data, whenever possible;

4.3.4. enhancing transparency as a pre-condition for meaningful consent and, where appropriate, facilitating the revocation of consent;

4.3.5. allowing individuals access to their data, and/or the right to have it erased;

4.3.6. providing for appropriate storage systems, in particular by reducing central storage of data to the strict minimum;

4.3.7. ensuring that biometric data are only used for the purpose for which they have been lawfully collected, and preventing unauthorised transmission of, or access to, such data;

4.4. establish, as appropriate, supervisory bodies to control the implementation of relevant legislation and provide for effective remedies for individuals in case of violations of their human rights and fundamental freedoms;

4.5. strengthen the compliance of private sector applications of biometrics with existing data protection law, especially by:

4.5.1. ensuring accountability of data controllers;

4.5.2. promoting the training of relevant actors in the appropriate handling of personal data;

---

2. Draft resolution adopted unanimously by the committee on 16 December 2010.

4.6. promote multidisciplinary research on new biometric technologies that would ensure a balance between the need for enhanced security and the respect for privacy, human dignity and transparency;

4.7. assess potential risks resulting from the use of biometrics for human rights and fundamental freedoms and exchange results between member states.

5. The Assembly also calls on member states to step up international co-operation, in particular with the United Nations, the Organisation for Economic Co-operation and Development and the European Union, with a view to harmonising standards on biometrics, in conformity with international human rights standards.

B. Draft recommendation[3]

1. The Parliamentary Assembly notes that the Council of Europe has already demonstrated its commitment to the protection of human rights in relation to data protection, in particular by adopting the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and through the work of its Consultative Committee. The Council of Europe is therefore well placed to promote the adoption at the European level of rules on the use of biometrics.

2. Referring to its Resolution … (2011), the Assembly invites the Committee of Ministers to:

2.1. revise the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in order to adapt it to the challenges stemming from the development of new technologies, including biometric technologies, in particular by developing a definition of "biometric data";

2.2. prepare guidelines for member states on legislative frameworks that would strike a fair balance between the interests of the parties concerned, including those of security and privacy;

2.3. continue to observe the development of biometric technology and its possible impact on the rights and freedoms enshrined in the European Convention on Human Rights and other Council of Europe instruments on human rights protection.

3. The Assembly also recommends that the Committee of Ministers develop its co-operation with the United Nations, the Organisation for Economic Co-operation and Development and the European Union, with a view to comparing the existing regulations on biometrics and promoting coherent guidelines concerning their use.

3. Draft recommendation adopted unanimously by the committee on 16 December 2010.

C. Explanatory memorandum by Mr Haibach, rapporteur

1. Introduction

1. On 5 October 2006, the Parliamentary Assembly decided to refer to the Committee on Legal Affairs and Human Rights, for report, the motion for a recommendation on the need for a global consideration of human rights implications of biometrics (Doc. 11066). At its meeting on 27 January 2009, the committee appointed me rapporteur.

2. Following the events of 11 September 2001 and other terrorist attacks, security issues have become a priority at the global level and have led to an ongoing search for secure and reliable methods of identification and verification using the intrinsic features of each human being, such as fingerprints, retina, DNA, voice or, more recently, body scans. In the absence of any specific legal framework covering this issue, the rapid development of biometric technology raises some concerns with regard to the protection of human rights and fundamental freedoms.

3. "Biometrics" refers to systems that use measurable physical or physiological characteristics or personal behavioural traits to recognise the identity, or verify the claimed identity of an individual.[4] In comparison with other means of authentification, such as badges and passwords, biometric data reduce the possibility of abuse because they cannot easily be transferred to third parties and do not rely to the same extent on verification or identification by security personnel, which is the main weakness of current security systems. Therefore, technologies using these biometric data to confirm an individual's claimed identity can both improve overall safety and reduce the risk of fraud. Although the advantages of biometrics in terms of security are indubitable, the proliferation of biometrics presents challenges concerning fundamental human rights, and in particular data protection. The collection and evaluation of biometric data as such does not seriously interfere with an individual's rights given that taking pictures or fingerprints, etc. with today's technology is fast and non-intrusive. But mass processing and central storage of personal data, as performed, for instance, in the Eurodac database for asylum applications in the European Union member states,[5] may interfere with the private sphere of individuals, since the integrity of the human body and the way it is used in collecting biometric data constitute an aspect of human dignity.

4. This report is intended to present the main issues concerning biometrics, such as the meaning of this term, the collection and conservation of biometrical data in practice and the concerns related to the latter.[6] It will also refer to the existing European regulations on data protection and will make some recommendations on how to fill loopholes identified in the legislative framework.

2. What does the term "biometrics" encompass?

5. Biometric data are unique individual physical or behavioural characteristics that differ from one human being to another and that remain, in most cases, unaltered for life. Examples of biometric data are DNA samples, fingerprint images, pictures of the iris or the retina, but also voice recording, individual gait or typing rhythm during logon.

6. Biometric systems are a highly reliable means of authentication as they allow for proof of a strong connection between an individual and his alleged identity through verification of his or her unique physical biometric data. Furthermore, the convenience of such systems makes them more acceptable. Instead of long identification and verification procedures conducted by security personnel, iris/facial scans as well as behavioural tracking allow for swift security checks even of large crowds of people. Despite the initial investment in up-to-date equipment, biometric technology is cost effective – avoiding for example the costs of forgotten passwords.

---

4. Glossary of the European Data Protection Supervisor. www.edps.europa.eu:80/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/72.

5. Eurodac is based on European Council Regulation No. 2725/2000 following the Dublin Convention. The database holds a collection of fingerprints of asylum seekers and aliens that have illegally crossed external borders. For more information on Eurodac, see: http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33081_en.htm.

6. In this context, I would like to express my appreciation for the help obtained from Professor Paul De Hert, Vrije Universiteit Brussels and Tilburg University. A background paper prepared by him has served as the principal source of this report.

7. The use of "first generation" biometrics (for example fingerprints and iris scans) has given rise to limited controversy as regards human rights, in particular as regards the conditions in which such data can be collected and for which purposes they may be used. The subsequent introduction of "soft biometrics" – which includes gender, weight, height, age and ethnicity for automated classification – has proved more contentious, evoking objections on the basis that it could constitute or facilitate discriminatory social profiling. "Second generation" biometrics aim to identify a person on the basis of his or her actual behaviour or activities. They may include measurements of the heart rate, body temperature, brain activity patterns and pupil dilation, which calls into question what we understand by "personal data". Also, it may be necessary to determine to what extent, if any, the (ab)use of body scanners ought to be dealt with in this context. The fact that such data can be collected without the individual's knowledge merely adds to the controversy. Today's video surveillance technology is capable of tracing individuals from a distance and creating profiles without the knowledge of the person concerned.

3. What are the different applications of biometric data?

8. The use made of biometrics varies across Council of Europe member states. Biometric systems will serve either one or both of two main purposes: identification of an individual, by which the identification is solely based on the biometric information, or verification of an individual, where a verification template is compared to an enrolment template. Identification requires a one-to-many comparison, while verification requires a one-to-one comparison. Different types of storage should be used depending on the overall objective of the given system. Generally speaking, identification poses a much greater risk to human rights than the direct use of biometric data, since in identification procedures such data are never under the strict and full control of the individual.

9. The most common applications of biometrics can be found in the field of immigration control. Here, biometrics may be used for passports, border control, visa applications and ID checks on asylum seekers. Large-scale databases such as the European Union Visa Information System and the Schengen Information System centralise and store such data in Europe.

10. In addition, most if not all Council of Europe member states allow the compulsory taking of fingerprints and cellular samples in the context of criminal proceedings. At least 20 member states make provision for collecting DNA information and storing it in national databases or in other forms (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Luxembourg, the Netherlands, Norway, Poland, Spain, Sweden and Switzerland). This number is steadily increasing.

11. Due to its convenience, the private sector also drives the rapid development of biometrics. Biometric data is used for access control to private buildings such as casinos, discotheques or fitness studios. Insurance companies have an immense interest in biometrics since any information on their clients' health status helps their cost/risk analysis. The extended use of loyalty cards demonstrates customers' willingness to reveal personal preferences, though customers are not always fully aware of the extent to which this involves the revelation of personal data.

12. The need to identify individuals accurately in both the public and private spheres makes the further development of these technologies inevitable. In the public sector, biometrics have become a key instrument for national and international security and immigration policies. The fight against terrorism and organised crime also benefits from the use of modern scientific techniques of investigation and identification. As a result, in addition to employing biometric systems for border control purposes, states are creating increasingly large central databases holding biometric data such as computer-readable facial photographs, fingerprints and DNA.[7] Meanwhile, biometric systems are gaining importance as a product in the private sphere as identity fraud becomes increasingly common in the growing field of e-business.

4. Risk of falsification

13. Biometric data are considered to be very reliable and, indeed, in most systems there is a high probability that in using biometric data for identification purposes, one is dealing with the correct individual.

---

7. For instance, in October 2009 the French authorities created a database "OSCAR" (*outil simplifié de contrôle des aides au retour*) which contains biometric data of aliens having received financial aid to return to their country of origin. This decision was contested to no avail by several French NGOs. See: www.ldh-toulon.net/spip.php?article4049.

14. But false positives or negatives remain possible due to the technical imperfections of biometrics. An error rate of 0.5% to 1% is the norm, so there is no such thing as an absolutely certain match or non-match. Poor light conditions or insufficient training of operators increase the risk of false identification/verification. Intentional manipulations are also possible.

15. Biometric characteristics, in principle, remain unchanged for the duration of an individual's life. There are, however, certain exceptions where a change in biometric features may occur, such as through surgery, accidents, or simply ageing. Studies on the long-term viability of biometrical data have shown, for example, that fingerprints may change as time passes.

16. Being affected by bodily growth, biometric features are not fully developed until early adulthood. Using children's fingerprints for passports or access control methods as already practised in some schools, increases the risk of mistakes. Until their biometric features are fully developed, children should not be subjected to the collection of biometric data, also in order to prevent premature categorisation and discrimination.

17. Additionally, there is the important issue of the security of stored biometric data. Biometric systems are vulnerable to hacking, unauthorised modification or destruction, tampering, unintentional loss, and improper disclosure. Falsification of biometric data, particularly fingerprints, has been shown to be entirely possible. Furthermore, the use of biometrics will not exclude identity theft or forgery, as shown in the case of the new e-passports introduced in a number of European Union member states.

5. Main human rights concerns concerning biometrics

18. Where personal data is dealt with, sufficient safeguards are of key importance in order to guarantee the protection of human rights. The technology of biometrics is capable of providing enhanced security whilst protecting human rights. What raises concern is the widespread unnecessary and careless use of such personal data.

19. The prospect of combining biometric data collected by public bodies and exchanging them with private businesses poses a serious threat to an individual's human rights.[8] The intense interest of the private business sector is caused by the benefits of detailed knowledge of their customer's physical features and habits, for example for an insurer's cost-risk-analysis or for marketing purposes. As a result, personal data have become valuable commodities.

20. The threat for individual rights is mainly posed by the danger of collecting and combining the data without the consent or even knowledge of those directly concerned and collecting more data than necessary.[9] Cash-strapped public bodies may be tempted to sell personal data as private businesses offer large sums for such information. Due to the legal complexity of the question of a possible effect of human rights among private actors (*Drittwirkung*), I will not go into detail on this issue as regards the biometrics field.[10]

5.1. Human dignity

21. Biometric data are collected or derived from the human body and, as such, the question arises whether this may affect a person's human dignity. Whilst some may not feel so affected, others may be uncomfortable with bodily scrutiny and resist collection of their biometric data. This may be due to religious, sociocultural or other personal reasons. Human dignity is the basis for human rights and, therefore, lies at the heart of all potential human rights violations.

---

8. National Consultative Ethics Committee for Health and Life Sciences. *Opinion No. 98 – Biometrics, Identifying Data and Human Rights*, 20 June 2007. www.ccne-ethique.fr/docs/en/avis098.pdf. An example from the United Kingdom where the government's e-borders data is linked with passenger information provided by airlines. Arnott, S. (2004). *Leak reveals details of eBorders trial routes*, www.computing.co.uk/computing/news/2071239/leak-reveals-details-eborders-trial-routes.

9. Example from the National Commission for Data Protection in Luxembourg which refused the application by a private spa operator to use biometric data as an access control method because the principle of proportionality had not been considered. Not until the operator had agreed to store the data individually, and not centrally, did the commission accept the application. See: www.cnpd.public.lu/fr/decisions-avis/2006/04/decision-traitement-biometrique/deliberation_33_2006.pdf.

10. For more information and related acts see my report on human rights and business, Doc. 12361 of 27 September 2010.

5.2. Right to respect for private life (Article 8 of the European Convention on Human Rights)

22. Clearly, the evaluation, but even more the collection and storage of data touch upon the right to respect for private life as guaranteed by Article 8 of the European Convention on Human Rights ("the Convention"). Since personal information is capable of revealing an individual's identity to a great extent, it is necessary to handle this information in a sensitive way.

23. Some data need to be collected in order to strike a fair balance between security and privacy. But the technology in the field is capable not only of collecting the data required for identification, but also of revealing a person's racial origin, medical status, or other genetic information. Iris scans reveal known or even diseases yet unknown to the individual. In combination with existing DNA technology – which in a technical sense is not considered as biometrics, but faces similar concerns regarding privacy – there is a very high risk of the complete exposure of a person's identity.

24. This poses a serious threat to sick and disabled individuals, in particular in terms of job opportunities, insurance coverage, etc., and also to an individual's sexual identity. It contradicts the right to respect for private life which includes the right to self-determination in terms of public recognition. Individuals who have changed their gender would not be recognised on the basis of their choice, but by biometric data. Those concerned may be exposed to discrimination and ostracism.

5.3. The prohibition of discrimination (Article 14 of the Convention)

25. The use of biometrics may also raise several concerns as to its compliance with the principle of non-discrimination, as set out in Article 14 of the Convention (and Article 1 of its Protocol No. 12 (ETS No. 177)[11]. In this context, we should, in particular, consider the implications of biometric systems for those with physical disabilities or people whose physical characteristics do not fit technical requirements. This may in itself raise data protection concerns as the mere fact of being processed under an alternative system reveals potentially sensitive information. Deriving such information from biometrical data may go beyond acceptable objectives of personal data collection. Increased use of biometrics could in future lead to stigmatisation and social exclusion of those who are disabled or those whose physical characteristics are not easily measurable. Studies have shown longer processing times and fewer possible methods for disabled individuals in almost all forms of biometric methods.[12]

26. Individuals are concerned that their biometric data is used for purposes other than those for which it was originally collected or other than what was consented to at the time of collection (so-called "function creep"). The best-known example of this in the biometrics field is the opening up of the Eurodac site to the police and other law enforcement agencies. The opening up of large databases such as this one may enable governments to secretly monitor the activities of individuals. What is more, such creeping changes may involve carrying out discriminatory research or sorting subjects into groups for dubious reasons. The use of biometric data to identify ethnic minorities for political purposes is a particular cause for concern.

27. The existence of creeping changes in the use of data collected in the public sector can be explained by the recent tendency of governments to focus on surveillance, control and fraud detection, an attitude that is fed by the global fear of terrorism following the events of 11 September 2001. This emphasis on controlling individuals has reduced the focus on the need for minimising data collection and on risk mitigation.

5.4. Right to a fair trial (Article 6 of the Convention)

28. Taking into account the risk of falsification (see Section 4 above), the use of biometrical data may also put at risk individuals' right to a fair trial (as guaranteed in Article 6, paragraph 1, of the Convention) and, in particular, the principle of the presumption of innocence (Article 6, paragraph 2[13]). An erroneous or manipulated result can have severe consequences for the individual concerned, for example when a person is falsely recognised as appearing on a list of wanted criminals. The practical effect of this could be that the person ends up having to prove his or her innocence. It is therefore vital that the probabilistic nature of biometrics is kept in mind and the presumption of innocence is respected; this principle being a core principle of a democratic society, it must not – at any point – be turned into the contrary.

---

11. To date only ratified by 18 Council of Europe member states.
12. UK Passport Service, *Biometrics Enrolment Trial, Report*, 2005, p. 8, http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf.
13. Article 6, paragraph 2: Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

29. Taking fingerprints is mostly associated with criminal conviction because the method has been used for a long time in this field. Considering that many asylum seekers have already experienced persecution, the biometric evaluation process may cause psychological trauma. As the case of *S. and Marper v. the United Kingdom* shows, biometrics may also violate an individual's right to a fair trial by not properly differentiating between convicted persons and those who have not been convicted of any offence.[14] This stigmatisation may infringe the presumption of innocence.

5.5. Freedom of movement (Article 2 of Protocol No. 4 to the Convention)

30. At the European level, freedom of movement is guaranteed, to a certain extent,[15] by Article 2, paragraph 1, of Protocol No. 4 to the Convention, and Article 2, paragraph 2, of this protocol provides for the right to leave any country, including one's own. Moreover, citizens of member states of the European Union enjoy the right to freely move and stay within the member state's territory under Article 21 of the Treaty on the Functioning of the European Union.[16] As biometric technology is often used in the field of border controls, the threat lies in the potential refusal of entry on illegitimate grounds or due to system errors. If the subject is in addition not properly informed of the procedures used, he or she may not be in a position to redress the situation.

6. Legal regulations

31. At present, there is no worldwide instrument dealing with biometrics. Existing legislation only addresses "personal data" in general but rarely defines what biometrics actually are. Taking into account that technology has developed rapidly over the last few years, regulations must be adapted to achieve a fair balance between security and human rights issues. The existing general coverage through personal data regulations may be applicable to biometrics, but second generation biometrics put human rights at a greater risk than earlier technologies.

6.1. At the global level: the United Nations

32. Article 17 of the International Covenant on Civil and Political Rights guarantees the right to respect for privacy. The United Nations set up general Guidelines for the regulation of computerized personal data files in 1990.[17] These guidelines seek to avoid insecure, inaccurate, discriminating and unlawful evaluation and processing of personal data. They stress the importance of earmarked processing and the importance of consent by the individual. An independent supervisory body shall control the collecting and processing of data. The principle of proportionality shall be taken into account and the transborder flow of personal data shall be subjected to security provisos.

33. Nevertheless, it has to be stressed that the guidelines drawn up by the United Nations do not specifically address biometric data, only general personal data; they are therefore somewhat outdated.

6.2. At the regional (European) level

6.2.1. Organisation for Economic Co-operation and Development

34. The Organisation for Economic Co-operation and Development (OECD) drew up its Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980.[18] Although these recommendations only address data and information in general, they indicate what is considered by the OECD to be "personal data". Moreover, the Working Party on Information Security and Privacy developed a detailed definition of "biometrics" in its report in 2004.[19]

---

14. European Court of Human Rights, *S. and Marper v. the United Kingdom*, Applications Nos. 30562/04 and 30566/04, judgment of 4 December 2008, paragraph 122.
15. According to this provision, "Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence". Paragraphs 3 and 4 of Article 2 of Protocol No. 4 set out further restrictions to the rights provided in this article.
16. The consolidated version of this treaty may be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:EN:PDF.
17. *United Nations guidelines for the regulation of computerised personal data files*, A/RES/45/95, www.un.org/documents/ga/res/45/a45r095.htm.
18. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
19. *OECD Working Party on Information Security and Privacy, Biometric-Based Technologies*, 2004,

35. The OECD advocates limitations regarding the collection of data, including for legitimate purposes. Like the United Nations, it stresses the importance of the consent of the data subject and the need for an independent, strong control mechanism. In the above-mentioned 2004 report, it expressed concern that, even though biometrics can enhance security when properly used,[20] there was still a high risk of system failures.[21]

6.2.2. Council of Europe

6.2.2.1. Article 8 of the Convention and the case law of the European Court of Human Rights

36. The European Convention on Human Rights and its additional protocols guarantee several rights and freedoms which may be directly concerned by the use of biometrical data: right to respect for private life, right to a fair trial and presumption of innocence, prohibition of discrimination and freedom of movement. Among these rights, the right to respect for private life, as stipulated in Article 8 of the Convention, is of particular importance for individuals in this context and has been at the origin of a rich case law of the European Court of Human Rights ("the Court"). However, this right is not an absolute right, as it may be subject to interferences that are justifiable according to Article 8, paragraph 2, of the Convention. Restrictions have to be "in accordance with law" and "necessary in a democratic society".

37. Under Article 8 of the Convention, the European Court of Human Rights has dealt with data protection in numerous cases. However, although the technology of biometrics is not new, there have not been many cases explicitly addressing biometrics. This is due to the fact that the technology has only recently entered into everyday life.

38. The principle of proportionality plays a key role in the decisions of the Court. The cases of *Kinnunen v. Finland,*[22] *Van der Velden v. the Netherlands,*[23] *Rotaru v. Romania*,[24]and *W. v. the Netherlands*[25]show that the question of privacy violations have to be answered on a case-by-case basis.

39. The Court's judgment of 2008 delivered in the case of *S. and Marper v. the United Kingdom*[26] stands as a landmark in the field of biometrics. This case concerns fingerprints and DNA samples that had been collected following the arrest of the complainants and retained even after their release, even though the complainants had asked for the destruction of the samples. The Court held that the long term retention of both fingerprints and DNA samples interfered with the individuals' rights to privacy and, consequently, found a breach of Article 8 of the Convention. This judgment should be applicable to other biometric data; the case also highlights the importance of consent of the data subject and the sensitivity of the data in question.[27]

40. This judgment is also in line with the previous findings of the Court concerning personal information in secret police registers[28] and the taking, retention and determination of DNA samples.[29] Biometric data that have been obtained in the course of criminal investigations tend to meet the legitimate aims requirement for as long as there is a reasonable suspicion against an individual. Legislation should generally be precise and provide not only exact definitions of the data in question, but also clearly state the legitimate purposes for collection, evaluating and processing such data.

---

www.oecd.org/officialdocuments/displaydocumentpdf?cote=dsti/iccp/reg(2003)2/final& doclanguage=en.

20. Ibid., p. 13.
21. Ibid., p. 38.
22. *Kinnunen v. Finland*, Application No. 24950/94, decision of 15 May 1996. The Court found that the taking of fingerprints and photographs following an arrest did not breach Article 8 of the Convention due to the lack of information that called for refutation.
23. *Van der Velden v. the Netherlands*, Application No. 29514/05, decision of 7 December 2006. The Court held that the systematic retention of DNA material for potential future use was sufficiently intrusive to constitute a breach of Article 8 of the Convention.
24. *Rotaru v. Romania*, Application No. 28341/95, judgment of 4 May 2000. The Court found a breach of the applicant's right to respect for his private life due to the lack of sufficient legal safeguards against abuse of the way in which the Romanian Intelligence Service (RIS) collects, keeps and uses information.
25. *W. v. the Netherlands*, Application No. 20689/08, decision of 20 January 2009. Taking DNA samples from a minor following a conviction does not violate Article 8 of the Convention if, besides the age of the convicted person, all requirements for taking DNA samples are met.
26. *S. and Marper v. the United Kingdom*, Applications Nos. 30562/04 and 30566/04, judgment of 4 December 2008.
27. Ibid., paragraph 84.
28. *Leander v. Sweden*, Application No. 9248/81, judgment of 26 March 1987, paragraph 48.
29. *Van der Velden v. the Netherlands*, see footnote 23 above.

6.2.2.2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

41. The main legal instrument emanating from the Council of Europe and relevant for biometrical data is the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) ("the Data Protection Convention") and its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181).

42. The Data ProtectionConvention has been ratified by 43 of the 47 member states to date. It aims to set up better defined standards of privacy protection, and harmonise and enhance privacy protection in the member states. It was the first international legally binding document to address such issues. It defines "personal data" as well as "controller" and "automatic processing" and thereby follows the regulations which had been established by the OECD a year before its adoption. It addresses the public as well as the private sector.

43. Article 5 of the Data Protection Convention sets out the principles of evaluating and processing personal data (lawful obtention, storage and use, and accuracy). In terms of data security (Articles 7 and 8), its provisions are rather general ("appropriate measures"), leaving much discretion to member states' legislation. The same applies to sensitive data such as health, sexual life, and political and religious beliefs. Such data may not be processed automatically, unless domestic law provides appropriate safeguards (Article 6).

44. Article 5.c requires "adequate, relevant and not excessive" use of data – an expression of the principle of proportionality which would benefit from being further strengthened in the light of the new challenges.

45. Since personal data defines a person in terms of his or her virtual existence, the right of self-determination has to play a key role in any legal regulation. Self-determination calls for consent. While the Data Protection Convention mentions the right of the data subject to obtain erasure of the collected data (Article 8.c), it is not clear whether the data subjects retain ownership of their data and, therefore, whether they are entitled to decide about the processing of it. Article 8.c thus reveals a certain weakness of the Data Protection Convention, which is setting up the right instruments whilst allowing for too many exemptions. Although keeping in mind that the convention "only" sets out principles that the member states have to implement, it should push member states towards stricter regulation.

6.2.2.3. Additional Protocol to the Data Protection Convention

46. In 2001, an additional protocol to the Data Protection Convention regarding the establishment of supervising authorities was opened for signature. So far, it has been ratified by 30 member states. According to this protocol, the Council of Europe member states are required to put independent control bodies in place.

6.2.2.4. Progress report

47. In 2005, the Council of Europe issued a Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data. This report was prepared by the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. It contains an analysis of the specificities of biometrics, a discussion on the criteria for choosing a system architecture and guidance for the application of convention to biometrics. In the first place, the problem was whether the convention applies to biometric data as such,[30] since it only addresses personal data. Doubts concerning its applicability arise from the fact that identification and verification do not work solely on the biometric information itself but always need a match in order to identify or verify.[31]

48. Nevertheless, as the process always involves a biometric trait which is unique to the individual concerned why would it not be considered as personal data? Considering name or date of birth as personal data, which are facts relating to a person, one can conclude *a maiore ad minus* that body traits or behaviour are also personal data, since these are not given to a person but rather are inherent or natural features of each person. Therefore, there is no need to base the applicability of the Data Protection Convention solely on the fact of automatic processing as is done in the report,[32] but it can be based on the fact of biometric data being personal data as well as on the automatic processing aspect.

30. See www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.
31. See paragraph 8 above.
32. Ibid.

49. Acknowledging the fact that many aspects of biometrics are not yet fully known, the report does not provide any final conclusions and leaves open the possible need to revise the Data Protection Convention in this respect. Biometric technology can strongly enhance security, but the line towards human rights infringements may easily be crossed. Many individuals are not sufficiently aware of the possibility of losing their privacy in order to gain more convenience and are willing to use new technologies without further reflection. Keeping in mind that valid consent cannot be given without the knowledge of its consequences, awareness of the consequences of the use of biometric data must be raised.

6.2.3. European Union

6.2.3.1. Charter of Fundamental Rights

50. Whilst it has not been altered in content, an immense change in the status of the right to privacy and personal data protection has been brought about by the entry into force of the Treaty of Lisbon, which has made the European Union Charter of Fundamental Rights ("the Charter") binding through Article 6, paragraph 1, of the Treaty on European Union[33] and by the reference to data protection in Article 16 of the Treaty on the Functioning of the European Union. The Charter not only protects private life in its Article7,[34] but also guarantees the protection of personal data in Article 8.[35] The status of the rights set down in the Charter highlights the importance of the need to protect such information.

6.2.3.2. Directive 95/46/EC

51. In 1995, the European Parliament and the Council of the European Union adopted Directive 95/46/EC,[36] which deals with protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive builds on Article 8 of the European Convention on Human Rights and on the provisions of Data Protection Convention. Like most of the existing legislation it does not explicitly deal with biometric data but more generally with personal data. It is upon this directive that European Union member states have based their data privacy regimes. Other instruments have also been adopted at European Union level as regards personal data protection.[37]

52. Directive 94/46/EC obliges European Union member states to enact legislation that strikes the right balance between security and privacy issues. Obviously, the directive does not cover data protection in non-member states of the Union.

53. Due to globalisation and recent technological developments, the European Commission, on 4 November 2010, proposed a strategy to strengthen European Union data protection rules, including the revision of Directive 95/46/EC. It envisages proposing, in 2011, a new general legal framework for the protection of personal data in the European Union,[38] which, among other things, will strengthen individuals' rights in the process of data collection.

---

33. See its consolidated version at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:EN:PDF
34. "Everyone has the right to respect for his or her private and family life, home and communications".
35. Article 8 – Protection of personal data
    1. Everyone has the right to the protection of personal data concerning him or her.
    2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
    3. Compliance with these rules shall be subject to control by an independent authority.
36. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
37. In particular Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2006/24/EC; Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
38. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=0&language=EN&guiLanguage=fr.

6.2.3.3. Council Regulation (EC) No. 2252/2004

54. Council Regulation (EC) No. 2252/2004[39] deals explicitly with the standards for security features and biometrics in passports and travel documents issued by European Union member states. The regulation aims to enhance security by harmonising and providing minimal security standards for biometrics in travel documents in order to avoid identity fraud and falsification.

55. Privacy issues, however, are only minimally addressed by this regulation, through the obligation to respect the principle of proportionality and to state the purpose of evaluating and processing biometric data. The question of proper storage is not even regulated but left to the discretion of member states. Nor does the regulation contain a definition of biometric features or biometric identifiers.

6.2.3.4. Article 29 Data Protection Working Party and the European Data Protection Supervisor

56. Additionally, as a result of the Directive 95/46/EC, the Working Party on Article 29 was created as a supervisory body consisting of members from all European Union member states plus the later established European Data Protection Supervisor (EDPS). The working party is an advisory body which helps member states to correctly set up the framework established by the directive and to work towards a uniform legislation.

57. The European Data Protection Supervisor was established in 2001. The EDPS' tasks are similar to those of the working party and consist of supervision, co-operation with national supervisory bodies as well as advising.

6.3. At the national level

58. At the national level, very few countries have enacted general legislation regulating the processing of biometric data. In most Council of Europe member states, national legislation does not explicitly mention biometrics. This subject usually falls under national data protection legislation.

59. Of the 47 Council of Europe member states, 34 have a provision on data protection in their constitution. Furthermore, most have specific national legislation covering personal data protection.[40] Whilst many states outside Europe have adopted legislation addressing the public and private sectors in separate laws (or rubrics within the same legislative framework) covering both sectors separately, most European states have adopted a single piece of legislation covering both the public and private sectors.

7. Concluding remarks

60. According to the 2005 progress report of the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, "The application of biometrics raises important human rights questions. The integrity of the human body and the way it is used with regard to biometrics constitutes an aspect of human dignity …".[41] The main human rights problems caused by the proliferation of biometrics concern the right to privacy, the right to a fair trial, the presumption of innocence, the freedom of movement and the prohibition of discrimination. Biometrics is in its infancy and there is still little knowledge about possible drawbacks. Once the technique is chosen on a larger scale, an irreversible development is started with unforeseeable effects. The precautionary principle requires a certain reticence under these circumstances. In future, the collection of data might not even be noticed anymore. Video surveillance programmes are already capable of tracking a person from a distance. Therefore, whenever biometric data is collected, this has to be announced clearly to those concerned beforehand, for example by information signs in public places.

61. Five years after the adoption of the 2005 progress report, it is time to look closely at biometrics again, bearing in mind the technological progress made in the meantime. One should also not forget that second generation biometrics extend their range and increase their accuracy and intrusiveness. Moreover, it should be noted that the information available on these issues is often contradictory, in particular due to the blurring of boundaries between potential (or future) and current capabilities of biometric applications. Therefore, a

---

39. 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R2252:EN:HTML

40. For an overview of national data protection legislation see: www.coe.int/t/dghl/standardsetting/dataprotection/National_laws_en.asp.

41. See footnote 30, paragraph 10.

systematic, constantly updated and forward-looking analysis and assessment of the societal, economic and legal impact of the increased application of biometrics is needed. The further development of biometric technologies should be contingent on limiting their potentially harmful consequences for human rights.

62. Studies have shown a need for clarification in terms of biometric data since most of the existing legislation only addresses personal data in broad terms.[42] Although open to new developments, broad definitions enhance the risk of inadequate implementation and legal loopholes. The example of the European Union Council Regulation No. 2252/2004, which prescribes the introduction of biometric data in passports, shows that it is essential to clarify the terms and concepts used as soon as possible.

63. One of the key issues the Council of Europe has to work on is raising awareness concerning the right to respect for private life and its scope, including the rules on data protection. While most Europeans know that they have a right to privacy, which is most often also guaranteed by their national constitution, many are not aware of its full extent. Private issues are often not regarded as such unless the consequences of revealing private data are obvious. For a little more convenience and a small gain of time, too many people are willing to disclose personal information. Due to the fact that data bases can easily be interconnected and combined to generate a detailed identity profile, the right to privacy is highly at risk. Regulations are also needed to cover the use of biometrics by the private sector.

64. Thus the Council of Europe should update its Data Protection Convention and carefully follow the development of biometric technology in order to ensure that the legislation adequately meets new challenges. Clear definitions have to be found in terms of what is biometric data, what legislation covers such data and who is the data controller. Whenever data protection legislation is adopted, it has to be guided by the principles of transparency, consent and proportionality in order to satisfy not only security interests but also the privacy and dignity of the individual.

65. The importance of the proper balancing process cannot be stressed enough. Unfortunately, states tend to collect and store more information than is necessary, also for future, preventive use, as the recent complaint by two NGOs against the French regulation of biometric passports shows.[43] Therefore, there is still a lot to be done in terms of legislation, awareness-raising measures and scientific research.

---

42. Korff, D. and Brown, I. *New Challenges to Data Protection*, 2010, p. 2, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_summary_en.pdf.

43. Complaint by IRIS (*Imaginons un réseau internet solidaire*) and the *Ligue des droits de l'Homme*, www.ines.sgdg.org/IMG/pdf/recours-passeport0708.pdf. This regulation goes far beyond the European Union regulation, requiring eight fingerprints, to be stored in a central data base. The case has been pending before the courts for more than two years now and shows the delicacy of the issue and the difficulties courts and legislators face in order to strike the right balance.