COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

PROGRESS REPORT

ON THE APPLICATION OF THE PRINCIPLES

OF CONVENTION 108

TO THE COLLECTION AND PROCESSING

OF BIOMETRIC DATA

January 2014*

Directorate General Human Rights and the Rule of Law

Report by Prof. Dr. Paul de Hert and Koen Christianen LLM BSc, Tilbug University.
The document is an expression of the author's personal viewpoint

*Editorial revision 2020

Table of Content

Chapter 1. Introduction and structure of the report

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[1] asked the authors of this report to prepare a study on biometrics including an analysis of the Member States' current regulatory framework on the protection of biometric data. The aim of this progress report is to provide an update of the Council of Europe's 2005 progress report on the application of the principles of convention 108 to the collection and processing of biometric data.[2]

The authors of this report use the following definition of biometric data and biometrics: *Biometric data (or biometrics[3]) are measurable, physiological or behavioural characteristics that can be used to determine or verify identity. Biometrics is also defined as "the automated use of physiological or behavioural characteristics to determine or verify individuals".*[4]

In order to gain information on the use of biometric systems in relation to the principles of Convention 108, the 47[5] Council of Europe Member States were sent a 7 question questionnaire drafted by the authors of this report. 23 countries out of 47 responded to the questionnaire. Section 7.1 summarizes the answers of 22 countries – Portugal has been omitted from the report.[6] These 22 answers and the research conducted by the authors will allow the Consultative Committee to form an opinion on the application of the principles of Convention 108 regarding biometrics across the Council of Europe's Member States. The 7 questions of the questionnaire were:

Question 1: Does your country have regulation/legislation with regard to biometrics (i.e. biometric data and biometric systems)? If yes, please provide the regulation/legislation in English and in the native language.
Question 2: What is the state of the art of biometrics in your country? In other words, what are the latest biometric technologies?
Question 3: Could you please indicate what types of biometric systems are currently being used in your country and for which reasons, both in the public and the private sector?

[1] Convention for the protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ETS No. 108 (Convention 108), entry into force 1 October 1985, Council of Europe, available online at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
[2] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (hereinafter Progress Report 2005), Strasbourg 2005, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.
[3] The plural form of biometric.
[4] This is the most accurate definition according to the authors, although numerous definitions exist. For example, the Article 29 Data Protection Working Party in 2012 suggested the following definition for biometric data: 'biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability', see Opinion 3/2012 on developments in biometric technologies (WP 193), issued by the Article 29 Data Protection Working Party, and adopted on 27th April 2012, available online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
Biometrics are regularly considered to be 'unique' characteristics, although this is not always the case, as DNA samples of identical twins are not unique. DNA is not immediately machine readable, therefore this type of biometric data will not be discussed in this report. All other biometrics are thought to be unique, even both eyes of the same person or the eyes of identical twins, and the fingerprints on each finger of the same individual or the fingerprints of identical twins. See Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy? Opinion* (hereinafter Irish Council for Bioethics Opinion 2009), Dublin: The Irish Council for Bioethics 2009, available online at http://irishpatients.ie/news/wp-content/uploads/2012/04/Irish-Council-Bioethics-Final_Biometrics_Doc_HighRes.pdf. The uniqueness is also considered to apply to behavioural biometrics, although further research is needed to confirm this premise.
Definitions of biometric data sometimes contain the word 'physical' or 'biological', but in this report it is omitted in favour of the word 'physiological' since the latter comprises physical, biological and chemical phenomena, see Encyclopaedia Britannica Online.
Although biometric systems are employed for several purposes (e.g. security or law enforcement), all systems have one basic function, namely authentication, subdivided into verification and identification, which are both used in the authors' definition of biometrics.
[5] Including 3 CoE members not party to Convention 108: Russia, Turkey, and San Marino.
[6] Portugal did not want its responses to be published.

Question 4: What problems or difficulties do the public and private sector in your country encounter with regard to biometrics or the regulation/legislation regarding biometrics?
Question 5: Does your country have a central database for biometric data in either the public or private sector or is your country planning to set up such a database? If yes, for which purpose(s) and is it regulated?
Question 6: Have there been situations in your country, since 2005, in which biometric systems were hacked or compromised? If yes, please explain the situation.
Question 7: If, on a national level, research has been conducted regarding biometrics, please attach the report(s) of this research.

Chapter 7 of this report contains a structured representation of the country responses.
The report firstly addresses the main findings of the Council of Europe 2005 progress report, including its 12 recommendations (Chapter 2). We elaborate on recommendations 1, 2, 5, and 8 of this 2005 report, because they remain significantly important with regard to the Council of Europe's future legal framework on the processing of biometric data.
The report then discusses recent developments within the Council of Europe (Chapter 3) and the European Union (Chapter 4). Subsequently, the developments and concerns of new types of biometric technologies, the so-called second-generation biometrics, are discussed (Chapter 5). In a next chapter we discuss technical performances of biometric systems. All these systems encounter errors and threats (Chapter 6). This chapter also addresses questions about biometric template protection being one possible solution to protect biometric data.
The overview of the country reports including their main results (Chapter 7) is followed by the general conclusions and recommendations (Chapter 8).

Chapter 2. The Council of Europe's 2005 progress report on biometric technologies

The Council of Europe's 2005 progress report on the application of the principles of Convention 108 to the collection and processing of biometric data was the result of work commenced in 2003 by the Project Group on Data Protection (CJ-PD) under the aegis of the European Committee on Legal Co-operation (CDCJ) and, further to the restructuring of the data protection committees, pursued in 2004 and 2005 by the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD).[7] The foreword of the 2005 progress report mentions that "[*The T-PD] was very conscious of the complex nature of biometrics and of the necessity to adopt a position on the application of data protection to biometrics as a matter of urgency, in order to contribute to the on-going debate and biometrics projects under way both at national and international level. For these reasons, the T-PD decided to prepare a progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*". Due to evolving technologies yielding new biometric possibilities and legal challenges the 2005 progress report needed an update.
The 2005 progress report contains 12 recommendations that we reproduce in Annex A of this report. In what follows we discuss the most relevant recommendations of the 2005 progress report. They require particular attention in this update of the progress report, because of the developments in biometric technology. For this reason, recommendation 1, 2, 4, 5, 8 and 10 are specifically addressed.

Recommendation 1 of the 2005 Council of Europe progress report: biometrics as sensitive data

The first recommendation states that biometric data should be regarded as 'a specific category of data' with the following argument: "*as they are taken from the human body, remain the same in different systems and are in principle inalterable throughout life*". Academic legal scholars and several reports tend to emphasize the importance of designating biometric data as sensitive data in European data protection legislation. Currently, biometric data are not yet considered sensitive personal data in Convention 108. As will be seen in the seventh chapter on the country responses, very few countries categorize biometric data as a special category of personal data. It is currently unclear what the precise consequences of such a categorization will be. Defining biometric data as sensitive personal data by default may result in imposing the very stringent requirements for the processing of such sensitive data for many basic applications. We will come back to this in chapter 4.

Recommendation 2 of the 2005 Council of Europe progress report: employ less intrusive alternatives for biometrics

Recommendation 2 states that controllers of biometric systems should consider possible alternatives that are less intrusive for private life. The idea to employ less intrusive alternatives for biometric systems if reasonably possible can be linked to Article 5 of Convention 108. Some DPAs apply Recommendation 2, but unfortunately not all of them.

[7] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* ('Progress Report 2005'), Strasbourg 2005, 3, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf.

Recommendation 4 of the 2005 Council of Europe progress report: function creep and surveillance

Recommendation 4 notices the risk of function creep. This means that (biometric) data originally collected for one specific purpose is subsequently used for another purpose without the explicit consent of the data subject. This poses a significant risk to the data subjects' data protection rights. The development of new biometric technologies (so called second generation biometrics) may give rise to covert authentication of which data subjects are not aware. If data subjects are not aware of the collection of their biometric data, the controllers of the biometric system may process these data (also) for illegitimate purposes. The risk of function creep is addressed in chapter 5 and chapter 6.

Recommendation 5 of the 2005 Council of Europe progress report: templates rather than actual biometrical data

Recommendation 5 states that biometric templates should be used instead of raw biometric data. This is a significant statement. Once raw biometric data is compromised, it cannot be used anymore as a method of authentication (subdivided into identification and verification) by the data subject. In comparison with conventional security methods (e.g. using a password or PIN), biometric characteristics are not revocable and cannot be reissued. Therefore, academic research is mainly focused on the protection of biometric templates. Once a biometric template is compromised, a new biometric template of the same original biometric feature (e.g. fingerprint) can relatively easy be generated. Converting raw data into templates is therefore regarded as more respectful of data protection principles.[8] Templates do the job of identification and subsequent processing and data mining as good as raw data. Once processed, there is no further need to store this actual biometric data. [9]
The country responses show that almost no data protection legislation and Data Protection Authority touches upon this possibility to strengthen the data protection framework for biometrics. See *below* chapter 3, section 1.

Recommendation 8 of the 2005 Council of Europe progress report: information and consent of the individual

Recommendation 8 states that the data subject should be informed about the purpose(s) of processing, the controller's identity, the personal data that are processed, and the parties to which the data will be disclosed when necessary. These are important requirements for controllers of biometric systems, particularly with regard to current developments in biometric technologies. At present, covert and distant authentication of data subjects is possible, as will be discussed in chapter 5, which is a serious concern. Biometric characteristics of people can be captured from a distance and on the move, allowing the data subject's authentication without his consent. A data subject should know whether biometric characteristics are being collected and processed.

Recommendation 10 of the 2005 Council of Europe progress report: security provisions

Recommendation 10 addresses the need for technical and organisational measures to protect biometric data against accidental or deliberate deletion or loss, as well as against illegal access,

[8] See also Pospisil R. & Skrob M., 'Actual trends in improvement of risk area security using combined methods for biometrical subject identification', *European Journal of Law and Technology*, Vol. 4, No. 2, 2013, (10p.), 2
[9] See also chapter 6 where we discuss the method of biometric template protection in order to protect the data subject's biometric data.

alteration or communication to unauthorised persons or any other form of illegal processing. As mentioned above under “recommendation 5” in this subsection, template protection can be a technical measure to tackle these potential risks. An elaborate overview of impostor threats and other additional threats are discussed in chapter 6.

In a next chapter we turn to recent reports of and developments within the Council of Europe after 2005.

Chapter 3. Recent developments within the Council of Europe

3.1. The Council of Europe's 2011 Parliamentary Assembly report

General

On 5 October 2006, the Parliamentary Assembly decided to refer to the Committee on Legal Affairs and Human Rights for a report on the motion for a recommendation on the need for a global consideration of the human rights implications of biometrics.[10] The Committee, *de facto* acting as the Assembly's legal adviser, appointed Holger Haibach rapporteur. Mr Haibach's report was published in February 2011.[11] The report notes that the Committee has been increasingly concerned about the rapid and uncontrolled development of biometric technologies. In the opinion of the Committee, the European legal framework regarding the use of biometric data remains vague. The Parliamentary Assembly therefore strongly believes that the Council of Europe should take steps to ensure that this legal framework is enhanced and modernised.[12] The 2011 report contains recommendations to both Council of Europe Member States and the Committee of Ministers. These will be discussed in the next two paragraphs.

The Assembly's recommendations to Member States (part 1 of the 2011 report)

The 2011 report states that due to the events of 11 September 2001, security issues have become a major concern at global level. They resulted in an ongoing search for secure and reliable methods of identification and verification through the use of the intrinsic physiological characteristics of a human being through the use of biometrics. According to the report, the use of biometrics may offer a solution to various security concerns, but it also engages several human rights. The Parliamentary Assembly is of the opinion that security has to be properly balanced against the protection of human rights. This balance is not yet appropriately reflected in Member States' legislation, according to the it.[13] The Council of Europe Member States should therefore take further measures to improve the current European legal framework regarding biometrics. Rapporteur Mr Haibach advised Member States to adopt specific legislation in this area and to produce a standardized definition of biometric data. Unfortunately, as will be seen in Section 7 on country responses, few countries have adopted specific legislation with regard to biometrics. The following suggestions of the Assembly for the Member States remain considerably relevant and important (emphasis added):

---

[10] Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Motion for a recommendation, Doc. 11066, available online at http://assembly.coe.int (search for Doc. 11066), Council of Europe 2006.

[11] Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Doc. 12522 (hereinafter Parliamentary Assembly Report 2011), available online at http://assembly.coe.int (search for Doc. 12522), Council of Europe 2011. The Assembly's recommendations to Member States are contained in its Resolution 1797 (2011), see Parliamentary Assembly, *The need for a global consideration of the human rights implications of biometrics*, Resolution 1797 (2011), available online at http://assembly.coe.int (search for Resolution 1797 (2011)), Council of Europe 2011.

[12] Parliamentary Assembly Report 2011, 3, par.3.

[13] See Parliamentary Assembly Report 2011, 3, par.1 and par.2:
par.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).'
par.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.'

- 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: 1) elaborate a standardised definition of "biometric data"; and 2) revise the existing regulations concerning general protection of personal data by adjusting them to current applications of enhanced biometrical technologies;

- 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;

- promote proportionality in dealing with biometric data, in particular by: 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; 2) providing individuals who are unable or unwilling to provide biometric data with alternative methods of identification and verification; 3) working with template data instead of raw biometric data, whenever possible; 4) enhancing transparency as a pre-condition for meaningful consent and, where appropriate, facilitating the revocation of consent; 5) allowing individuals access to their data, and/or the right to have it erased; 6) providing for appropriate storage systems, in particular by reducing central storage of data to the strict minimum; 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;

- - 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;

- - strengthen the compliance of private sector applications of biometrics with existing data protection law, especially by: 1) ensuring accountability of data controllers; 2) promoting the training of relevant actors in the appropriate handling of personal data;

- 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;

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

The 2011 report contains more recommendations than the 2005 report. They are also made more concrete. The 2011 report highlights that Council of Europe Member States *"[…] should adopt specific legislation in [the area of biometrics], produce a standardised definition of "biometric data", put in place supervisory bodies and promote multidisciplinary research."* The country reports (discussed in chapter 7) demonstrate that currently very few countries have legislation specifically aimed at biometrics. Therefore, this recommendation of the 2011 report remains relevant.

Unlike the 2005 progress report, the 2011 report addresses the need for a standardised definition of biometric data.[14] The responses of 22 countries show that very few countries have adopted legislation specifically aimed at the protection of biometric data.[15] Georgia and Montenegro are the only two countries which have adopted a definition of biometric data. In Georgia biometric data is defined as "*any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person*". In Montenegro biometric data is defined as "*data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly".*

The 2011 report specifically addresses second generation biometrics.[16] In 2005, these biometrics were in the development phase. Second generation biometric technologies include those enabling covert authentication through capturing biometric features from a distance and on the move, without the data subject's awareness and consent. This poses risks to the data subjects' data protection rights. None of the country reports addresses second generation biometrics.

The 2005 and 2011 reports both recommend alternative methods for biometric systems that are less intrusive for private life, although the 2011 report specifically addresses the need for alternative methods of identification and verification to be provided to individuals who are unable or unwilling to provide biometric data. The concept of subsidiarity is addressed in the Monaco country report.[17] During an investigation conducted on 14 March 2011, staff of the Monegasque Data Protection Authority noted the existence of an unsecured central database for fingerprints for which no approval had been granted. The use of the biometric system was stopped at the request of the Data Protection Authority.

The 2005 and 2011 report both recommend the use of templates instead of raw biometric data. The country reports show that very few countries address the need to use templates. Mr Haibach's recommendations regarding the use of templates have been noticed only in Estonia and Italy. The Estonian report underlines the importance to use biometric templates instead of raw biometric data.[18] The Italian DPA thinks that biometric data require specific precautions to prevent harming data subjects. For example, the storage of encrypted templates exclusively held by the data subject should be preferred to storage in central databases. Data protection legislation should include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.

The 2005 and 2011 report both address the need for provisions in data protection legislation containing the requirement that biometric data are only to be used for the purposes for which they have been lawfully collected. Due to the development of second-generation biometric technology enabling advanced capabilities of covert collection of biometric this requirement is even more important to prevent function creep.

[14] A short and proper definition of biometric data already mentioned in the introduction to our report: 'biometric data are measurable, physiological or behavioural characteristics that can be used to determine or verify identity'
[15] See chapter 7 for the analysis of country reports mentioning the adoption of legislation specifically aimed at biometric data.
[16] Chapter 5 elaborates on second generation biometrics.
[17] See chapter 7 for the Monegasque response to the questionnaire.
[18] See chapter 7 for the Estonian response to the questionnaire.

Unlike the 2011 report, the 2005 report includes the recommendation (Recommendation 1) to define biometric data as a specific category of data. This is a recommendation worthy of consideration and underlines the vulnerability of biometric data. The country reports show that few countries have adopted legislation defining biometric data as a specific category of personal data. In Estonia biometric data is considered sensitive personal data.[19] In Georgia and the former Yugoslav Republic of Macedonia[20] biometric data is considered a special category of personal data.[21]

The Assembly's recommendations to the Committee of Ministers (part 2 of the report)

The 2011 report contains not only recommendations to Council of Europe Member States but recommendations to the Committee of Ministers as well.[22] 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, particularly by adopting Convention 108 and through the work of its Consultative Committee.[23] For the Assembly, "*[t]he Council of Europe is therefore well placed to promote the adoption at the European level of rules on the use of biometrics*".[24] The country reports (discussed in chapter 7) demonstrate that currently very few countries have legislation specifically aimed at biometrics. Therefore, the following recommendations to the Committee of Ministers remain relevant and important (emphasis added):

- 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";
- 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;
- 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.

The country reports show that only 7 in 22 countries that responded to the questionnaire have adopted legislation and regulation specifically aimed at the protection of biometric data. These countries are (in alphabetical order) **Estonia**, **France**, **Georgia**, **Italy, the former Yugoslav Republic of Macedonia**, **Montenegro** and **Slovenia**.[25] France and Georgia are pioneering the field of data protection in general and biometric data in particular.[26] The processing of biometric data is regulated in French and Georgian data protection law. France has strict regulation and, since 2004, has specific doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. The Georgian data protection act contains several articles regulating the processing of biometric data in particular.

---

[19] See chapter 7 for the Estonian response to the questionnaire.

[20] As of February 2019, the official name of the country changed to North «Former Yugoslav Republic of Macedonia».

[21] See chapter 7 for the Georgian response to the questionnaire. See chapter 7 for the former Yugoslav Republic of Macedonia in response to the questionnaire.

[22] The Assembly's recommendations to the Committee of Ministers are also contained in its Recommendation 1960, see Parliamentary Assembly of the Council of Europe, *The need for a global consideration of the human rights implications of biometrics*, Recommendation 1960 (2011), (hereinafter Parliamentary Assembly Recommendation 2011), available online at http://assembly.coe.int (search for Recommendation 1960 (2011)), Council of Europe 2011.

[23] Parliamentary Assembly Report 2011, 5, par.1.

[24] Parliamentary Assembly Report 2011, 5, par.1.

[25] See chapter 7.

[26] *Ibid.*

In the authors' opinion the 2011 Parliamentary Assembly's report captures all the main issues of the current legal debate on biometrics. The report contains many creative policy ideas regarding the regulation of biometrics. The central message is that additional regulatory measures, either soft law or hard law, need to be implemented in order to keep pace with developments in biometric technology and to harmonise the biometric legal framework across the CoE Member States. Data protection legislation should for example include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. The 2005 and 2011 report both recommend the use of templates instead of raw biometric data. Unfortunately, the country reports show that only Estonia and Italy have taken note of, and implemented, this recommendation. Regulatory initiatives should also include a correct and useful definition of 'biometric data'. Chapter 7 on the country responses shows that very few countries have adopted legislation specifically aimed at the protection of biometric data. Georgia and Montenegro are the only two countries which have adopted a definition of biometric data. France and Georgia are pioneering the field of data protection in general and biometric data in particular.

3.2. The Consultative Committee's modernisation work of Convention 108

Currently, the Council of Europe Consultative Committee is working on a modernisation of Convention 108.[27] [28] The Committee recently finalised the first stage of the modernisation work of the Convention, and proposed a new text.[29] This modernisation proposal of Convention 108 was adopted in November 2012 by the 29th plenary meeting of the Committee. The new article 6 on the processing of sensitive data includes a provision concerning biometrics.[30] It states that the processing of biometric data uniquely identifying a person shall only be allowed where the applicable law provides appropriate safeguards. These shall prevent the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. By means of this proposal the Committee categorizes biometric data as sensitive personal data, in order to particularly protect biometric data. However, it is not clear what the consequences of such a categorization are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that distinction can no longer be made between more and less intrusive types of biometric processing. Moreover, in the Marper judgment, to be discussed in the next chapter, the European Court of Human Rights states that not all biometric data should be treated equally.

In its 2013 draft explanatory report, the Consultative Committee states that it identified already in 2009 several angles of potential work on the Convention, such as technological developments

[27] The Consultative Committee was set up by virtue of Article 18 of Convention 108.
[28] Convention 108, Article 19 in conjunction with Article 21.
[29] The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Modernisation of Convention 108* (hereinafter Modernisation Proposal 2012), Strasbourg: Council of Europe 2012, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf.
[30] The new Article 6 reads as follows:
1. The processing of genetic data, of personal data concerning offences, criminal convictions and related security measures, the processing of biometric data uniquely identifying a person, as well as the processing of personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where the applicable law provides appropriate safeguards, complementing those of the present Convention.
2. Appropriate safeguards shall prevent the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

and information to be provided to the data subject.[31] As biometric technologies evolve quickly a major privacy concern of biometric recognition technologies is the advancing capability of capturing biometric features from a distance and on the move, which may allow for covert authentication. In such a case, the data subject is not aware of being identified by a biometric system, and probably did not give permission to collect biometric data, while a legitimate purpose for this collection may also be lacking. Convention 108 lacks criteria for the legitimate processing of data in general and the legitimate processing of biometric data in particular. One such criterion should be the explicitly given informed consent of the data subject.

The draft explanatory report categorizes biometric data as sensitive data if it enables the identification of an individual. Paragraph 54 of the Report reads as follows: *"The processing of biometric data uniquely identifying a person (data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter) is also considered sensitive per se. This does not imply that all processing of 'biometric data' (such as pictures for instance) is to be considered as a sensitive processing but solely the processing which will enable the unique identification of an individual*."

Paragraph 56 of the Explanatory Report mentions the importance to prevent potential risks (e.g. discrimination or injury to an individual's dignity or physical integrity) by means of employing *"[…] appropriate safeguards (which are adapted to the risk at stake), such as the data subject's consent, a risk analysis or a statutory regulation of the intended process ensuring the confidentiality of the data processed".*

The same remarks regarding the 2012 modernisation proposal apply to the 2013 draft explanatory report. Caution should be exercised when biometric data are considered sensitive personal data. It is not clear what the consequences of such a categorisation are.

The importance of the data subject's consent and a risk analysis are evident, but second generation biometrics (Chapter 5) creates new legal challenges. New biometric technologies are capable of capturing biometric features from a distance and on the move, whilst the data subject remains unaware of their operation. This poses significant risks for the individual's rights and freedoms.

In the 2012 modernisation proposal of Convention 108, drafted by the Council of Europe's Consultative Committee of Convention 108, the new Article 6 on the processing of sensitive data includes a provision concerning biometrics. By means of this proposal the Committee categorizes biometric data as sensitive personal data. The 2013 draft explanatory report of the Consultative Committee includes the same categorisation, although it is not clear what the consequences of such a categorization are. It may imply that no longer a distinction can be made between more and less intrusive types of biometric processing. In the *Marper* judgment, to be discussed in the next sections, the European Court of Human Rights states that not all biometric data should be treated the same, because not all types of biometric data are equally intrusive. This strengthens the idea that research must be conducted on the consequences of biometric data as a specific category of sensitive personal data prior to the introduction of a new article 6 in Convention 108.

[31] Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD-BUR), *Draft explanatory report of the modernised version of Convention 108* (hereinafter Draft Explanatory Report 2013), Strasbourg: Council of Europe 2013, available online at http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD-BUR(2013)3_EN%20draft.pdf.

3.3. The European Court of Human Rights: recent case law on biometrics

Marper (2008) and Schwarz v. Stadt Bochum (2013): biometric data are protected by the right to privacy

A crucial judgement in relation to the challenges of large-scale databases containing personal information was pronounced by the European Court of Human Rights is *S. and Marper*.[32] The proceedings concerned two non-convicted individuals who wanted to have their records removed from the DNA database used for criminal identification in the United Kingdom.[33] More concretely, they asked for their fingerprints, cellular samples and DNA profiles, which had been obtained by police, to be destroyed.[34]

The Court held that there had been a violation of Article 8 as the retention of the fingerprints, cellular samples and DNA profiles of two persons who have been suspected, but not convicted of criminal offences is regarded as a disproportionate interference with those persons' right to respect for private life under Article 8 of the ECHR. The Court noted that "*all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Council of Europe data protection convention*[35] *as they relate to identified or identifiable individuals."*[36]

Although the Court recognised that fingerprints do not contain as much information as either cellular samples or DNA profiles, it stated that "*fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life".*[37]

This finding is echoed in *Peruzzo and Martens* (*below*) and in *Schwarz v. Stadt Bochum* a judgment of the European Court of Justice.[38] In *Schwarz* the Court of Justice, referring to *Marper*, accepts that fingerprints and iris scans are protected both under the right to privacy and the right to data protection both explicitly protected by the 2000 EU Charter on Fundamental Rights,[39] *but* it adds the remark that collecting fingerprints *and* collecting facial images are no major privacy intrusions since fingers and faces are public.[40] This finding then paves the way,

---

[32] ECtHR, Judgement of 4 December 2008; *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04 (hereinafter, *'Marper'*).

[33] As criminal proceedings against them had ended with an acquittal or had been discontinued (*Marper*, par. 3).

[34] The applicants based their application on Articles 8 and 14 ECHR.

[35] Convention for the protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ETS No. 108 (Convention 108), entry into force 1 October 1985, Council of Europe.

[36] *Marper*, par. 68.

[37] *Marper*, par.78 & 84.

[38] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*). This judgement on the European Passport system will be discussed in chapter 4.

[39] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 24-30: '(par. 24:) Article 7 of the Charter states, inter alia, that everyone has the right to respect for his or her private life. Under Article 8(1) thereof, everyone has the right to the protection of personal data concerning him or her. (par. 25:) It follows from a joint reading of those articles that, as a general rule, any processing of personal data by a third party may constitute a threat to those rights. (par. 26:) From the outset, it should be borne in mind that the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual (Joined Cases C- 92/09 and C- 93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I- 11063, paragraph 52, and Joined Cases C- 468/10 and C- 469/10 *ASNEF and FECEMD* [2011] ECR I- 12181, paragraph 42). (par. 27:) Fingerprints constitute personal data, as they objectively contain unique information about individuals which allows those individuals to be identified with precision (see, to that effect, in particular, ECtHR judgment in *S. and Marper v. United Kingdom*, par. 68 and 84, ECtHR 2008). (par. 28:) In addition, as can be seen from Article 2(b) of Directive 95/46, processing of personal data means any operation performed upon such data by a third party, such as the collecting, recording, storage, consultation or use thereof. (par. 29:) Applying Article 1(2) of Regulation No 2252/2004 means that national authorities are to take a person's fingerprints and that those fingerprints are to be kept in the storage medium in that person's passport. Such measures must therefore be viewed as a processing of personal data. (par. 30:) In those circumstances, the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation No 2252/2004 constitutes a threat to the rights to respect for private life and the protection of personal data. Accordingly, it must be ascertained whether that twofold threat is justified'.

[40] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 48: 'In this respect, it is be borne in mind, on the one hand, that that action involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken.'

as we will see in chapter 4, to a balancing act under the proportionality test in favour of state interest.
The argument behind the finding of the ECJ is problematic in at least two regards. First, intimacy is not the final test to judge the intensity of an intrusion with regard to the right of privacy. The ECtHR has adopted a broad approach to the privacy right including next to intimacy other areas of topical interest such as sexual freedom, identity, and protection against surveillance,[41] having brought the scope of protection of the right to privacy far beyond intimacy. Second, the ECJ itself finds that fingerprinting and iris scanning affects not only the right to privacy, but also the right to have personal data protected. This right has been developed next to the privacy right to protect personal data even when this is not privacy relevant. The right seeks to protect the citizens against having their data processed by others by imposing duties such as security and proportionality and by granting the affected citizen certain important control rights over processing of their personal data. Intimacy plays a role in the case of fingerprinting, since states now require something of ordinary citizens that used to be 'asked only' to criminals and specific targeted groups. Apart from that, intimacy is not the real data protection problem here: it is the scale of the system, the error rate, the fact that other countries only use iris biometrics in their passports and do not require fingerprints, the possibility of using a biometrical database for surveillance and other purposes, etc. To marginalise biometrics as only a minor problem of privacy and data protection seems unreasonable. We will come back to this point in chapter 4 but return here to the case law of the European Court of Human Rights.

The European Court of Human Rights noted in *Marper* that fingerprints, DNA profiles and cellular samples constitute personal data within the meaning of Convention 108 and are protected by Article 8 of the ECHR, but it distinguishes fingerprints from cellular samples and DNA profiles: because of the information they contain, the retention of cellular samples and DNA profiles has a more important **impact on private life** than the retention of fingerprints.
In the Court's judgment one can find an argument not to label all biometric data as sensitive personal data. It is not clear what the consequences of such a categorisation are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that no longer a distinction can be made between more and less intrusive types of biometric processing.
The Court also considers that states which claim to be pioneers in the development of new technologies bear special responsibility for striking the right balance between biometric data retention and the right to respect for private life. In the opinion of the authors of this report it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a **privacy impact assessment**. Such an obligation is provided in the proposed Data Protection Regulation, but it is not mentioned in the proposed Data Protection Directive.

Marper (2008): biometrics and the proportionality requirement

In *Marper* the Court established that it is contrary to the requirements of Council of Europe European Convention of Human Rights[42] to store for unlimited periods of time that type of personal information related to innocent people in such a database.[43] It concluded that the

[41] See for a discussion: A. Galetta & P. De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review*, 2014, Vol. 10, No. 1, 55-75.
[42] Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November.
[43] As such storage represents an interference with the right to respect for private life established by Article 8 of the ECHR (*Marper*, par. 77 and par. 86) that cannot be judged proportionate.

blanket and indiscriminate nature of the powers granted to UK authorities constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered as necessary in a democratic society,[44] amounting therefore to a violation of Article 8 of the ECHR.[45]
The Court also considers that any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance between the retention of biometric data and the right to respect for private life.[46] As stated above, in the opinion of the authors of this report it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a privacy impact assessment[47]. Such an obligation is provided in the proposed regulation, but it is not mentioned in the proposed directive.[48]

The general principles for proportionality testing are spelled out in par. 101 and 102 of the *Marper* judgment:

> An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are *relevant and sufficient*.[49] Since the outcome of this test is never given beforehand, it is understood that national authorities make the initial assessment in all these respects, with a final evaluation by the Court.[50]
> States are given a margin of appreciation in this assessment that depends on a number of factors including:
> - the nature of the Convention right in issue;
> - its importance for the individual;
> - the nature of the interference and
> - the object pursued by the interference.[51]
> The margin will tend to be narrower where the right at stake is crucial for the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the state will be restricted. Where, however, there is no consensus within the states, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider.[52]

We have demonstrated elsewhere that there is no rigid set of 'general principles' with regard to testing limitations to Article 8 of the ECHR. In other judgments the Court applies a loose proportionality test, avoiding or omitting certain 'principles', in other cases more 'principles' are taken into consideration, often, but not always leading to more scrutiny of the state in question.[53] The proportionality test of *Marper* is copied faithfully in *Peruzzo and Martens* (discussed *below*).[54] Although reference is made to *Marper* we find a shortened set of *Marper*-

[44] *Marper*, par. 125.
[45] Art. 8 of the ECHR states: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.
[46] *Marper*, par. 112.
[47] A privacy impact assessment is sometimes termed otherwise, for example data protection impact assessment.
[48] Chapter 4 elaborates on the proposed regulation and proposed directive of the European Union.
[49] *Marper*, par. 101.
[50] *Marper*, par. 101.
[51] *Marper*, par. 102.
[52] *Marper*, par. 102, with ref. to see *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECtHR 2007; *Dickson v. the United Kingdom* [GC], no. 44362/04, § 78, ECtHR 2007; *Connors v. the United Kingdom*, no. 66746/01, § 82, 27 May 2004, with further references)
[53] A. Galetta & P. De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance', *Utrecht Law Review*, 2014, Vol. 10, No. 1, 55-75.
[54] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 41.

principles in of *M.K. v. France* (discussed *below*),[55] but then a long exposé on the need for legal safeguards that ensure pertinence of the data, proportionality and non-excessiveness etc.
In the 2013 judgment of the Court of Justice of the European Union, *Michael Schwarz v. Stadt Bochum*, the principles for testing necessity or proportionality are appropriateness, availability of less intrusive alternatives and the existence of legal guarantees to protect against misuse and abuse (see *below*).

In practice we note that within the framework of proportionality testing, the Court will, once it has found a technology useful for a certain legitimate purpose (for instance crime fighting), concentrate on the presence of safeguards to prevent authorities to go for blanket and indiscriminate taking and retention of biometrics or to prevent misuse or long storage.
This verification of safeguards seems to be a safer activity for the judges than asking straight proportionality questions about for instance appropriateness or availability of less intrusive alternatives.
Illustrative for this fix on criteria and principles that have more to do with the legality requirement under Article 8 ECHR, than with the proportionality requirement under Article 8 of the ECHR, is par. 31 of *M.K. v France* (only available in French) where the Court states that in the present case the legality test and the proportionality test largely overlap since they both center around checking legal safeguards.[56]

Peruzzo and Martens v. Germany & M.K. v. France (2013): more on proportionality

Peruzzo and Martens v. Germany, a 2013 a judgment on DNA sampling in the area if criminal law, allows us to better understand the proportionality test with regard to use of DNA.[57] The case was brought before the ECtHR by two individuals that were subjected to an 'Article 81g procedure'.[58] Pursuant to Article 81g of the code of criminal procedure, a procedure can be launched before the German courts, outside pending criminal proceedings, and this at the prosecution authorities' request with a view to determining the applicants' DNA profiles for use in possible future criminal proceedings.[59] The two applicants complained that the taking and retention of DNA material for the purpose of establishing their identity within the scope of potential future criminal proceedings constituted an inadmissible and disproportionate interference with their right to informational privacy (*informationelles Selbstbestimmungsrecht*).
The ECtHR first had to deal with a legal-technical question about the clarity and foreseeability of German law.[60] The Court then turned to the proportionality check and found that two sets of

[55] The court insist on a "pressing social need" and, in particular, on the requirement that the interference is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are *relevant and* sufficient. Cf. ECtHR, Decision of 18 April 2013, *M.K. v. France*, applications nos. 7841/08 and 579000/12, with ref. to *Marper*, par. 101.
[56] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 31: "En l'espèce, la Cour constate que l'ingérence est prévue par la loi, à savoir l'Article 55-1 du code de procédure pénale et le décret no 87-249 du 8 avril 1987 modifié. Quant à la question de savoir si la législation en cause est suffisamment claire et précise s'agissant des conditions de mémorisation, d'utilisation et d'effacement des données personnelles, la Cour note que le requérant évoque ces problèmes dans le cadre de ses développements sur la proportionnalité de l'ingérence. En tout état de cause, elle estime que ces aspects sont en l'espèce étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique et qu'un tel contrôle de la « qualité » de la loi dans la présente affaire renvoie à l'analyse ci-après de la proportionnalité de l'ingérence litigieuse (S. et Marper, précité, § 99)".
[57] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, application no. 19522/09, par. 33 with reference to *Marper*, par. 101.
[58] Peruzzo, the first applicant, had been convicted of several drug-related offences when a district court ordered cellular material to be taken from him with a view to determining his DNA profile for identification purposes in any future criminal proceedings. This decision was reached in view of the seriousness of the offences he had committed and his negative criminal prognosis. In the case of Martens, the second applicant, a district court ordered the taking of DNA samples on account of his repeated commission of violent offences
[59] The purpose of this power is to collect DNA profiles of potential recidivist for identification purposes on the occasion of future criminal proceeding. The procedure can be launched outside any pending procedure.
[60] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 38. Both applicants argued that the notion of "criminal offences of considerable significance" employed in Article 81g of the code of criminal procedure referred to an undetermined legal concept that was open to interpretation. It was not sufficiently clear and foreseeable what type of criminal offences fell within the ambit of the provision and the

safeguards were absent in *Marper* and elaborated appropriate safeguards to prevent any use of personal data inconsistent with the guarantees of Article 8:[61] *firstly*, under the German law, DNA records can only be taken, stored and retained from persons who are convicted of serious criminal offences and are likely to be the subject of criminal proceedings in the future. In the case of the applicants, the German courts had ordered the measure only after a *concrete* study of each case and had provided relevant and sufficient reasons for their assumption that new criminal investigations might one day follow. The Court notes that in *Marper* it found DNA records of applicants who had not been convicted of a criminal offence an infringement. *Secondly*, there are appropriate safeguards in German law and in practice that limit the risk of blanket and indiscriminate taking and retention of DNA samples, misuse or abuse.[62] The Court notes that, in *Marper*, it found a system of blanket and indiscriminate nature of the power of retention of DNA records without limit of time and irrespective of the nature or gravity of the offence or the personal circumstances of the individual concerned.

In *M.K. v. France*, of the same year, the Court looked at a complaint by a French national about the fact that his fingerprints had been retained on a database by the French authorities and so based on the French code of criminal procedure, a 1987 decree and a 2006 '*ordonnance*'. In the past, the applicant had been the subject of two investigations concerning book theft, which ended in one case with his acquittal and in the other with a decision not to prosecute. In 2006 the applicant wrote to the public prosecutor requesting the removal of his fingerprints from the database, but this request was granted only in relation to the fingerprints taken during the first set of proceedings. M.K. turned to the European Court of Human Rights and complained that the retention of data concerning him in the computerised database of fingerprints had infringed his right to respect for his private life. He also alleged a violation of Article 6.
As written *above* the Court will under Article 8 of the ECHR insists, in its discussion of general principles, on the need for legal safeguards ensuring that stored data by police is relevant and not excessive in relation to the purposes for which they were stored and where checks are built in on the length of time for which they were retained. These safeguards are needed because the data is stored in databases *and* used for policing purposes **and** there is a risk for stigmatisation as the database comprises data on non-convicted persons.[63]
Reviewing the French law and the facts of the case, the Court will find that the retention of the data in question amounted to disproportionate interference with the applicant's right to respect his private life and that France had gone beyond the margin countries were to have in these matters

With regard to the collection of the data the Court notes that:
- the French public prosecutor had refused removal of the fingerprints with the argument that storage was in the interest of M.K. and would protect him against identity theft. In the Court's

resulting interference had thus not been "prescribed by law" within the meaning of Article 8 § 2. The Court, after having found similar terms in other provisions of German law, admits that the definition may give rise to interpretation, but makes it nevertheless foreseeable for an individual that a conviction for repeated drug trafficking accompanied by illicit importation of drugs triggering a prison sentence of over five years (as was at issue in the first applicant's case) and convictions for violent crimes and stalking (as was at issue in the second applicant's case), constitute a crime of at least medium gravity and may consequently give rise to a court order pursuant to Article 81g of the Code of Criminal Procedure.

[61] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 44-50.

[62] Pursuant to Article 81g of the Code of Criminal Procedure any cellular material obtained is to be used only for the purpose of establishing a DNA profile. The identity of the individual from whom the sample is obtained cannot be disclosed to the experts in charge with drawing up the profile. These experts are furthermore under an obligation to take adequate measures to prevent any unauthorised use of any material examined. The cellular material itself must be destroyed without delay once it is no longer needed for the purpose of establishing the DNA profile. Only the DNA profiles extracted from the cellular material can be kept in the Federal Criminal Police Office's database and then only for a maximum of ten years, subject to regular review.

[63] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 35 and 36.

view, that argument, which moreover had no basis in legislation, could end up justifying a measure as extreme as storing the details of the entire population. [64]
- the main point of critique of the Court regarded the 1978 Decree. This text allows collection and storage not only to facilitate the prosecution of suspects involved in criminal proceedings and needing to be identified, but also allowed collection and storage of persons to facilitate cases in the hands of the judicial authorities and of persons implied in a criminal procedure (without being suspected) when identification of these persons was necessary. This second and third ground for collection and storage were phrased too broadly, not being limited to criminal offences and could again, end up justifying a measure as extreme as storing the details of the entire population. [65] In addition, it did not make any distinction based on the seriousness of the allegations, and the present case showed that the system also allowed collection and storage for minor offences.
- in addition, the Decree applied indiscriminately to persons who had been convicted and those who, like the applicant, had never been found guilty of an offence, and were therefore at risk of being stigmatised, irregardless of their right to be presumed innocent.[66]

With regard to the storage of the data the Court notes that:
- the right to erase the data laid down in the 2006 '*ordonnance*' is balanced in favour of the law enforcement authorities that are said to need the broadest database possible, which makes a right to erase theoretical and illusory.[67]
- a maximum length of time was built in but was set at 25 years. Taken together with the illusory right to demand erasure, this creates a system with retention for an indeterminate period.[68]

The Court therefore concluded that the French courts had overstepped their margin of appreciation and had failed to strike a fair balance between the public and private interests at stake.

Biometrics, precaution and the presumption of innocence
Discussing *Marper*, we saw that the European Court of Human Rights understands the risk of stigmatisation caused by retention of (biometrical) data in a database, [69] explaining in its finding that the storage of such data, when related to non-convicted or to minors, has to be limited.[70]
This is far from a principled rejection of use of (stored) biometric data in criminal law under any circumstances. On the contrary. In *Peruzzo and Martens*, the Court notes that in recent years DNA records had made a substantial contribution to law enforcement and the fight against crime.[71] What is needed is a balancing act, since too much storage infringes on the protection of personal data of fundamental importance for the enjoyment of the right to respect for private life. The specific procedure in *Peruzzo and Martens* seems to respect this requirement of balancing and explains the finding of the Court that the domestic German rules on the taking and retention of DNA material from persons convicted of offences reaching a certain level of gravity as applied in the case of the applicants had struck a fair balance between the competing

[64] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 40.
[65] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 41.
[66] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 42.
[67] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 44.
[68] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 45.
[69] *Marper*, par. 122. Moreover, the Court highlighted that the stigmatisation can be especially harmful when minors are concerned (ibid., par. 124).
[70] The judgment reviews different national approaches in Europe to the taking and retention of DNA information in the context of criminal proceedings, and notes that the UK is the only Council of Europe Member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.
[71] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 42.

public and private interests and fell within the respondent State's acceptable margin of appreciation.[72]

Hence a balanced approach to DNA sampling is proportional *and* serves a legitimate purpose within the meaning of the second paragraph of article 8 ECHR. The Court addresses the legitimacy requirement under Article 8 of the ECHR in par. 40:

> Concerning the legitimate aim served by the impugned measure, the Court has previously held that the compilation and retention of DNA profiles serve the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others (see S. and Marper, cited above, § 100). While the Federal Constitutional Court in its decision of 14 December 2000 held that the measures permitted under article 81g of the Code of Criminal Procedure did not aim at the prevention of future criminal offences, it did, nevertheless, specify that such measures pursued the purpose of facilitating the investigation of future crimes. [73]

The judgments of the Federal Constitutional Court are extensively summarized in the *Peruzzo and Martens* judgment. [74] We learn from this that in a first judgment of 14 December 2000,[75] the German Court declared Article 81g of the Code of Criminal Procedure constitutional, because the DNA profiling technique used did not affect the core of the personality rights protected in the German Constitution (*Kernbereich der Persönlichkeit*). The collection, retention and future use of DNA profiles do affect the constitutionally guaranteed right to self-determination over personal data (*informationelles Selbstbestimmungsrecht*), but it was justified by an overriding public interest and complied with the principle of proportionality.
Interesting in the proportionality assessment of the Constitutional Court is, firstly, the observation of the Court that *'while Article 81g was not aimed at the prevention of future criminal offences, it did however facilitate the investigation of future crimes of considerable significance and thus served the proper administration of justice'*. Why this rather cryptic message was re-used by the ECtHR is not immediately clear. More interesting is the holding of the Court that the precautionary ("*vorsorglich*") taking of evidence permitted under Article 81g did not infringe the principle of proportionality. The taking of such evidence could only be ordered in the event the concerned person had previously been convicted of an offence of considerable significance and in the event there were concrete indications that further proceedings concerning criminal offences of considerable significance were to be conducted against him or her in the future. Moreover, by strictly limiting the use of cellular material collected for the purposes defined in the Article and by making its destruction compulsory once the concerned person's DNA profile was established, the legislator had provided for safeguards to prevent abuse of cellular material obtained.
In a subsequent judgment dated 14 August 2007,[76] the Federal Constitutional Court stressed that the procedure did not allow the domestic courts to automatically conclude that the repeated commission of offences justified an order for the taking of cellular material. Domestic courts were obliged to have regard to the specific circumstances of the individual case and in particular the personality of the person concerned and the manner in which the offences had been committed. On this basis they had to proceed to an overall assessment of the degree of unlawfulness reflected in the offences committed and to be expected in the future while always observing the principle of proportionality in their decision-making.

[72] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 49.
[73] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 40.
[74] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par. 25 & 26
[75] German Federal Constitutional Court, 14 December 2000, 2 BvR 1741/99; 2 BvR 276/00 and 2 BvR 2061
[76] German Federal Constitutional Court, 14 August 2007, 2 BvR 1293/07

It is clear that the German Constitutional Court judgments on the use of DNA in criminal proceedings have oriented the Strasbourg Court's reasoning in *Peruzzo and Martens*. The sheer taking and storing of DNA samples is based on precautionary or pre-emptive arguments,[77] but if this is done in a fundamental rights respectful way, with requirements such as seriousness and destruction of the original sample after establishing the profile, it is both legitimate and proportional under Article 8 of the ECHR.

Whether this position will stand in the way of nation-wide databases in the name of equality,[78] or in the name of public health considerations,[79] remains to be seen.

Interesting is the question of the legitimacy in the name of the right to the presumption of innocence. Relying on Article 6 § 2 of the ECHR the applicants in *Peruzzo and Martens* contend that the domestic courts' assumption, as reflected in their impugned decisions, that the applicants would commit further criminal offences in the future, infringed the principle of the presumption of innocence. We recall that Article 6 § 2 of the ECHR reads as follows: "*Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law*." The Court rejects the complaint with a textual argument. A "charge" in the sense of Article 6 § 2 of the ECHR can be defined as the official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence or any measure carrying the implication of such an allegation and substantially affecting the situation of the suspect.[80] It is true that the decisions by the domestic courts referred to past convictions of the applicants as well as their future criminal prognosis but the Court holds, without implying any allegation that the applicants would be suspected of reoffending.[81] Hence, there is nothing to demonstrate that the applicants were "charged with a criminal offence" in the sense of Article 6 § 2 of the ECHR

It will be difficult to explain to non-lawyers the reasoning that a question about a database founded to combat potential recidivism has nothing to do with the right to be presumed innocence, but the foregoing teaches us that the skills of lawyers are, as always, near the powers of magic.
A more convincing message is given in *M.K. v. France*, where the right to be presumed innocent is used as a tool or protection against stigmatisation. We already discussed one of the findings of the Court in the context of the Article 8 of the ECHR proportionality testing that making no distinction between persons who had been convicted and those who had never been found guilty of an offence are at risk of being stigmatised, in disregard of their right to be presumed innocent.[82]

[77] R. Van Brakel & P. De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', in Evelien De Pauw, Paul Ponsaers, Kees van der Vijver, Willy Bruggeman, Piet Deelman (eds.) *Technology-led policing* (CPS 2011 - 3, nr. 20), *Journal of Police Studies*, 2011, vol. 20(3), nr. 20, 163-19; Marieke De Goede & Beatrice De Graaf, 'Sentencing Risk: Temporality and Precaution in Terrorism Trials', *International Political Sociology*, 2013, vol. 7, 313–331
[78] D.H. Kaye & Michael E. Smith, '*DNA Identification Databases: Legality, Legitimacy, and the Case for Population-wide Coverage',* 2003, Wisconsin Law Review, 413–459.
[79] A. Raine, *The Anatomy of Violence: The Biological Roots of Crime*, 2013, Pantheon, 496p. (in particular the last chapter)
[80] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par 52 with ref. to *G.K. v. Poland*, no. 38816/97, par. 98, 20 January 2004 and to *Šubinski v. Slovenia*, no. 19611/04, par. 62, 18 January 2007, and *Eckle v. Germany*, 15 July 1982, par. 73, Series A no. 51.
[81] ECtHR, Decision of 4 June 2013, *Peruzzo and Martens v. Germany*, par 53.
[82] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 42 : "En outre, la Cour note que le décret n'opère aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public. Or, dans son arrêt S. et Marper, la Cour a souligné le risque de stigmatisation, qui découle du fait que les personnes qui avaient respectivement bénéficié d'un acquittement et d'une décision de classement sans suite - et étaient donc en droit de bénéficier de la présomption d'innocence - étaient traitées de la même manière que des condamnés (§ 22). La situation dans la présente affaire est similaire sur ce point, le requérant ayant bénéficié d'une relaxe dans le cadre d'une première procédure, avant de voir les faits reprochés par la suite classés sans suite".

The Court clarifies that storing data of persons that have never been found guilty does not equate an expression of suspicion, but the conditions of the storage may not create the impression that they are not considered innocent.[83]

[83] ECtHR, Decision of 18 April 2013, *M.K. v. France*, par. 36 : "Enfin, il appartient à la Cour d'être particulièrement attentive au risque de stigmatisation de personnes qui, à l'instar du requérant, n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence, alors que leur traitement est le même que celui de personnes condamnées. Si, de ce point de vue, la conservation de données privées n'équivaut pas à l'expression de soupçons, encore faut-il que les conditions de cette conservation ne leur donne pas l'impression de ne pas être considérés comme innocents (S. et Marper, précité, § 122).".

Chapter 4. Recent developments in the European Union

4.1. The 2011 Opinion of the Working Party 29 on the category of sensitive data

The Data Protection Directive (95/46/EC) and the Council of Europe Data Protection Convention of 1981 are based on the premise that certain categories of personal data, as distinct from all other personal data, require extra protection and may be processed by private and public bodies only for specific purposes and under special conditions. Article 8 of the Directive defines sensitive data as personal data revealing racial origin, political opinions or religious or philosophical beliefs, trade-union membership and data concerning health or sex life. In an Advice Paper of 2011,[84] the Article 29 Working Party analysed this article more closely and discussed the option of changes to the categories of sensitive data mentioned in Article 8 (1) of the Directive as well as to the exceptions in Article 8 (2) – (4), (5) and (7).

In general the Working Party favored the current approach to sensitive data – which is characterised by a conclusive list of data being regarded as sensitive per se – but proposed, on the one hand, to build in more flexibility to include new forms of sensitive data or new forms of data and data processing which could lead to severe infringements of privacy and also on the other hand, to include more exceptions to the prohibitive regime for sensitive data.
With regard to the data categories listed in Art. 8 (1) of the Directive, the majority of the Working Party members were in favour of explicitly including genetic data in the catalogue of sensitive data. Only some DPAs were in favour of also including biometric data. The Advice Paper therefore recommends that biometric data, as well as possible further new categories of sensitive data, should not be enacted without the support of a solid definition.

In the country reports we find an intermediary position under the **Slovenian** data protection act, where sensitive personal data includes not only the standard types of sensitive personal data, but also biometric information if it can be used to identify sensitive personal data about a data subject.

4.2. The 2012 reform package of the European Commission

On the 25th of January 2012, the European Commission published two significant proposals regarding the future European Union legal framework on data protection. The proposed EU Regulation[85] (hereinafter proposed Regulation) applies to the private and public sector, except for law enforcement, and the proposed EU Directive[86] (hereinafter proposed Directive) applies to law enforcement.

---

[84] Article 29 Working Party, *Advice Paper on special categories of data ("sensitive data")*, Letter of March 20, 2011 from the Article 29 Working Party addressed to Ms Le Bail to deliver input to the Commission on the current practices at national level, the problems encountered in implementing the Directive as well as some suggestions for improvements or changes in relation to special categories of data ("sensitive data"), notification and the practical implementation of the Article 28(6) of the Directive 95/46/EC via http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[85] Proposal for a Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter proposed Regulation), COM(2012) 11 final, 2012/0011 (COD) C7-0025/12, available online at
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0011_/com_com(2012)0011_en.pdf;

[86] Proposal for a Directive of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereinafter proposed Directive), COM(2012) 10 final, 2012/0010 (COD)C7-0024/12, available online at
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0010_/com_com(2012)0010_en.pdf.

It is remarkable that the term 'biometric' is only mentioned twice in the proposed Regulation. It is used for a first time in Article 4(11) of the proposed Regulation containing a definition of biometric data. [87]

Article 33 of the proposed Regulation contains a second mention of the term. The provision comprises the requirement for the controller or processor of a biometric system to carry out a so-called data protection impact assessment, which is an assessment of the impact of the envisaged processing operations on the protection of personal data. This is required because the *"[…] processing operations [of biometric data] in particular present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes […]".* Biometric data is not included as a special category in the proposed regulation. Article 9 on the processing of special categories of personal data elaborates that genetic data and data concerning health count as special categories of personal data whose processing should be prohibited in principle (unless one of the exceptions in Article 9 is applicable).

The proposed Directive does not add much to the present legal framework with respect to biometrics. For example, it does not include concept of privacy impact assessment (sometimes called data protection impact assessment). The term 'biometric' is only mentioned once in the proposed Directive. Article 3(11) of the proposed Directive contains the same definition of biometric data as the one contained in the proposed Regulation.[88]

The proposed Directive, unlike the proposed Regulation, does not contain a requirement of a privacy impact assessment. Such a requirement is also lacking in the 2005 progress report and the 2011 Parliamentary Assembly report. Privacy impact assessments are important to limit the biometric systems' risks posed to the individual's rights and freedoms, particularly with regard to large biometric systems used for Eurodac, SIS, VIS and the European Biometric Passport – these will be discussed which in the next chapter.

The proposal of the Commission for a regulation has been debated in the European Parliament and the following amendments were proposed:[89]
- a slight modification of the definition of 'biometric data' meaning any <u>personal</u> data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data (Art. 4(11));
-inclusion of biometric data under the definition of 'special categories of data) under article 9.1: *"The processing of personal data, revealing race or ethnic origin, political opinions, religion or <u>philosophical</u> beliefs, <u>sexual orientation or gender identity</u>, trade-union membership <u>and activities</u>, and the processing of genetic or biometric data or data concerning health or sex life, <u>administrative sanctions</u>, <u>judgments</u>, criminal <u>or suspected offences</u>, convictions or related security measures shall be prohibited".*

[87] ''biometric data' means any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data'
[88] ''biometric data' means any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data'.
[89] Committee on Civil Liberties, Justice and Home Affairs, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Rapporteu, Jan Philipp Albrecht, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), November 21, 2013

It is noteworthy that the European Commission, unlike the Council of Europe, does not define biometric data as sensitive personal data or even a special category of personal data. The Council of Europe steers another course. In the modernisation proposal of the Consultative Committee regarding Convention 108 and the Consultative Committee's 2013 draft explanatory report of the modernised version of Convention 108, biometric data is considered sensitive data (see Chapter 3.2). The European Commission, like the Council of Europe's Consultative Committee, acknowledge the importance of a standardised definition of biometric data, as they both suggest one. The Committee's 2013 draft explanatory report contains the following definition of biometric data: "*data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter*". In the European Parliament, the text of the proposal has been modified in order to include biometrical data under the special categories of data.

The European Commission and the Council of Europe are aware of the necessity to implement the requirement of a privacy impact assessment (sometimes called a data protection impact assessment). The proposed Regulation contains such a requirement in Article 33, and the 2012 Modernisation Proposal of the Council of Europe's Consultative Committee includes such a requirement in Article 8bis(2). The country reports show that no Member State has yet implemented in their data protection legislation an obligation to perform a privacy impact assessment. However, France, Italy, "former Yugoslav Republic of Macedonia", Monaco, Montenegro and Slovenia incorporated the requirement of prior checking in their data protection legislation.

4.3. The Eurodac System

General

The Eurodac system, operational since 15 January 2003, enables European Union (EU) countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of one of the Union's external borders. This second function, apprehending illegal immigrants, was added to the original purpose of the system (management of asylum applicants) under pressure from certain states that were also pushing to make this possible in the Schengen system.[90]
By comparing fingerprints with the system, EU countries can determine whether an asylum applicant or a foreign national found illegally present within an EU country has previously claimed asylum in another EU country or whether an asylum applicant entered Union territory unlawfully.

The database contains all ten fingerprints of every asylum applicant and alien over 14 years old apprehended for irregular border crossing or found illegally present in a member state. These prints are taken and are kept together with other data, such as place and date of the asylum application, the member state of origin, gender and a reference number transmitted by the member state to the system.[91]

[90] See more in detail about the intimate connection between both systems: D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', in D. Broeders, M.K.C. Cuijpers & J.E.J. Prins (eds.), *De staat van informatie*, WRR-verkenning 25, Amsterdam, Amsterdam University Press, 2011, 264.
[91] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis*, Law, Governance and Technology Series, Volume 12, Dordrecht Heidelberg New York London, Springer, 2013 (975p.), 66.

The Eurodac system consists of: a central unit managed by the European Commission, a central computerised database of digital fingerprints, electronic means for data transfers between member states and the central database. The 2006 Commission Staff Working Document[92] of the Commission of the European Communities shows that in 2005 the EURODAC Central unit has again given very satisfactory results in terms of speed, output, security and cost-effectiveness. The database is therefore said to be 'a very successful IT tool'. [93]
Only national authorities responsible for asylum applications have access to the central database. These are the three categories of persons of which Eurodac gathers information: asylum seekers older than 14 years, aliens apprehended in connection with the irregular crossing of an external border and aliens illegally on the territory of a member state. The following data are registered: the member state of origin, the digital fingerprint, the gender and the reference number used by the ember state of origin.[94]

Data subjects entered on the Eurodac database do not carry a document containing the biometric data for verification or identification because the databank is the human body itself. Every time the person is subject to a control for the purposes of Eurodac, they will have to provide a body reading that can then be checked against the data held in the database.
These arrangements have attracted considerable criticism because Eurodac requires the mandatory disclosure of biometric information by people who have not committed a crime. Some commentators have questioned whether it is morally justifiable to require asylum seekers and aliens to provide biometric data, which is then placed in the public arena and out of their immediate control. The increase in recent years of the so-called 'special searches' triggered concerns about possible misuse of the purpose of this functionality by national administrations.[95] Therefore, the Commission has included in its proposal for the amendment of the Eurodac Regulation a requirement for member states to send a copy of the data subject's request for access to the competent national supervisory authority.[96]
The Commission also proposes to give law enforcement agencies access to the Eurodac database.[97] Such access poses a large risk for function creep and should only be possible in exceptional and well-defined circumstances.

The new Eurodac regulation

The Eurodac Regulation 2000 sets up Eurodac.[98] The Commission has tried to adapt this regulation on several occasions in view of allowing use of Eurodac by member states' law enforcement authorities and Europol.[99] In the near future this will be made possible. Although

[92] Commission of the European Communities, *Third annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit*, Commission Staff Working Document, SEC(2006) 1170, Commission of the European Communities 2006, available online at http://ec.europa.eu/dgs/home-affairs/e-library/docs/pdf/sec_2006_1170_en_en.pdf.
[93] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm
[94] When there is an alert the data are transferred through the DubliNet system. DubliNet is a secure electronic communication network between the national authorities dealing with asylum applications. The two involved member states can exchange personal data through DubliNet that differ from Eurodac data, like name, date of birth, nationality, photo, details on family members and in some cases addresses.
[95] European Commission, *Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit* 2011 (Report from the Commission to the European Parliament and the Council), COM(2012) 533 final, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0533:FIN:EN:PDF.
[96] *Ibid*, section 1.5.
[97] *Ibid*, section 1.2.
[98] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, *O.J.*, 15 December 2000, L 316, 1-10
[99] Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person) and to request comparisons with EURODAC data by member states' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, Brussels, 30 May 2012, COM(2012) 254 final 2008/0242 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0254:FIN:EN:PDF See for a brief history: E. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis*, 67.

there are currently enough databases around that are useful for law enforcement purposes, there are, according to the latest proposal, no effective possibilities available for law enforcement authorities to exchange information on asylum seekers.
The intention of the amendment is to allow consultation of Eurodac by law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences. Law enforcement authorities will be able to request the comparison of fingerprint data with those stored in the Eurodac central database when they seek to establish the exact identity of or get further information on a suspected person. On a 'hit'/'no hit' basis, the requesting law enforcement authority will be informed if information on the person is available in the national asylum database of another member states.

The Eurodac system, operational since 15 January 2003, requires the mandatory disclosure of biometric information (fingerprints) by asylum-seekers (people who have not committed a crime). It enables EU countries to identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union.
This use of fingerprints outside the context of law enforcement has of course attracted law enforcement attention. Because fingerprint data constitute an important element for establishing the identity of a person and because of its long tradition as a tool for prevention, detection and investigation of crime,[100] there has been a constant policy push towards extending the purposes of the database. The risk for function creep is especially present when access is given to law enforcement agencies, as currently proposed by the Commission. The proposed regulation allows national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in Eurodac for the purpose of the prevention, detection and investigation of serious crimes and terrorism. It remains to be seen how this requirement (only 'terrorism and other serious crime') is implemented in the EU Member States

4.4. The Schengen Information System

The Schengen Information System is the largest information system for public security in Europe. The system has been operational since 1995. The Schengen Information System (SIS) was established as an intergovernmental initiative under the Schengen Convention, now integrated into the EU framework. It is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. It holds information on persons who may have been involved in a serious crime or may not have the right to enter or stay in the EU. It also contains alerts on missing persons, in particular children, as well as information on certain property, such as banknotes, cars, vans, firearms and identity documents, that may have been stolen, misappropriated or lost. Information is entered into the SIS by national authorities and forwarded via the Central System to all Schengen States.
The legal basis for the Schengen Information System is laid down in the 1990 Schengen Convention that was incorporated into the EU legal *acquis* with the 1998 Amsterdam Treaty. On paper the Convention has much charm: it defines the Information System as a 'sober'[101] 'hit/no' hit machine that gives policemen in the field and other users only limited information on the subjects and objects contained in the system, it defines the users and the purposes of the alerts, data subject rights and the role of data protection authorities. In a landmark study in

[100] See page 3 of the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU); Brussels, 30 May 2012, COM(2012) 254 final 2008/0242 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0254:FIN:EN:PDF
[101] 'Sober' in the sense that the user does only get a limited amount of information needed to take action in case of a hit. See D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', in D. Broeders, M.K.C. Cuijpers & J.E.J. Prins (eds.), *De staat van informatie*, WRR-verkenning 25, Amsterdam, Amsterdam University Press, 2011, 260

2008, Evelien Brouwer finds many weaknesses in the system, from imprecise and unchecked criteria for different entry categories, lack of control on compliance with the purpose limitation principles and legal remedies that are hardly effective for the data subjects.[102] The same year a report was produced by the Dutch DPA criticising differences between states concerning the use of Schengen alerts and the interpretation of terms regarding these alerts in the Schengen Convention.[103]

The Schengen tool is however very popular amongst its users, apparently appreciating the discretion made possible by the legal framework. It is accessible at border stations and from police cars and frequently used to 'google' number plates of cars that happen to pass the gaze of the patrolling policemen.[104] It is especially from their side that demands were made to improve the system and to make the (sober) hit system more intelligent.[105] Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system.
A European Parliament report has pointed out that there has been no targeted impact assessment on the use of biometrics, and that specific provisions detailing fallback procedures to protect individuals who are wrongly identified are lacking. The real capabilities of the biometric identifiers chosen within SIS II for identification have not yet been assessed.

So far, a record in the SIS did not include more than 2 lines worth of data, in other words, not more than the simple search entry. SIS 2 will thoroughly change this. From now on, photos, fingerprints and, if necessary, even DNA profiles will be included in the SIS personal records. The character of the system is therefore substantially changed. Up to now, SIS has been used first and foremost by officers controlling entry at the borders. In future, it will increasingly be police crime investigation units who are interested in the SIS. *Sweeping searches* to compare a fingerprint with fingerprints stored in the database will become a possibility, turning the SIS from a control system into an investigative tool. [106] The possible use of SIS II biometric data for investigative purposes might pose serious risks for data subjects if the significance of biometric evidence is over-estimated by the courts.

---

[102] E. Brouwer, *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*, Leiden, Martinus Nijhoff Publishers, 2008, 566p.

[103] College Bescherming persoonsgegevens, *Afronding onderzoek artikel 99 SUO*, March 20, 2008, via https://www.cbpweb.nl/downloads_int/eindbrief_minister_Justitie_docSUO.pdf See for an in debt critique of the lack of policy streamlining between member states with regard to the system: D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', 263-265. See also M. Besters , 'The downside of the Schengen Information System' in G. MUNNICHS, M. SCHUIJFF & M. BestersS (eds.), *Databases The promises of ICT, the hunger for information, and digital autonomy*, The Hague, Rathenau Institute, 2012, 74-85; M. Besters, 'De schaduwzijden van het Schengen informatiesysteem' in G. Munnichs, M. Schuijff & M. Besters (ed.), *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, The Hague, Rathenau Institute, 2010, 74-85.

[104] See 'Data statistics: Schengen Information System (SIS)', *Statewatch*, 1999, vol. 9, no. 3 & 4, 23 -24. In this shorter comment the author discusses the very low success-rate for the system and, more importantly, the important shift in policing that the System has made possible. By being accessible everywhere random searching (or google searching as we called it in our tekst) became an integrated police concept: *"In practice, this means that control is not initiated on grounds of a particular suspicion but on ground of the presence of a 'terminal' combined with relevant appearance related 'clues'. This kind of non-suspect control has traditionally only been allowed at boarders. The introduction of national search systems in individual western European states since the 1970's, brought about major changes. With the introduction of the SIS, however, the so-called 'random' search (the shifting of border controls into the interior) became an integrated police concept, which especially in Germany, is enshrined in law"* (p. 24).

[105] See D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', 261.

[106] D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', 261.

The Schengen Information System (SIS) is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics (e.g. photos, fingerprints and, if necessary, even DNA profiles), the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. As soon as SIS II becomes operational it will increasingly be police crime investigation units who are interested in the SIS. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities. The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. The use of (biometric) data for another purpose than originally collected for, poses serious risks for the individual's rights and freedoms, particularly if more authorities will be granted access to SIS.

4.5. The Visa Information System (VIS)

Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS) (1) established the VIS as a system for the exchange of visa data between member states.[107] The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. It enables the exchange of visa data in relation to Schengen uniform visas and "national visas" among the member states that have abolished checks at their internal borders. Its objectives is to facilitate the fight against fraud, to contribute to the prevention of "visa shopping", to improve visa consultation, to facilitate identifications for the application of the Dublin II regulation and return procedures, to improve the administration of the common visa policy and to contribute towards internal security and combating terrorism. To this end, the VIS database will include information on the identity of about visa applicants (incl. biometric data), status of visa, authority that issued the visa and a record of persons liable to pay board and lodging costs.
The VIS is expected to handle more than 20 million visa requests from 25 participating states and 45 million requests to check on the validity of issued visas per year. The list of countries whose nationals must comply with the Schengen visa requirement in order to cross the external frontiers is set by Council Regulation (EC) 539/2001 of 15 March 2001.
Biometric data (digital facial image and fingerprints) have been added to the VIS. The Council Guidelines of 13 June 2002 indicate "*digitized photographs and other biometric data on the holder of the visa could also be entered into the VIS when they are added to the visa file*".

As said above, the system is said to help not only in implementing a common visa policy, but also to the Union's internal security and especially to the fight against terrorism. Law enforcement access by Europol and national authorities was therefore advocated as early as March 2005 and became possible with the 2008 Council Decision concerning access for consultation of the Visa Information Systems (VIS) by designated authorities of member states and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.[108] Access is only possible when "*there are reasonable grounds to consider that consultation of VIS data will substantially contribute to*

[107] Cf. Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC, *OJ* L 213, June 15, 2004, 1-5; Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), *OJ* L 218, August 13, 2008, 60-81.
[108] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJ*, L 218 , August 13, 2008, 129 -136

the prevention, detection or investigation of any of the criminal offences in question". VIS data, which may be used for the search, are limited to: surname, surname at birth, first names, gender and date, place and country of birth; current nationality and nationality at birth of the visa applicant; type and number of the travel document, the authority that issued it and the date of issue and expiry; main destination and duration of the intended stay; purpose of travel, and intended date of arrival and departure; intended border of first entry or transit route; residence; fingerprints; type of visa and number of the visa sticker; and details of the person that has either issued an invitation for the visa applicant or is liable for the applicant's subsistence costs during his/her stay.
If the search with any of the above data is successful, the authorities may in addition access other data. This includes any other data on the visa application, photographs and any supplementary information added onto the application when the visa was issued, refused, annulled, revoked or extended.[109]

Although these criteria can be labelled strict, one is struck by the loose argument used in the preamble of the 2008 Decision to recognise the access right: "*It is essential in the fight against terrorism and other serious crimes for the relevant services to have the fullest and most up-to-date information in their respective fields. The Member States' competent national services need information if they are to perform their tasks. The information contained in the VIS may be necessary for the purposes of preventing and combating terrorism and serious crimes and should therefore be available, subject to the conditions set out in this Decision, for consultation by the designated authorities*" *(emphasis added).*

The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. The VIS database will include information about personal identification of visa applicants (including biometrical data such as facial image and fingerprints), status of visa, authority that issued the visa, and record of persons liable to pay board and lodging costs.
Law enforcement access is build in not as a creepy second function of the database but as a genuine second objective of the system: "*The information contained in the VIS may be necessary for the purposes of preventing and combating terrorism and serious crimes and should therefore be available*".

4.6. Common thread: availability and interoperability

The EU has a double faced policy with regard to data protection law: both promoting it, but at the same time making its enforcement difficult by creating policies that seems to cut in the heart of its principles. In the field of EU police and judicial cooperation, a major step was the creation of the 'principle of availability'.[110] The European Commission adopted in 2005 a proposal on the exchange of information under such principle.[111] The adoption of the proposal was eventually put aside by the Council, while a number of member states agreed on other information sharing commitments under the Prüm Treaty.[112] In 2007 an EU Decision

[109] http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14512_en.htm
[110] We borrow from Gl. González Fuster, P., De Hert & S. Gutwirth, 'State-of-Art Report on the Current Scholarship on the Law-Security Nexus in Europe', D.2.1., Deliverable submitted November 2008 (M8) in fulfillment of requirements of *the FP7 Project, Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX),* 2009, 46p., (http://www.inexproject.eu/)
[111] EC (2005), Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final), 12.10.2005, Brussels.
[112] The Prüm Treaty on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, was signed by several members of the European Union on 27 May 2005. The treaty sets out rules for the supply of fingerprinting and DNA data to other contracting parties and their automated checking against their relevant data bases. The treaty provides *inter alia* that 'the Contracting Party administering the file may process the data supplied (...) solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording... The supplied data shall be deleted immediately following data comparison or automated

transposed most of the substance of the Prüm Treaty (including provisions on fingerprints, DNA and vehicle registration data) into the EU institutional framework. The European Commission saw this as a partial implementation of the 'principle of availability'.[113] 'The Future Group' report on the upcoming programme for EU Justice and Home Affairs discusses a 'convergence principle', which is to follow on, in a sense, from the 'principle of availability' and the 'interoperability' of EU information systems;[114] it also recommends implementing an EU information management strategy "promoting a coherent approach to the development of information technology and exchange of information".[115]

Currently the EU is setting up a biometric matching system, a search function that will match the biometric data of a given person with the biometrical data stored in all large-scale EU databases (VIS, Eurodac and Schengen II). Another system, the entry/exit-system, not discussed in the report, is also intended to be connected with the search function.[116]

Overseeing the legal landscape of EU large-scale databases has brought certain eminent academics to propose a directive with minimal guarantees for the individual that is controlled at EU borders.[117]
The proposed Directive foresees a full article on rights regarding personal data used by controlling authorities. Article 5 foresees amongst others that authorities shall inform a person without delay on the purpose of the processing for which his or her data are intended, the recipients or categories of recipients of the data, the time during which the data will be stored and the existence of the right of access to and the right to rectify the data. This must happen at the moment that the information is obtained from the person, and no later than the time when the data are first entered into a data system. The same article also proposed that in the case of decisions made on the basis of the processing of personal data, the individual concerned would be informed in writing about the official authority that forwarded the data or entered the data into the database.
The proposals echo certain recommendations made in the European Parliament about the Schengen System: "*that citizens should be better informed about the SIS; refers to the principle that data subjects have a right to access to and rectification of their individual data and that, if the right to access cannot be observed in full or in part, data subjects must be notified of their right to appeal to the competent authority; asks that there be a right of appeal at the European level to the Ombudsman and/or the Data Protection Supervisor"*.[118]

replies to searches unless further processing is necessary for the purposes mentioned (Article 35)." See on the Prüm Treaty: Th. Balzacq, D. Bigo, S. Carrera & E. Guild, 'Security and the Two-Level Game: the Treaty of Prüm, the EU and the Management of Threats', *CEPS Working Document*, 2006, No. 234, CEPS, Brussels, January; R. Bellanova, 'The "Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange?, in E. Guild & Fl. Geyer (eds.), *Security versus Justice?: Police and Judicial Cooperation in the European Union*, Ashgate, Aldershot, 2008, 203-221.

[113] EC (2008), Communication from the Commission to the Council and the European Parliament: Report on Implementation of the Hague Programme for 2007, COM(2008) 373 final, 2.7.2008, Brussels, 7.

[114] T. Bunyan, *'The Shape of Things to Come: EU Future report'*, Statewatch, 2008, September, 37.

[115] Informal High Level Advisory Group on the Future of European Home Affairs Policy ('The Future Group') (2008), *Freedom, Security, Privacy: European Home Affairs in an open world, Report*, June, 9.

[116] D. Broeders, '*Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa'*, 261 with on page 270-275 a discussion of the proposed entry/exit system.

[117] Standing Committee Of Experts In International Immigration, Refugee And Criminal Law Utrecht, The Netherlands, *Border control and movement of persons. Towards effective legal remedies for individuals in Europe*, Utrecht, 2003, 23p. via http://media.leidenuniv.nl/legacy/Meijers%20Committee%20Effective%20Legal%20Remedies.pdf

[118] Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, *Report with a proposal for a European Parliament recommendation to the Council on the second-generation Schengen information system (SIS II) 2003/2180(INI)*), Rapporteur: Carlos Coelho, November 7, 2003, 18p.

4.6. The European Biometric Passport

What

Regulation No 2252/2004[119] provides that passports and travel documents are to include a highly secure storage medium that must contain, besides a facial image, two fingerprints. Those fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder.
Article 1 of the Regulation contains the main idea: passports and travel documents shall include a storage medium, which shall contain a facial image. Member states shall also include fingerprints in interoperable formats. The data shall be secured, and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. Under article 1(1) to (2a) of Regulation No 2252/2004:

> 1. Passports and travel documents issued by Member States shall comply with the minimum security standards set out in the Annex.
> 2. Passports and travel documents shall include a highly secure storage medium which shall contain a facial image. Member States shall also include two fingerprints taken flat in interoperable formats. The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.
> 2a. The following persons shall be exempt from the requirement to give fingerprints:
> (a). children under the age of 12 years.
> (b). persons, where fingerprinting is physically impossible.

On all pages inside the passport or travel document a unique document number should be printed or perforated or, in passport cards, a unique document number should be integrated using the same technique as for the biographical data. It is recommended that in passport cards the unique document number is visible on both sides of the card.[120] The Regulation does not give any information about the possibility of establishing a European centralised database and leaves the decision as to whether or not to create a national database to the national governments.
Persons to whom a passport or travel document is issued shall have the right to verify the personal data contained in the passport or travel document and, where appropriate, to ask for rectification or erasure.[121]
No information in machine-readable form shall be included in a passport or travel document unless provided for in this Regulation, or its Annex, or unless it is mentioned in the passport or travel document by the issuing member state in accordance with its national legislation.[122]
The biometric features in passports and travel documents shall only be used for verifying: (a) the authenticity of the document; (b) the identity of the holder by means of directly available comparable features when the passport or other travel documents are required to be produced by law.[123]

[119] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ 2004 L 385, 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ 2009 L 142, 1; corrigendum: OJ 2009 L 188, 127).
[120] Council Regulation of 10 December 2004, Annex, sub 3C.
[121] Council Regulation of 10 December 2004, Article 4, 1.
[122] Council Regulation of 10 December 2004, Article 4, 2.
[123] Council Regulation of 10 December 2004, Article 4, 3

.

Historical background

The European Commission adopted a proposal for this regulation in 2004.[124] In the Explanatory Memorandum to the Commission Proposal, the Commission recalled that the idea of a "European Passport" was already accepted by the Member States "*to facilitate the free movement of nationals of Member States*" and as an instrument *"to promote any measures which might strengthen the feeling among nationals of the Member State that they belong to the same Community*".[125] The proposal was said to be in line with the ICAO report that adopted a facial recognition standard based on a contact-less chip in May 2003. ICAO recommended the use of a single biometric technology by all states, as this would ensure global interoperability, but allowed states to use two biometrics.[126] Following the events of 11/9 the need was felt to enhance the security of travel documents by adding biometric elements.[127] At the EU level, the G5, an informal group of ministers and officials belonging to the department of homeland affairs started pushing for the mandatory inclusion of fingerprints,[128] followed by the Council that added a second mandatory biometric identifier to the proposal, viz. fingerprints.

The main reason for preferring a regulation to a directive is that the proposal provides for harmonisation up to minimum standard for the security elements of such documents, and their biometric identifiers, thus leaving no room for discretion to the member states.[129] In the Explanatory Memorandum, the creation of a 'European register for issued passports' is named as a second step, but the Commission stresses that further research is necessary to "*examine the impact of the establishment of such a European Register on the fundamental rights of European citizens, and in particular their right to data protection".*[130]

The European Parliament voted a non-binding legislative resolution on the Commission proposal on 2 December 2004 based on a report by the Committee on Civil Liberties, Justice and Home Affairs of 28 October 2010.[131] This resolution was adopted by 471 votes in favour to 118 against with 6 abstentions.[132]
The Parliament proposed an amendment to the Commission's proposal stating that the biometric features in passports shall only be used for verification of the authenticity of the document and the identity of the passport holder and that it shall be stored on "*a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored"*. With the amendment, the Parliament aimed to better define the purpose for which the data will be used: "*it has to be made absolutely clear that the data can only be used for verification and under no circumstances for other purposes, in particular hidden surveillance*".[133]

---

[124] Commission of the European Communities, *'Proposal for a Council Decision on standards for security features and biometrics in EU citizen's passports'*, Brussels, 18 February 2004, COM(2004) 116 final, 20p.
[125] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 2.
[126] International Civil Aviation Organisation (ICAO) in Document 9303, See ICAO, Biometrics Deployment of Machine Readable Travel Documents, ICAO TAG MRTD/NTWG Technical Report: 'Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation Using MRTDs ' (Montreal ICAO, 2003).
[127] Ibid.
[128] D. Broeders, 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa', 274
[129] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 6.
[130] Commission of the European Communities, 'Proposal for a Council Decision on standards', *l.c.*, 8.
[131] The vote was based on the following report: European Parliament's report of 28 October 2010 on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), including voting list and all amendments, via http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A6-2004-0028+0+DOC+PDF+V0//EN. Rapporteur: Carlos Coelho
[132] Article 29 Data Protection Working Party's Opinion (WP 112) on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *Official Journal L 385*, December 29, 2004 1-6, adopted on 30 September 2005.
[133] European Parliament's report of 28 October 2010 on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)), 16

Another amendment proposed by the Parliament stipulated that "*no central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up".*
According to the report by the Committee on Civil Liberties, Justice and Home Affairs of 25 October 2004, "*the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets."*

In December 2004, the Council adopted the regulation, without incorporating any of the amendments proposed by the Parliament. The choice for mandatory facial images as well as finger scans was not questioned.[134] The idea of a centralised database was not mentioned, but neither prohibited as asked for by the Parliament.
It is not unfair to say that little attention has been paid by the EU legislator to the requirement of proportionality and necessity.[135] Nowhere in the Commission's proposal or in the final Council Regulation is it demonstrated that two biometrics and a centralised database are proportional and necessary in a democratic society. The sheer fact that the Commission had initially limited itself to making only one biometric obligatory and seemed hesitant to argue for and propose databases at national or European level, indicates that it had taken another view. On the basis of current data protection legislation choices for more biometrics and for a centralised database do not seem automatically justified. We will come back in a next section on the arguments of *Privacy First*, a Dutch NGO, about the lack of numbers proving the capability of passport biometrics to combat *look-alikes*.

The Council of European Justice and Home Affairs ministers adopted Regulation (EC) No 2252/2004 ('Regulation on standards for security features and biometrics in passports and travel documents issued by Member States') on 13 December 2004 without taking into account amendments proposed by the European Parliament. The choice of mandatory facial images as well as finger scans and the idea of a centralised database was not questioned. Furthermore, little attention has been paid by the EU institutions to publicly accounting for the requirements of proportionality and necessity. The approach of the EU in the biometrics initiatives discussed here, confirm a broader trend of EU institutions imposing disproportionate data processing practices without simultaneously substantiating the privacy and data protection safeguards.[136] The particular dynamics of EU integration have been facilitating the proliferation of situations in which data processing measures are adopted and implemented while effective privacy and personal data protection are deferred, delegated to different actors, or both postponed and handed over to another level of decision-making.

It can be concluded that the EU does not always pay the requisite attention to privacy issues regarding biometrics. The country reports discussed in chapter 7 show that very few countries incorporate privacy protecting provisions in legislation concerning biometrics. More

[134] Council Regulation of 10 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Doc. 15152/04, 9 p. and one Annex, 5p.
[135] In its February 2004 Proposal, the Commission inserts a full paragraph on 'subsidiarity and proportionality', but a closer look reveals that these requirements are only understood in their federalist meaning, viz. to explain why this issue is taken up by the Union and not left to the discretion of the member states. A proportionality argument can be found in the assertion that the 'harmonisation of document formats and of their security features will provide a guarantee against counterfeiting. By preventing forgery and counterfeiting of travel documents the Commission intends to enhance the high level of security, a target set out both by the Treaty and the European Council of Thessaloniki' (*Ibid*).
[136] F. Gonzalez Fuster, P. De Hert & S. Gutwirth, *Situating Privacy and Data Protection in a Moving European Security Continuum*, D.2.5., Deliverable submitted March 2011 in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the International Security Continuum in Europe (INEX), 2009, 14p., published by the International Peace Research Institute (PRIO), Norway (http://www.inexproject.eu/

transparency is needed with respect to European procedures through which extended biometrical powers come into being. These procedures are characterised by a considerable veil of secrecy, which excludes the public from the discussion. [137]

4.7. The European Biometric Passport and the Court of Justice in *Schwarz v. Stadt Bochum*

General discussion of Schwarz v. Stadt Bochum

The validity of Council Regulation (EC) No 2252/2004 and the legitimacy of the obligation in this Regulation to provide fingerprints were questioned in *Schwarz v. Stadt Bochum*.[138] We briefly discussed one aspect of this judgment in a section above on the Court on Human Rights in chapter 3, since the Court of Justice in *Schwarz v. Stadt Bochum* refers to *Marper* when stating that fingerprints are protected both under privacy law and data protection law. The positions of the two European courts are thus very close, but not identical since the Court on Human Rights addresses biometrics in the context of Article 8 ECHR, where the Court functions in the realm of the EU Charter with a more modern, longer list of recogniSed rights and finds that biometrics both involve or touch upon the right to privacy (Article 7 EU Charter) and the right to the protection of personal data concerning an individual protected (Article 8 EU Charter).[139]

Let us first recall briefly the facts of the case. Mr. Schwarz applied to the city of Bochum for a passport but refused at that time to have his fingerprints taken. After the city rejected his application, Mr. Schwarz brought an action before an administrative court based in Gelsenkirchen in which he requested that the city be ordered to issue him with a passport without taking his fingerprints. Before that court, Mr. Schwarz disputed the validity of the regulation that created the obligation to take the fingerprints of persons applying for passports. He submitted that that regulation did not have an appropriate legal basis and was riddled with procedural defects. Both Article 7 and 8 of the Charter of Fundamental Rights of the European Union applied in his view but had not been respected.
The administrative court turned to Luxemburg seeking to establish whether the regulation was valid, particularly in light of the EU Charter, in so far as it obliges any person applying for a passport to provide fingerprints and provides for those fingerprints to be stored in that passport.

In the preliminary ruling, AG Mengozzi concluded that Regulation 2252/2004 is valid and that the obligation to provide fingerprints is legitimate on the grounds that the effective protection of the outside borders of the Schengen area is a recognised general interest of the EU and the registration of fingerprints is an indispensable tool to safeguard this interest. This positive fundamental rights reading was followed by the Court of Justice in its judgment of June 2013, but the judgment contains an important specification with regard to the possibility for member states - not excluded in the regulation, to store the biometrics in national central databases:
- firstly, the Court states it central position: although the taking and storing of fingerprints in passports constitutes an infringement of the rights to respect for private life and the protection

[137] A. Vedder, L. Van Der Wees, E.-J. Koops & P. De Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag, Rathenau Instituut, 2007, Studie 49, 90p.
[138] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*). See http://curia.europa.eu/juris/document/document.jsf?text=&docid=143189&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=103497
[139] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 30: 'In those circumstances, the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation No 2252/2004 constitutes a threat to the rights to respect for private life and the protection of personal data. Accordingly, it must be ascertained whether that twofold threat is justified'.

of personal data, those measures are in any event justified by the aim of protecting against any fraudulent use of passports. The Court finds that neither Article 7, nor Article 8 contains absolute rights and recalls that Article 52 of the Charter allows for limitations that are provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, are necessary and genuinely meet objectives of general interest recognized by the Union or needed to protect the rights and freedoms of others.[140]
- secondly, follows the analysis of the Court checking whether these requirements are met. In the opinion of the Court this is the case: Article 1(2) of Regulation No 2252/2004 lays out an appropriate legal basis for the collection and storing of fingerprints when issuing passports (par. 35 of the judgment); the measures serve the general interest objective of preventing illegal entry into the EU, by preventing both the falsification of passports and the fraudulent use thereof (par. 35-38 of the judgment); the passport project does not affect the essence of the right to privacy or the right to personal data protection (par. 39) and respects necessity and proportionality in the sense that the system does not go beyond what is necessary to achieve the objective of preventing illegal entry into the European Union (par. 40-65).

A closer look at the proportionality test in Schwarz v. Stadt Bochum

The necessity or proportionality test that the Court develops in par. 40 to 65 of the judgment consists of three parts: appropriateness (par. 40-45), availability of less intrusive alternatives (par. 46 to 54), and the existence of legal guarantees to protect against misuse and abuse (par. 55-65).
Firstly, the appropriateness (par 40-45 of the judgment) criterion is discussed – also applied in *Volker und Markus Schecke* and *Eifert*.[141] The reasoning that the Court develops is particularly interesting and is based on two argumentative steps:

- Argument 1a: it is 'common ground' that fingerprint technology is appropriate while it will reduce the risk of passports being falsified and to facilitate the work of the border-authorities (par. 41);
- Argument 1b: the error-rate of fingerprint technology (more on this in chapter 5 of this report) does not make the technology less appropriate. On the contrary, the technology 'significantly' reduces the work (par. 43) and 'exceptional' 'mismatches' can be corrected at the spot through human intervention (par. 44-45).[142]

[140] ECJ, Case C-291/12 of 13 June 2013 (Michael Schwarz v. Stadt Bochum), par. 33: 'Next, regarding whether the processing of fingerprints can be justified on the basis of some other legitimate basis laid down by law, it should be borne in mind from the outset that the rights recognised by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, *Volker und Markus Schecke and Eifert*, paragraph 48, and Case C- 543/09 *Deutsche Telekom* [2011] ECR I 3441, paragraph 51)'.
[141] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 40: 'the Court must establish whether the limitations placed on those rights are proportionate to the aims pursued by Regulation No 2252/2004 and, by extension, to the objective of preventing illegal entry into the European Union. It must therefore be ascertained whether the measures implemented by that regulation are appropriate for attaining those aims and do not go beyond what is necessary to achieve them' (with reference to ECJ, *Volker und Markus Schecke* and *Eifert*, Joined Cases C 92/09 and C 93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I- 11063, paragraph 74).
[142] '(par. 42:) Mr Schwarz submits that the method of ascertaining identity using fingerprints is not appropriate for attaining the aim of preventing fraudulent use of passports, since there have been mistakes when implementing that method in practice; given that no two digital copies of a set of fingerprints are ever identical, systems using that method are not sufficiently accurate, resulting in not inconsiderable rates of unauthorised persons being incorrectly accepted and of authorised persons being incorrectly rejected. (par. 43:) In that regard, however, it must be held that the fact that the method is not wholly reliable is not decisive. Although that method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance that would exist if that method were not used. (par. 44:) Although it is true that the use of fingerprints as a means of ascertaining identity may, on an exceptional basis, lead to authorised persons being rejected by mistake, the fact remains that a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union, as is pointed out in the second subparagraph of Article 4(3) of Regulation No 2252/2004. A mismatch of that kind will simply draw the competent authorities' attention to the person concerned and will result in a more detailed check of that person in order definitively to establish his identity. (par. 45:) In the light of the foregoing, the taking and storing of fingerprints referred to in Article 1(2) of Regulation No 2252/2004 are appropriate for attaining the aims pursued by that regulation and, by extension, the objective of preventing illegal entry to the European Union'.

Secondly, after having found that the contested measures are appropriate for attaining the aim of protecting against the fraudulent use of passports, by significantly reducing the likelihood that non-authorised persons will be allowed to enter the EU, the Court turns to a second criterion for measuring proportionality or necessity, also taken from the *Volker und Markus Schecke* and *Eifert* judgment: how proportional is the passport system in the light of available alternatives?[143] Several steps are taken in the argument that the Court advances:

- Argument 2a: collecting two fingerprints *and* collecting facial images are no major privacy intrusions since fingers and faces are public;[144]
- Argument 2b: it is true that two biometrics are gathered (*note: implicitly the Court seems to respond here to the observation that international law and the ICANN norms only recommend one biometric, namely iris data)*, but there is no principled or empirical evidence that more rights infringement is caused by using two biometrics; [145]
- Argument 2c: there is only one real alternative to fingerprinting and that is an iris scan, but there is no evidence that this interferes 'less' with the rights recognised in article 7 and 8 and this technology is less effective and more costly.[146]

Thirdly, there is, as was required by the Court on Human Rights in *Marper*, the presence of specific guarantees against misuse and abuse contributing to the proportionality of the passport system. The Court of Justice analyses Regulation No 2252/2004 and finds those guarantees built in.[147] True as it may be, the Court says that Regulation No 2252/2004 does not exclude explicitly central databases and function creep (for instance use of the fingerprints in criminal investigations or for surveillance), but the regulation cannot be seen as offering *any* legal basis for member states for the centralised storage of data collected or for the use of such data for purposes other than that of preventing illegal entry into the European Union.[148] Would member

[143] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 46: 'Next, in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the European Union rules in question (see, to that effect, *Volker und Markus Schecke and Eifert*, paragraph 86)'.

[144] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 48: 'In this respect, it is be borne in mind, on the one hand, that that action involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature. Nor does it cause any particular physical or mental discomfort to the person affected any more than when that person's facial image is taken.'

[145] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 49-50: '(par. 49:) It is true that those fingerprints are to be taken in addition to the facial image. However, the combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation. (par. 50:) Thus, as regards the case in the main proceedings, nothing in the case file submitted to the Court permits a finding that the fact that fingerprints and a facial image are taken at the same time would, by reason of that fact alone, give rise to greater interference with those rights.'

[146] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 51-53: '(par. 51:) On the other hand, it should also be noted that the only real alternative to the taking of fingerprints raised in the course of the proceedings before the Court is an iris scan. Nothing in the case file submitted to the Court suggests that the latter procedure would interfere less with the rights recognised by Articles 7 and 8 of the Charter than the taking of fingerprints. (par. 52:) Furthermore, with regard to the effectiveness of those two methods, it is common ground that iris-recognition technology is not yet as advanced as fingerprint-recognition technology. In addition, the procedure for iris recognition is currently significantly more expensive than the procedure for comparing fingerprints and is, for that reason, less suitable for general use. (par. 53:) In those circumstances, the Court has not been made aware of any measures which would be both sufficiently effective in helping to achieve the aim of protecting against the fraudulent use of passports and less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints.'

[147] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 55-57: '(par. 55:) In that regard, the legislature must ensure that there are specific guarantees that the processing of such data will be effectively protected from misuse and abuse (see, to that effect, ECHR judgment, *S. and Marper*, cited above, par. 103). (par. 56:) In that respect, it should be noted that Article 4(3) of Regulation No 2252/2004 explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder. (par. 57:) In addition, that regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons. In that regard, Article 1(2) of that regulation makes it clear that such data are to be kept in a highly secure storage medium in the passport of the person concerned.'

[148] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 58-61: '(par. 58:) however, the referring court is uncertain, in the light of its assessment, whether Article 1(2) of Regulation No 2252/2004 is proportionate in view of the risk that, once fingerprints have been taken pursuant to that provision, the – extremely high quality – data will be stored, perhaps centrally, and used for purposes other than those provided for by that regulation. (par. 59:) In that regard, it is true that fingerprints play a particular role in the field of identifying persons in general. Thus, the identification techniques of comparing fingerprints taken in a particular place with those stored in a database make it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly. (par. 60:) However, it should be borne in mind that Article 1(2) of Regulation No 2252/2004 does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone. (par. 61:) The regulation not providing for any other

states enact legislation to centralise or use the data for other purpose, then this would have to be looked at in new procedures before the Courts, but that does not currently affect the validity and conformity with fundamental rights of Regulation No 2252/2004.[149]

A critical comment

A lot of arguments used by the Court of Justice are debatable. One can defend or not the general finding that the inclusion of fingerprints, next to what is internationally required (iris scans) in the EU electronic passports is lawful. One can rejoice in seeing the Court follow the *Marper* finding that taking and storing of fingerprints in passports constitutes an infringement of the rights to respect for private life and the protection of personal data. But claims that taking fingerprints is not that sensitive, because it "*involves no more than the taking of prints of two fingers, which can, moreover, generally be seen by others, so that this is not an operation of an intimate nature*" (argument 2a) are of course controversial. We already criticised the argument that the public nature of the collection reduces the impact on individuals in chapter 3, [150] but it is worth coming back to it: not only is there something valuable at stake in the public area that needs to be protected by the right to privacy, but also it is difficult to maintain that biometric capturing devices perceives biometric characteristics in an entirely similar way to human beings, or with the same purpose.
The proportionality test of the Court with its threefold constructions seems quite elaborate but some open questions remain. Will criminals, once aware of the use of the data for investigation purposes, leave false traces (other persons' fingerprints) to thwart investigation?[151] Is the problem of false entries caused by look-alike fraud with passports real? A Dutch NGO argues that this is not the case, criticises the lack of qualitative research by the Court and advances Dutch numbers of look-alike fraud with passports that point at a very minor problem; 2009 only 33 cases were reported, in 2010 only 21, in 2011 only 19 and in 2012 only 21.[152]

---

form or method of storing those fingerprints, it cannot in and of itself, as is pointed out by recital 5 of Regulation No 444/2009, be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the European Union.'

[149] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*), par. 62-: '(par. 62:) In those circumstances, the arguments put forward by the referring court concerning the risks linked to possible centralisation cannot, in any event, affect the validity of that regulation and would have, should the case arise, to be examined in the course of an action brought before the competent courts against legislation providing for a centralised fingerprint base. (par. 63:) In the light of the foregoing, it must be held that Article 1(2) of Regulation No 2252/2004 does not imply any processing of fingerprints that would go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports. (par. 64:) It follows that the interference arising from Article 1(2) of Regulation No 2252/2004 is justified by its aim of protecting against the fraudulent use of passports. (par. 65:) In those circumstances, there is no longer any need to examine whether the measures put into effect by that regulation are necessary in view of its other aim (namely, preventing the falsification of passports). (par. 66:) In the light of all the foregoing considerations, the answer to the question referred is that examination of that question has revealed nothing capable of affecting the validity of Article 1(2) of Regulation No 2252/2004.'

[150] Privacy in public is an important value precisely because the anonymity of the crowd provides an individual with privacy (Nissenbaum 1997). Biometric systems could identify individuals and thus violate this expectation of privacy or render superfluous the legal criterion of the public nature. Moreover the biometric machine/software ''perceives'' biometric characteristics in an entirely different manner than human beings. Therefore, it is not relevant that police use the system in public. This is because the software can store the data and render it searchable (inferring information not available to the naked human eye)" (M. Pocs, 'Legally compatible design of future biometric systems for crime prevention', *Innovation.The European Journal of Social Science Research*, 23013, vol. 26, 1-2, (36-56), 40). Compare: "Some more recent biometric technologies which are being investigated rely on information such as the walking rhythm of a person (gait). Although it is for everyone visible how someone walks, especially in a public space, this information, if processed, will in general, in so far the other elements of the definition are met, be personal data and shall be treated accordingly. The information of other biometric characteristics, such as the facial image, is also visible and increasingly recorded in public places. Based on this clarification in Opinion 4/2007, it is in our view clear that the fact that information about biometric characteristics is *visible or sometimes even 'left' in public places* (e.g., fingerprints on a glass door) does not mean that this information because of its 'public content' should not be considered personal data anymore" (E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 106). See also EDRI, European Court Of Justice: Fingerprints In Electronic Passport Are OK, 23 October 2013, via http://edri.org/european-court-of-justice-fingerprints-in-electronic-passport-are-ok/

[151] R. Leenes, 'Denk na, omdat het kan', in H. van Kempen & G. Munnichs (dds.), *Privacy - Kenniskamer 17 december 2009*, The Hague, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2010, 37-38

[152] Privacy First, 'EU Hof verbiedt centrale opslag vingerafdrukken', October 17, 2013, via https://www.privacyfirst.nl/aandachtsvelden/biometrie/item/682-eu-hof-verbiedt-centrale-opslag-vingerafdrukken.html. Also *'Fraudebestrijding met vingerafdrukken in paspoorten is en blijft schieten met kanon op een mug'*, October 30, 2013, via http://www.privacynieuws.nl/nieuwsoverzicht/binnenlands-nieuws/id-plicht-paspoort/11499-fraudebestrijding-dmv-vingerafdrukken-in-paspoorten-is-en-blijft-schieten-met-kanon-op-een-mug.html

The error problem with biometrics is acknowledged by the Court, but marginalized (argument 1b). If one oversees the extent of the data collecting even a small percentage of mismatches might create extensive problems for many citizens.[153] Numbers are one aspect of the problem, the stigmatising impact on an individual of a hit, be it a false hit or not, is another one.[154]

In the Netherlands the commotion around the fingerprints and the idea of central storage (not prohibited in the Regulation) has led to many controversies and some concrete results: the idea of including fingerprints in the identity card was dropped and the new passport law seemingly abandons the original proposal to centralise the fingerprints taken from those citizens in need of a passport.[155]

One of the major lessons to be learnt from the assessment of the European Court of Human Rights in the *Marper* case is that the storage of data such as fingerprints, cellular samples and DNA profiles in a database such as the one under examination is not inconsequential, irrelevant or neutral. On the contrary, the mere storage of such information conveys by itself a risk of stigmatisation:[156] *shadows of suspicion*, one could say, are projected upon those whose data is stored in a database dedicated to criminal identification and mainly destined to the storage of data of convicted people. Therefore, the storage of such data, when related to non-convicted individuals, has to be limited.[157]
Marper seemingly contradicts the finding of the Court of Justice in *Schwarz v. Stadt Bochum.* Where the ECJ finds no proportionality problem with EU Regulation No 2252/2004 requiring the collection and storing of fingerprints of all EU citizens when issuing passports: the measure serves the general interest objective of preventing illegal entry into the EU, by preventing both the falsification of passports and the fraudulent use thereof; the passport project supposedly does not affect the essence of the right to privacy and the right to personal data protection, and respects necessity or proportionality in the sense that the system does not go beyond what is necessary to achieve the objective of preventing illegal entry into the European Union.

The EU has been an active stakeholder in promoting large-scale biometric systems. These are introduced with only small-scale, or totally without, pilot studies,[158] and with choices regarding biometrics and law enforcement access that has raised a number of critical voices. Legislators have to show that there are no less intrusive alternatives available and that by using the biometric system, law enforcement agencies such as police can in fact detect organised crime

[153] J. van Someren, '*Vingerafdrukken, wel of niet essentieel'*, September 21, 2013, https://www.privacyfirst.nl/privacy-first/columns/item/675-vingerafdrukken-wel-of-niet-essentieel.html
[154] "Further, it is not only false positives or ''false hits'' that stigmatise individuals. Rather, the mere fact of a match is problematic. This is because the match solely confirms that one belongs to a certain category that might based on other evidence be involved in criminal action. Therefore, a match or a ''hit'' must not imply guilt. Police and courts must not treat innocent people as criminals. This is even true if the hit is not a false hit because the inclusion of a person in a wanted list could be erroneous too" and "The impact on individuals is more serious if the data subject is put under pressure to offer an explanation (Bundesverfassungsgericht 2010, 212) or is stigmatized (Bundesverfassungsgericht 2005, 351). Biometric (one-to-many) identification systems are subject to specific error rates (TeleTrust-Arbeitsgruppe Biometrie 2006, 15). Individuals could therefore be subject to ''false hits'' which stigmatize them" (M. Pocs, '*Legally compatible design of future biometric systems for crime prevention'*, 40 and 42).
[155] Rijkswet van 18 december 2013 tot wijziging van de Paspoortwet in verband met een andere status van de Nederlandse identiteitskaart, het verlengen van de geldigheidsduur van reisdocumenten en Nederlandse identiteitskaarten, een andere grondslag voor de heffing van rechten door burgemeesters en gezaghebbers en het niet langer opslaan van vingerafdrukken in de reisdocumentenadministratie (Wijziging van de Paspoortwet in verband met onder meer de status van de Nederlandse identiteitskaart), *Staabsblad* 2014/10. See http://njb.nl/wetgeving/staatsbladen/wijziging-paspoortwet.6443.lynkx
[156] *Marper*, par. 122. Moreover, the Court highlighted that the stigmatisation can be especially harmful when minors are concerned (ibid., par. 124).
[157] The judgment reviews different national approaches in Europe to the taking and retention of DNA information in the context of criminal proceedings, and notes that the UK is the only Council of Europe Member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.
[158] "Unfortunately, the introduction of biometric systems for large scale use in the public sector in the context of EU security, immigration and border control policies – notably in large scale systems such as Eurodac, VIS and SIS II, or as result of the inclusion of biometric characteristics in passports and travel documents – has not been preceded by small scale pilot projects, which could have allowed a gradual process of learning by doing" (P. Hustinx, 'Preface' in E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, v).

and terrorism. It is not enough to present facts that sound plausible. Rather one needs to conduct an empirical study. This study has to stand the test of the latest state of the art criminology.[159] Apart from organisational and technical polices to address errors and false hits (discussed in chapter 6), permanent research is needed to study how authorities are using large scale databases and how they organise the various groups of persons subject to data collection (witnesses, contact persons, informants, victims, etc.) and this in view of reducing the number of people that are subjected to data collection.[160]

[159] M. Pocs, '*Legally compatible design of future biometric systems for crime prevention'*, 40
[160] More in detail: M. Pocs, '*Legally compatible design of future biometric systems for crime prevention'*, 50.

Chapter 5. Technological developments

5. 1. Introduction

This chapter only addresses selective issues regarding technological development. Looking back at recent years **'the'** development was of course the function of large-scale governmental databases with biometrics in the area of border control and law enforcement (see above). A common thread seems to be that biometrics are increasingly extending to people who are not suspects. Biometrics leaves the world of the criminal. In the world of law enforcement, legal restrictions on the use of biometrics are being eased or lifted and police, the judiciary and intelligence receive right to access to biometric information that has been collected for purposes other than for intelligence and crime control. Consequently, people can more quickly become the subject of an investigation, without them knowing anything about this. [161]

In the private sector there were fewer spectacular developments (see also our country reports). One stakeholder talks about a 'delayed take-up of large-scale biometric applications by the commercial sector' that can be 'related to the privacy concerns'. [162]
This trend could be reversed by the launch on September 10th, 2013 by Apple of a new iPhone with a fingerprint reader underneath the home button. It will be interesting to see whether this US IT firm, that so far has not had a privacy unfriendly track record, will answer privacy and security questions raised by experts. [163] HTC and Samsung brought out similar smartphones, with fingerprint sensors, on the market in the beginning of 2014.
Time will also tell whether this development will change people's perceptions about fingerprinting.
Another important development is the rise of facial recognition technology currently being used by businesses, for instance by Facebook. Companies are beginning to use facial recognition for a wide range of commercial applications. Businesses are incorporating facial recognition capabilities into photo management software, in-store camera systems, online services, game consoles, and mobile devices. On December 3, 2013, the U.S. Department of Commerce's National Telecommunications and Information Administration ("NTIA") announced a new multi-stakeholder process to develop a code of conduct regarding the commercial use of facial recognition technology. The first meeting was held in February 2014.[164] Additional meetings are planned for the spring and summer of 2014.

In what follows we will discuss the definition of biometrical technologies in the light of data protection law (see 5.2.) and developments towards second generation biometrics (see 5.3. and 5.4.).

5.2. Biometrics as personal data and technological developments

Referring to a 2012 Opinion by the Article 29 Working Party we defined biometric data in this report as *measurable, physiological or behavioural characteristics that can be used to determine or verify identity. Biometrics is also defined as 'the automated use of physiological or behavioural characteristics to determine or verify individuals.*[165]

[161] A. Vedder, L. Van Der Wees, E.-J. Koops & P. De Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag, Rathenau Instituut, 2007, Studie 49, 90p.
[162] European Association for Biometrics (EAB), *iPhone 5S: heralding a paradigm shift?*, EAB Position Paper, November 2013, 5p. via http://www.eab.org/files/documents/2013-11-04_EAB-EABAC_paper_on_iPhone5s.pdf
[163] European Association for Biometrics (EAB), *iPhone 5S: heralding a paradigm shift?*, EAB Position Paper, November 2013, 5p. via http://www.eab.org/files/documents/2013-11-04_EAB-EABAC_paper_on_iPhone5s.pdf
[164] http://www.ntia.doc.gov/print/blog/2013/privacy-and-facial-recognition-technology
[165] This is the most accurate definition according to the authors, although numerous definitions exist. For example, the Article 29 Data Protection Working Party in 2012 suggested the following definition for biometric data: 'biological properties, behavioural aspects,

But are biometrics personal data in the sense of Directive 95/46/EC, that defines 'personal data' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity' (article 2 (a))?

In her book *Privacy and Data Protection Issues of Biometric Applications*, Els Kindt develops a full chapter on the question to what extent biometrics are to be considered as personal data. **[166]** She amongst others refutes the argument advanced by some that templates, stored on a chip card for 'off-line verification', are not personal data when the template is not linked with other personal data.[167] Kindt convincingly argues that all templates should be considered personal data,[168] and considers terms such as 'anonymous biometric data' and 'untraceable biometrics' to be misleading in the context of the argument that biometric data can be used for anonymous but secure verification: "In both cases of presumably 'anonymous' and 'untraceable' biometric data', the biometric data used remain in principle personal data while reducing however the risks for the data subject".[169]

The central message in her analysis is that almost all biometrical data is personal data **and** that the scope of biometrical data falling under personal data expands with contextual factors such as technological developments. This explains why the EU Working Party has issued not one but several opinions in which the scope of data protection law regarding biometrics is explored, the 2012 Opinion being the most recent one.[170] We refer for a broader analysis to these opinions and to the work of Kindt, but here we would like to underline the relevance of technological developments to this report. The test to apply to data, to determine whether it is personal or not in the legal sense, is **dynamic.**

Interesting is that the Article 29 Working Party also stated that the test is a **dynamic** test. What counts is the state of the art in technology at the time of the processing **and** the possibilities of future technologies during the period of the processing of the data. "*The period during which the data will be stored, will hereby and in general therefore play an important role".*[171] Stored biometric information, that does not on the basis of available technologies or with reasonable means, permit the identification of the data subjects, may allow later identification based on the use of **new methods or techniques**. "*An example relevant in the context of our research are*

---

physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability', see Opinion 3/2012 on developments in biometric technologies (WP 193), issued by the Article 29 Data Protection Working Party, and adopted on 27th April 2012, available online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

Biometrics are regularly considered to be 'unique' characteristics, although this is not always the case, as DNA samples of identical twins are not unique. DNA is not immediately machine readable, therefore this type of biometric data will not be discussed in this report. All other biometrics are thought to be unique, even both eyes of the same person or the eyes of identical twins, and the fingerprints on each finger of the same individual or the fingerprints of identical twins. See Irish Council for Bioethics, *Biometrics: Enhancing Security or Invading Privacy? Opinion* (hereinafter Irish Council for Bioethics Opinion 2009), Dublin: The Irish Council for Bioethics 2009, available online at http://irishpatients.ie/news/wp-content/uploads/2012/04/Irish-Council-Bioethics-Final_Biometrics_Doc_HighRes.pdf. The uniqueness is also considered to apply to behavioural biometrics, although further research is needed to confirm this premise.

Definitions of biometric data sometimes contain the word 'physical' or 'biological', but in this report it is omitted in favour of the word 'physiological' since the latter comprises physical, biological and chemical phenomena, see Encyclopaedia Britannica Online.

Although biometric systems are employed for several purposes (e.g. security or law enforcement), all systems have one basic function, namely authentication, subdivided into verification and identification, which are both used in the authors' definition of biometrics.

[166] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis*, Law, Governance and Technology Series, Volume 12, Dordrecht Heidelberg New York London, Springer, 2013 Chapter 3.

[167] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 95

[168] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 100

[169] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 103 and also see her Chapter 7.

[170] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies (WP 193)*, adopted on 27th April 2012, available online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf See also (and on the same website): Article 29 Data Protection Working Party, *Working Document on Biometrics (WP 80)*, 1 August 2003, 11 p.; Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services (WP 192)*, 22 March 2012, 9 p.

[171] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 113.

the pictures, posted by social network users, on social network sites. One could have argued some years ago that the collection of these pictures relate to persons who are for people, not belonging to a specific group of friends, not identifiable. However, face recognition technology similar to the technology used for tagging names to the social network users' pictures has become available for anyone on the Internet. This technology, which is becoming widely available, should be considered as a means likely reasonably to be used to render persons on pictures identifiable".[172]

This dynamic test and argumentation shed an interesting perspective on the discussion about a definition of biometrics. Are normal pictures personal data? Yes, of course, if they pass the dynamic test discusses above. Are normal pictures biometrical data? If the data allows identification, directly or indirectly, with current or future 'real' technologies, we see no objection. Classifying 'biometric data' within the category of 'sensitive data', and thus making picture fall under this prohibitive category may however be a step too far.

Biometrical data, including templates, should be considered personal data in legal terms. It is misleading to talk about 'anonymous' and 'untraceable' biometric data' that allows verification. A dynamic test explains why most stored biometrics that allow identification on basis of technology that exist or will exist in the foreseeable future are to be considered personal data.
In an area where face recognition technology is commonly used, pictures, posted by social network users, on social network sites fall under the category of personal data

5.3. Second generation biometrics

The 2011 report of the Parliamentary Assembly recommends the Council of Europe's Member States to 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. Second generation biometrics aims to identify a person on the basis of his or her behaviour or activities.

Pospisil and Skrob give several examples of what the new technologies can bring about for the user:[173] it can be used to detect lost children,[174] children that come near dangerous areas, [175] the elderly which fall on the street,[176] or abnormalities include gunshots, car crashes, shattering glass or the spraying of walls on houses and monuments. Evidently these applications can greatly facilitate the work of security and welfare forces that would otherwise have to go through dozens and dozens of hours of recordings or would have to be much physically present.

Philippe Frowd quotes Justin Florence and Robert Friedman finding six benefits in the use of behavioural profiling methods at borders: it provides an additional layer of security; it focuses on people rather than objects but avoids watchlists; it makes a more efficient use of screening resources by prioritising and profiling passengers; it avoids blanket passenger interviewing as

[172] E. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, 114.
[173] Pospisil R. & Skrob M., 'Actual trends in improvement of risk area security using combined methods for biometrical subject identification', *European Journal of Law and Technology*, Vol. 4, No. 2, 2013, (10p.), 2
[174] When a child is lost that has been seen in the area covered by the biometric identification system, 'the operator can simply request through the user application to find a girl with a height of approximately 110 cm who was wearing a blue shirt, red skirt and was last seen playing in the playground on 09/08/2012. The data is processed by data-mining layer and returns any information found on the likely occurrence of the girl after 09/08/2012'.
[175] 'The security service marks the surrounding area as potentially dangerous for children and transmits this information to the user application detection algorithms. In the event that a child is close to that danger point, the situation will be detected by the combined system of biometric identification and will alert the security person, who subsequently prevents the potential threat of injury to the child'.
[176] 'We will be able to detect the position of the subject, such as whether it is in a vertical or horizontal position. In the situation that an elderly subject will go down the street and while walking suddenly changes from a vertical to horizontal position, the system will detect this condition and mark it as potentially dangerous. The competent security service will then be notified that there is someone lying on the street with a likely health problem'.

is the case in Israeli airports; it avoids ethnic and racial profiling; and yields – anecdotal – results.[177]

Is it all for the greater good? No. The handling of first generation biometric data (e.g. fingerprints and iris scans) already creates fundamental discussions about the scope of data protection and human rights law. The introduction of soft biometrics, i.e. the use of general traits such as gender, weight, height, age, or ethnicity for automated classification, is even more contested. It has attracted criticism of indiscriminate social sorting, as automated decisions are created that divide people into categories for further processing. What are the legal implications of automated sorting of people on the basis of their behaviour (and/or general traits) into classifications such as for example, Asians and non-Asians, young and old, gay and hetero, and so forth? On the one hand, as machines are taking the decisions, the act of sorting takes on a seemingly neutral dimension. On the other hand, the embedded systems, ambient intelligence, distant sensing and passive biometrics involved require no conscious cooperation from subjects and thus pose a challenge to the traditional concepts used in the fields of data protection and human rights.

What are the important elements of second-generation biometrics and will they give rise to a new set of legal issues to be analysed and discussed? We identify two developments in biometrics that together form the main step away from the first generation biometric applications. The first is the emergence of new biometric traits and the second is the shift to embedded biometric systems, with elements such as distant sensing and 'passive' biometrics. These distinct developments are the basic changes that might catapult us into the world of ambient intelligence and ubiquitous computing. Then, the already complex legal assessment of biometric data processing will be taken to a different level altogether and pose serious challenges to existing legal approaches (basically based on data protection law). The dream of second generation of biometrics is a person's identification on the basis of that person's dynamic behaviour. In fact, the attempt is not made to identify a person, no: the objective is to read the person's mind.

The 2011 report of the Parliamentary Assembly recommends the Council of Europe's Member States to 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. Second generation biometrics aims to identify a person on the basis of his or her actual behaviour or activities. Second generation biometrics comprises a new type of biometric features such as gait (manner of walking), voice, body odour, ECG (brainwave pattern), EEG (electrical activity of the heart), body temperature, and pupil dilation. These biometric characteristics can sometimes be collected from a distance whilst the data subject is unaware. This makes it more difficult to monitor whether biometric controllers comply with data protection legislation (e.g. informed consent by the data subject prior to biometric data processing).

[177] Ph. M. Frowd, 'SPOT the Terrorist: Border Security and the Behavioural Profiling Paradigm', in *Living In Surveillance Societies: The State of Surveillance* in W. R Webster, G. Galdon, N. Zurawski, K. Boersma, B. Sagvari, Chr. Backman & Ch. Leleux (eds.), CreateSpace Independent Publishing Platform, 2013, (496p.), 404-416, 407

5.4. Specific concerns raised by second-generation biometrics

Problematic legal aspects of second generation are covert data capture, lack of transparency and consent. Many second-generation biometrics are collected whilst the data subject is unaware. Data is collected from a distance and the collection does not need to be apparent. The paradigm change here is that tracking and tracing becomes the norm resulting in a surveillance society. Instead of enrolling and identifying or verifying a person, second generation biometrics is aimed at a categorisation of individuals. The threats caused by this de-personalisation are manifold. Of course, unjustified selection according to profile will result in discrimination. Stigmatisation will occur and will involve allocation to a group on the basis of relatively random profiles that will impact the persons' future. Confrontation of individuals with unwanted information is another side effect that is very likely to occur. Finally, there will be unknown effects in linking dispersed information.
One of the most fundamental challenges in the protection of personal biometric data is related to the incremental change from visible to invisible data collection. The obvious risk that the systems (and not only personal data) may be used by other persons and for other purposes than foreseen (**function creep**) is difficult to minimise, without the traditional possibilities for individual participation (informed consent). A number of transparency tools can be developed that give the individual more insight into who is taking which decisions on the basis of data collected. The current lack of possibilities to enforce individual participation is regrettable when it comes to assessing the applicability of data protection law in situations where the subject is unaware of the invisible data collection. Therefore, the main legal concern regarding second-generation biometrics is the applicability of data protection regulation in those situations and the specific use of the data for **profiling**. Firstly, there is the applicability of data protection regulation. If no attempt is made to identify a person, can we define the data concerned as personal data? If not, what guarantees remain against unwarranted and unfit social categorisation? Secondly, there is the issue of profiling. It is not clear whether and when profiling falls directly under the Convention. In conclusion, the use of second-generation biometrics will have to lead to a re-assessment of the traditional data protection approach that only data relating to identify or identifiable persons have to be protected.

The Council of Europe's 2010 Recommendation on profiling[178] is an important document for member states. It contains recommendations on the collection and processing of personal data used in the context of profiling, notably by taking measures to ensure that the principles set out in the appendix to this Recommendation are reflected in their law and practice. The Recommendation states that collected data (e.g. traffic data, consumer buying habits, geo-location data, data stemming from social networks, video surveillance systems, biometric systems and RFID systems) are processed by *"[…] calculation, comparison and statistical correlation software, with the aim of producing profiles that could be used in many ways for different purposes and uses by matching the data of several individuals",* while *"[…] the development of ICTs enables these operations to be performed at a relatively low cost".* Due to this linking of a huge amount of individual, anonymous, data, the profiling technique is capable of having severe impact on the people concerned by placing them in predetermined categories, frequently without their knowledge. Data subjects' profiles make it possible to generate new personal data – even sensitive data – for which no consent has been given by the data subject. The Council of Europe concludes in its 2010 Recommendation that it is necessary

[178] Council of Europe Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (23 November 2010).

to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Several recommendations are provided in the annex.

Due to second generation biometrics an incremental change from visible to invisible data collection may occur. Biometric data may be originally collected for one specific purpose, but subsequently used for another purpose (**function creep**). It becomes more difficult to exercise the right to object to certain types of data processing. Moreover, biometric data may be used for **profiling** activities, while it is not clear whether and when profiling falls directly under the Convention. The Council of Europe concludes in its 2010 Recommendation that it is necessary to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Second generation biometrics can be used for profiling, meaning that individuals can be categorized. Unjustified selection due to profiling may result in **discrimination** and **stigmatisation**.

Chapter 6. Security risks

All biometric systems (without exception) have some intrinsic errors having a negative effect on the system's performance and accuracy (i.e. efficacy). These will be discussed in section 6.1.
Biometric data, namely, is not only valuable to the controller of the biometric system but can also be valuable to impostors as they may use such data to commit, for example, identity fraud. In order to acquire these data they may attack a biometric system. Additionally, it is not implausible that third parties obtain biometric data through intentional or unintentional data leakage. Section 6.2 identifies (some) categories of intentional impostor threats, as these are often the most striking threats to a biometric system. However, threats do not merely arise from impostor attacks, but may also emerge due to intentional or unintentional acts of the system's controllers, personnel or other individuals having legitimate access to biometric systems and/or data. Section 6.3 addresses methods to overcome the problem of compromised biometric templates, as it is a major concern in biometric applications. Section 6.4. discusses function creep and other examples of additional risk.

6.1. Intrinsic errors of biometric systems

What

All biometric systems (without exception) have some intrinsic errors having a negative effect on the system's performance and accuracy (i.e. efficacy). It is therefore important to address the different types of errors accompanying all biometric systems. The main errors are the failure to enrol, failure to acquire, false accept error and false reject error, usually expressed in the accompanying rates (i.e. proportion or probability).
The **failure to enrol rate (FTE)** reflects the proportion of individuals of whom the biometric system is unable to extract sufficient characteristics, e.g. because the individual is unable to produce an image of sufficient quality, is unable to reproduce his biometric consistently, or is unable to present the required biometric, as he for example misses a particular finger. This error is an important consideration since enrolment failures directly reduce the efficiency, accuracy and usability of the biometric system.
The **failure to acquire rate (FTA***)* reflects the proportion of attempts for which the biometric system is unable to capture an image of sufficient quality, e.g. due to an injured finger. Although the FTE and FTA are usually quite low, it is necessary to have a fall back procedure in case such failures occur, e.g. human intervention, enrolment of another finger or enrolment of a different modality (i.e. the kind of biometric) provided that the system comprises of at least two different biometric modalities, for example iris recognition and fingerprint recognition.
The **false acceptance rate (FAR)** is the probability a biometric system will incorrectly accept someone. This could be an illegitimate user who accessed the biometric system by means of spoofing, but also a person whose image/template is by accident mistakenly matched with another enrolled person's image/template. FAR is considered to be the most crucial security error of a biometric system and generally ranges from 1% (low security applications) to 0.00001% (very high security applications), although biometric vendors often quote unreliable FAR numbers and provide a best-case scenario. These rates normally concern passive impostor attempts (an imposter's attempt to spoof the system is observed by staff) as the actual rates of a biometric system in operation often remain unnoticed. The actual FAR is probably much higher, because tracing back in case of a false acceptance will generally reveal the person who

actually belongs to the biometric instead of revealing the impostor. Low false accept errors are particularly required in high security applications (e.g. nuclear power plants).
The **false rejection rate (FRR***)* is the probability a biometric system will incorrectly reject someone. Generally, FRR ranges from 0.1% to 20%[179], although an FRR of 0.1% is not likely in practice. A 2005 study conducted in the UK by Atos Origin resulted in an FRR of approximately 20% for fingerprints.[180] False rejection errors are inconvenient to a legitimate user, who needs to re-attempt the authentication process or has to be authorised by means of an alternative method (e.g. a different biometric modality or human intervention).[181]
It has to be noted that FRR and FAR are not performance criteria.[182] These numbers are units to measure the performance. The criteria are determined by the biometric system operator (also termed processor) by setting the threshold. The FAR and FRR are inversely proportional, i.e. decreasing the FAR will result in an increased FRR and vice versa. This phenomenon is sometimes called the trade-off between FAR and FRR. Main consequence is that reducing the FAR (in order to attain a higher security level), results in an increased FRR (implying reduced convenience and efficiency), and vice versa. The FAR and FRR can be adjusted by the system operator. In has to be noted that false acceptance errors and false rejection errors (and all other errors involving biometric systems) are usually tested in laboratory environments, and consequently may not be an accurate indication of the system performance in practice. Biometric system vendors often refer to testing results of the NIST (National Institute of Standards and Technology), which is the most authoritative testing institute regarding biometrics. The NIST, however, does not take into consideration particular operational circumstances, which evidently affect the testing results of a biometric system.[183] Therefore, every biometric system, especially large-scale systems, needs to be tested in a 'real world' situation.
The point of intersection of FAR and FRR (i.e. FAR=FRR) is called the equal error rate (EER), which is considered to be the best choice of operation for civilian applications.[184]

Solutions

All four intrinsic errors negatively affect the efficacy and efficiency of a biometric system. The FTE can often be reduced by means of assistance of trained personnel (human intervention) to the individuals who need to provide their biometrics. The FAR and FRR negatively affect the accuracy and efficiency of the entire biometric system and mainly depend on the quality of the biometric images (e.g. fingerprint or facial image). Therefore, the FAR and FRR can be reduced (although not to zero)[185] by increasing the quality of biometric images.[186]

---

[179] European Commission Joint Research Centre, Institute for Prospective Technology Studies, *Biometrics at the Frontiers: Assessing the Impact on Society* (hereinafter European Commission 2005), Seville, 2005, 163. Available online at: http://www.biteproject.org/documents/EU_Biometrics_at_the_Frontiers.pdf.
[180] See http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec3extra/UKPSBiometrics_Enrolment_Trial_Report.pdf.
[181] Irish Council for Bioethics Opinion 2009, 8.
[182] Wetenschappelijke Raad voor het Regeringsbeleid (WRR), the Dutch Scientific Council for Government Policy, Webpublicatie nr. 51, *Het biometrisch paspoort in Nederland. Crash of zachte landing* (hereinafter WRR 2010), Max Snijder, 2010, 111-112, via http://www.wrr.nl/.
[183] WRR 2010, 31.
[184] European Commission 2005, 49.
[185] This is due to the *intra-class variation*. The matching process (between biometric sample and stored reference template, provided that the biometric feature is stored by means of a generated template instead of the raw biometric data) does not provide a 100 per cent accurate binary yes/no answer regarding the fact whether the sample and stored reference template are identical. Instead, it is a statistical process since no two biometric samples (of the same biometric modality) from the same person are ever completely identical and therefore the biometric systems, by their very nature, generate results that are 'probabilistic'. This phenomenon is called intra-class variation and is caused by several factors such as varying ambient conditions (e.g. atmospheric humidity), imperfect imaging of the biometric, (slightly) changed biometric characteristics, or changes in the interaction between user and sensor. Due to this variation every time a person presents his biometric, the systems' algorithm provides a score of the degree of similarity between the sample and the stored reference template. The higher the degree of similarity, the more 'certain' the conclusion that the two templates belong to the same individual. The threshold level can be adjusted, depending on the specific application of the biometric system. This intra-class variation produces the intrinsic errors FAR and FRR.
[186] Unfortunately, international quality standards with respect to biometric images/templates are lacking.

The quality of images is crucial particularly in large-scale systems (systems that have stored millions of templates (i.e. transformed images/scans)) running in identification mode (1:n). Identification based systems, namely, by definition require a centralised database in which possibly millions of stored biometric templates are to be compared with the query biometric template (i.e. the fresh template as opposed to the stored reference template). The more images or templates available to compare with the query template, the higher the negative influence of image/template quality and the higher the errors involved (e.g. FAR, FRR) will be.[187] For that reason, a switch from verification based biometric systems to identification-based systems inherently comes along with increased error rates. Therefore, reducing error rates is even more important in identification based biometric systems.[188] Empirical research on large-scale biometric systems will and needs to be informing us about these threats. We will come back to India's National ID program – Aadhaar – below. Unquestionable is the need to have a coherent approach and policy with regard to these errors to avoid persons coming under pressure to offer explanations; to avoid stigmatisation; to respect the legal principles of data protection law – particularly those of data accuracy and the legal prohibition on automated decisions – and to respect basic values such as the assumption of innocence; equality; as well as the rights to free movement and freedom to travel. [189]

Experts therefore insist on organisational and technological measures with regard to the data structure mechanism allowing the operators to make corrections to the stored data and their interconnections,[190] for instance in the case of incorrectly assigned templates more generally one could say that biometric systems require human intervention be it to correct collected data and interconnections or to allow individuals to identify themselves in more classical ways.
Intrinsic errors (in particular FTA, but also FTE, FAR and FRR) can also be reduced by employing multimodal biometric systems, which make use of several biometric modalities. Two design modes offer best accuracy: (1) multiple biometrics from the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger).[191] The first option creating multimodal biometric systems, based on the collection of information from different biometrics (requiring fingerprint scans and, using voice recognition), is more concerning from a data protection viewpoint and is in tension with the idea of data minimisation. It is the option taken in the EU with the European passport. The second option for multimodal biometric systems, based on the collection of more than one unique image or more information from the same marker (i.e., multiple images of an iris, or scans of the same finger), is more respectful of these data protection requirements.[192]

[187] WRR 2010, 143. See on practical solutions for limitations such as image distortion, low image resolution, camera view angel and camera position: Pospisil R. & Skrob M., 'Actual trends in improvement of risk area security using combined methods for biometrical subject identification', *European Journal of Law and Technology*, Vol. 4, No. 2, 2013 (10p.), 4-5.
[188] Aware of the need for quality control, the National Institute of Standards and Technology (NIST) in 2004 introduced the NIST Fingerprint Image Quality (NFIQ) algorithm, which facilitates the measurement of image quality of fingerprints in order to reduce the FAR and FRR. The NFIQ is currently the most important instrument to assess the quality of fingerprints, yet not sufficiently to guarantee uniform quality.[188] Development of international quality standards for various biometric characteristics is ongoing, but not yet available in the coming years. See WRR 2010, 24.
[189] M. Pocs, 'Legally compatible design of future biometric systems for crime prevention', 51
[190] More in detail: M. Pocs, 'Legally compatible design of future biometric systems for crime prevention', 51; Pospisil R. & Skrob M., 'Actual trends in improvement of risk area security using combined methods for biometrical subject identification', *European Journal of Law and Technology*, Vol. 4, No. 2, 2013 (10p.), 7-8
[191] Irish Council for Bioethics Opinion 2009, 55.
[192] Wikipedia refers to the following Article for a detailed discussion of tradeoffs of response time, accuracy, and costs between integration modes: Soyuj Kumar Sahoo, Tarun Choubisa, SR Mahadeva Prasanna (1 January 2012). 'Multimodal Biometric Person Authentication : A Review'. *IETE Technical Review* 29 (1): 54. doi:10.4103/0256-4602.93139

All biometric systems (without exception) have some intrinsic errors which have a negative effect on the system's performance and accuracy.
All identified intrinsic errors negatively affect the efficacy and efficiency of a biometric system. These errors impact negatively on a series of legal values (such as data accuracy) and human values and need to be addressed accordingly through a series of organisational and technical measures. Accordingly, how best to consider these problems ought to begin in the design phase of the system.
One controversial solution to errors is employing multimodal biometric systems. Two design modes offer best accuracy: (1) multiple biometrics from the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger). From a data protection perspective, asking for more biometrics to enhance efficiencycan be problematic.
It can be concluded that the biometric systems' performance and accuracy depend on error rates, which can be reduced – for example by human intervention, technological options to correct stored data and interconnections, multimodal biometric systems or a higher quality of biometric image. The European legal framework on data protection should include provisions aiming to reduce the errors of biometric systems, such as provisions on human intervention, multimodal biometrics, high quality images and fallback procedures.

6.2. Impostor threats

Impostor threats can be defined as impostors' intentional efforts to illegitimately access or circumvent the biometric system. A significant impostor threat is an attack to the biometric database (*database attack*). Large-scale central databases are more susceptible to such database attacks, compared to decentralised databases. Although large-scale databases are often better protected, an impostor can obtain a large amount of (valuable) biometric information through one attack. Impostors may also take away objects with latent fingerprints on them.
Jain *et al* have categorised impostor threats into three main classes, with regard to the biometric system (not necessarily including a biometric database): administration attack, no secure infrastructure, and biometric overtness.[193]
Administration attack concerns vulnerabilities due to improper administration of a biometric system. Such an attack compromises the integrity of the enrolment process (e.g. whether the correct credentials are presented), and may include coercion or collusion between an impostor and the system operator (e.g. intentional leakage) or a legitimate user (e.g. enrolment fraud).
Nonsecure infrastructure concerns vulnerabilities due to manipulation of software, hardware and communication channels inside the biometric system, possibly resulting in security breaches. Examples of infrastructure vulnerabilities are: **Trojan horse attacks** (input of malicious software to manipulate data in the biometric system), **replay attacks** (circumventing the sensor by inserting a recorded image from a legitimate user back into the biometric system), **tampering** (modifying data in stored templates or during authentication in order to guarantee a high match score of one's own biometric), **masquerade attack** (submitting an artefact image, created from a fingerprint template, but not necessarily resembling the original image, to ensure a match), **substitution attack** (accessing or overwriting a stored template, or replacing this template by the impostor's template), **overriding the yes/no response** (inserting a false yes (i.e. match) response in the biometric system in order to pose as a legitimate user).[194]

[193] A.K. Jain, K. Nandakumar & A. Nagar, 'Biometric Template Security', *EURASIP Journal on Advances in Signal Processing*, Special Issue Advanced Signal Processing and Pattern Recognition Methods for Biometrics, 2008, vol. 8, 2-3, via http://www.hindawi.com/journals/asp/2008/579416, 2-3.
[194] Irish Council for Bioethics Opinion 2009, 10; A.K. Jain, K. Nandakumar & A. Nagar, 'Biometric Template Security', 4.

Biometric overtness concerns vulnerabilities due to the use of physical artefacts of a biometric trait subsequent to the covert acquisition of such traits from a genuine user. If the biometric system is incapable of distinguishing between a genuine biometric presentation and an artificial biometric spoof, an impostor can circumvent the system by means of spoofing.

6.3. Biometric template protection

In chapter 2 we discussed the fifth recommendation of the 2005 COE progress report stating that biometric templates should be used instead of raw biometric data because of many advantages in terms of data protection (the idea of cancellable biometrics). In principles, templates, - a mechanism analogous to **hash** codes – allow the same functions as the raw data; templates are also not reproducible, and it is in principle not possible to recreate their original image or sound data.
A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric.[195] As a result of intra-class variation,[196] it is impossible to store a biometric template in an encrypted form (through standard encryption methods) and subsequently perform matching in the encrypted domain.[197] Even small differences in the values of feature sets, which are extracted from the raw biometric data, will lead to enormous differences in the resulting encrypted features. To overcome this problem one could decrypt the template and then perform matching between the query template and the decrypted reference template. However, it has been demonstrated by Feng and Jain that a minutiae template (i.e. template of a fingerprint) can be reverse engineered into the original image, which may pose security risks to the biometric template, the biometric data as such and consequently the privacy of users involved.[198] Previously, scientists faced the problem of (additional) spurious minutiae generated in the reconstructed image, while these minutiae were not included in the original minutiae template. Feng and Jain have overcome this problem by creating a novel algorithm enabling the reconstruction of the fingerprint with limited spurious minutiae. The algorithm was evaluated in respect of two categories of attacks (matching the reconstructed fingerprint against the original fingerprint and matching the reconstructed fingerprint against different impressions of the original fingerprint) by means of a commercial fingerprint recognition system.[199] Feng and Jain demonstrated that both attacks can be successfully performed using the reconstructed image. Hence, the protection of biometric data does not merely comprise data storage, but also the entire process of retrieving the reference template during the authentication procedure, including the decryption of the template and the matching process.

Ideal properties of template protection design

As conventional encryption techniques require decryption in order to compare the query template with the reference template, which poses risks to the biometric data, they do not possess the four properties of an ideal biometric template protection design to prevent impostor attacks, and additional threats: diversity, revocability, security, and performance.[200] Diversity encompasses protection against cross matching across databases in order to guarantee the user's privacy. Revocability refers to the possibility to revoke the compromised biometric template

[195] Feng and Jain demonstrated that a fingerprint template can be reconstructed into the original image, see J. Feng & A.K. Jain, 'Fingerprint Reconstruction: From Minutiae to Phase', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2011, vol. 33, no. 2, 209-223.
[196] See chapter 6.
[197] A.K. Jain, K. Nandakumar & A. Nagar, 'Biometric Template Security', 6.
[198] J. Feng & A.K. Jain, 'Fingerprint Reconstruction: From Minutiae to Phase'. Feng (member of IEEE) and Jain (fellow of IEEE) are currently conducting research on 'Fingerprint Reconstruction From Minutiae' at the Department of Computer Science and Engineering of Michigan State University, see http://biometrics.cse.msu.edu/projects/fingerprint_reconstruct.html.
[199] J. Feng & A.K. Jain, 'Fingerprint Reconstruction: From Minutiae to Phase', 209.
[200] A.K. Jain, K. Nandakumar & A. Nagar, 'Biometric Template Security', 5-6.

and reissue a new template, based on the same previously provided biometric data, without the need to re-enrol. Security of templates involves protection against adversary attacks through mathematical algorithms. Performance entails the obtaining of template protection without degrading the recognition performance (FAR, FRR) of the system. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorised in **feature transformation** and the employment of a **biometric cryptosystem.**[201] Basically, feature transformation is encryption of a biometric and biometric cryptosystems generate a cryptographic key directly from or with help of the biometric (i.e. biometrically facilitated encryption). So, simply put, feature transformation and biometric cryptosystems operate reversely. Feature transformation is the most significant template protection design with respect to this thesis as it produces a yes/no response (i.e. match or non-match), as in conventional non-transformed biometric systems. Biometric cryptosystems, on the other hand, produce a cryptographic key, which technique is therefore less usable for verification and identification purposes.

Biometric systems are susceptible to several threats, such as impostor threats (e.g. identity fraud, biometric database attack, enrolment fraud, spoofing and Trojan horse attacks) and additional threats (e.g. function creep, tracking and tracing, linking of biometric data to other personal information, system failures and leakage of biometric data). Several mechanisms to overcome vulnerabilities in biometric systems are human intervention, human supervision, liveness detection and multimodal biometrics. A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorised in **feature transformation** and the employment of a **biometric cryptosystem**. Both are effective methods to protect biometric templates. Although biometric templates as such are significantly safer than the use of raw biometric data, the country reports show that very few countries address the need to use templates. The Council of Europe's 2005 progress report and the 2011 Parliamentary Assembly both recommend the use of **templates** instead of raw biometric data, but Mr Haibach's recommendations (in the 2011 report) regarding the use of templates have been noticed only in **Estonia** and **Italy**. The Estonian report underlines the importance to use biometric templates instead of raw biometric data.[202] The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects. For example, the storage of **encrypted templates** exclusively held by the data subject should be preferred over storage in central databases. Data protection legislation should include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.

6.4. Function creep and other additional threats

Several other threats apart from impostor threats exist. This section does not intend to give an exhaustive overview of all possible additional threats, but limits itself to some examples to show that the threats to biometric data and systems not only arise from impostor attacks, but can also arise from acts of controllers of biometric systems, personnel or other individuals having legitimate access to biometric systems and/or data – such acts may be performed intentionally. Equally, biometric information may be originally collected for one specific purpose, but subsequently intentionally used for another purpose. This phenomenon is generally termed function creep.

[201] A.K. Jain, K. Nandakumar & A. Nagar, 'Biometric Template Security', 6.
[202] See chapter 7 for the Estonian response to the questionnaire.

Other examples of threats are surveillance activities (tracking and tracing of individuals) or the use of biometric systems for otherwise excessive control activities by governmental institutions or private companies, as biometric data can be covertly collected. Also, the linking of biometric data to other personal information, a threat which is particularly present in case of storage of biometric data in databases, may cause privacy concerns. Biometric templates stored in such databases may also be matched against templates in other databases, a phenomenon called cross matching.
Unintentional threats, on the other hand, are threats to the biometric system or biometric data without necessarily the intention of deliberate misuse. Some examples of unintentional threats are system failures, accidental leakage (by individuals who have access to the biometric data), derivation of additional personal information from biometric data (e.g. ethnic origin or health information) or the case where some biometric data are (left) in the public domain (e.g. someone's face is taken 'public information' or fingerprints left on a glass).

It is easy to imagine scenarios where some of these threats come together. Matthias Pocs offers a scenario of airport police that scan fingerprint traces left on luggage before boarding. Should a terrorist cause the aircraft to crash, the data captured before the flight are searched against already known data from a database of criminals. This is one example of possible future crime detection scenarios where biometric data play a role. In this scenario the police captures data before knowing that the person checked is a criminal or before a crime is committed. Pocs speaks about precautionary data capture where biometric characteristics are captured without the individual having given cause for suspicion, and where a large number of persons are subject to the practice.[203]
Pocs thesis is that societies can avoid risks to individual freedoms and democracy caused by these scenarios by means of technology and organisational design. Function creep and creeping surveillance can be controlled and avoided to a certain degree.
Although this message might be hopeful, it is important to see that function creep can emerge from simple human calculation and the using available resources. The examples of massive scale databases such as Eurodac and the Passport system are striking. Not having access to biometric databases of all citizens, it is more than temping for law enforcement agencies to turn to these databases and push for access right to them. When the legislator is responsive to these calls, there is very little that one can do to stop formalised function creep. A Dutch committee of experts, the Meijers Committee, is of the opinion that access for law enforcement authorities and Europol to Eurodac violates fundamental rights of asylum seekers, including the right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment, and will lead to stigmatisation of this particular group. However, taking into account the political reality that policy makers are willing to create powers for such an access, the Meijers Committee saw no other solution than to suggest certain legal amendments to improve the standards in Eurodac and to regulate access with sufficient safeguards.[204]

In 2007, a study shone a spotlight on this process of governments approving one law after another, each of which drastically increased the intelligence-gathering powers of the police, judiciary and intelligence services.[205] The central message in the analysis is the difficulty in those processes to have a societal discussion on the overall effect of these developments. Public discussions about these measures in general were very limited. It seems that, if a discussion

[203] M. Pocs, 'Legally compatible design of future biometric systems for crime prevention', 51
[204] The Meijers Committee update No.1 March 2013, http://www.commissie-meijers.nl/assets/commissiemeijers/Meijers%20Committee%20Update%20No1_March%2020133.pdf
[205] A. Vedder, L. Van Der Wees, E.-J. Koops & P. De Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*, Den Haag, Rathenau Instituut, 2007, Studie 49, 90p.

arises, it mostly concerns just one individual measure; how these measures interact – and possibly reinforce each other – is not considered.
A well-considered opinion about the security measures and how these affect the privacy of individuals requires an understanding of these cumulative effects. How the balance between privacy and other interests should be sought, depends upon the exact context concerned. One author rightly observes that the function creep mechanism, even underpinned by regulatory reform, makes the balancing exercise more opaque: taken individually, new legal powers can be said to be 'privacy conform' but taken together they loose their proportional nature.[206] What is lost in the process is the contextual integrity: information used in one context is applied in another context without taking into account the original context-specific meaning, creating the likelihood that inaccurate images of the person concerned and undermining the trust needed in the respective context to develop meaningful relations. [207] Legally speaking, the core idea of purpose-limitation is sacrificed in the name of security: information can be accessed when needed for security purposes without additional concrete balancing of interests.[208]

Regarding function creep, we need to refer to the European Court of Justice (ECJ) 2008 judgment *Huber* regarding the use for crime fighting purposes of a system of processing for personal data of non-national EU citizens.[209] The proceedings dealt with the existence in Germany of a centralised, nationwide database containing information on non-German EU citizens for the sake of applying the law relating to the right of residence, and its use by German authorities to fight crime. The register was in place even though no similar register had ever been created to store equivalent information on German citizens, so no equivalent processing of German citizens' personal data ever took place. The European Court of Justice was required to examine different questions in relation to the existence of such a database and the secondary use of its content.
The issue of discrimination was at the very core of the case. Indeed, the European Court of Justice concluded that the database discussed was not contrary to Community law insofar as it contained only the data necessary for the application of residence legislation, and insofar as its centralised nature enabled such legislation to be more effectively applied. However, it established that its use for crime fighting purposes had to be interpreted as the putting in place of a system of processing for personal data precluded by the principle of non-discrimination of EU-citizens. In its assessment, the Court took the view that, as the fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of the nationality of their perpetrators, it follows that, as regards a member state, the situation of its nationals cannot be different in relation to this objective from that of non- national EU citizens who are resident on its territory.

The Advocate General appointed to the case, Poiares Maduro, had arrived at the same conclusion concerning the discriminatory nature of the processing of the registered personal data for the sake of crime fighting.[210] Poiares Maduro had pointed out that the coexistence of different data processing practices, one for nationals and the other for non-national EU citizens

[206] R. Leenes, 'Denk na, omdat het kan', in H. van Kempen & G. Munnichs (dds.), *Privacy - Kenniskamer 17 december 2009*, The Hague, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2010, 39
[207] R. Leenes, 'Denk na, omdat het kan', 40 with ref. to H. Nissenbaum, 'Privacy as contextual integrity', *Washingon Law Review*, 2004, vol. 79, 119-158
[208] E. Dommering, 'Privacy als zelfbeschikkingsrecht', in H. van Kempen & G. Munnichs (dds.), *Privacy - Kenniskamer 17 december 2009*, The Hague, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2010, 56
[209] ECJ, *Huber v. Germany*, Case C-524/06, Judgement of 16 December 2008. See Gl. González Fuster, P. De Hert, E., Ellyne & S. Gutwirth, 'Huber, Marper and Others: Throwing new light on the shadows of suspicion', *Inex Policy Brief*, June 2010, No. 11, 8p. http://www.ceps.eu/book/huber-marper-and-others-throwing-new-light-shadows-suspicion

[210] Poiares Maduro (2008), *Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v Bundesrepublik Deutschland)*, delivered on 3 April 2008

– the latter being much more strictly and systematically monitored – casts an "unpleasant shadow" over non-national EU citizens. The Advocate General underlined that, although the combating of crime and threats to security can be a legitimate public policy reason qualifying rights granted by Community law, it cannot justify the difference in treatment between nationals and non-nationals that are citizens of other member states: member states cannot invoke such an aim selectively.
The importance of the *Huber* judgment lies in the emphasis put on the issue of discrimination, and in particular on the indirect effects of foreseeing secondary uses of information originally stored for other purposes. It warns against the temptation, apparently regularly experienced by policy-makers, to allow for the use of any existing database or available data for the purpose of crime fighting. The grounds for, and limits to, such initiatives are often sought in the nature of the crimes to be investigated, as if the seriousness of some crimes could justify all kinds of data processing operations. The ruling, however, recalls that these decisions need also to take into account the **shadows of suspicion** that are de facto projected by different data processing practices.

6.5. A critical note on the EU passport system and the Aadhaar system

On Thursday January 23rd, 2014 a panel was organised at the Conference CPDP 2014 discussing 'Biometrics in India', with experts such as Nikhil Dey, MKSS (IN), Travis Hall, Humboldt Institute for Internet and Society (DE), Malavika Jayaram, Jayaram & Jayaram lawfirm (IN), R. Ramakumar, Tata Institute of Social Sciences (IN).[211] The central topic was Aadhaar, India's National ID program. Aadhaar is the largest biometric database of the world, already operational and aiming to cover the entire population of 1.25 billion in the next few years.[212] The system was set up to enable better governance, with significant humanitarian and social welfare goals. Through the system a biometrics-based digital identity is assigned for a lifetime, verifiable online instantly in the public domain, at anytime, from anywhere. The system is completely paperless. This identity is based on biometric data (fingerprint, iris scan and face photo), along with the demographic data (name, age, gender, address, parent/ spouse name, mobile phone number) of a person. All citizens enrolled receive an 'Aadhaar Number' that is written on a piece of paper, but it should be stressed, this paper is not the intended purpose of the system. The stated purpose is that the digital identity verifiable online.
The civil liberty and academic members of the CPDP panel stressed several serious problems with this database. The first is the poor legal basis for the system – there is in fact no explicit law to back the system. Underneath we highlight two to three others:
- errors: the system contains many errors ranging from persons enrolled twice in the system without it being noticed, and even the enrolment of a dog, again unnoticed. Large quantities of the rural population simply have no reliable fingerprints and clearly not all of the 50,000 operators enrolling citizens are adequately skilled and trained;
- consent and function creep: enrollment is based on consent but many authorities make vital societal services dependent on enrolment and the police treats citizen without an Aadhaar number as more suspicious.

Europe might think conditions are better on this side of the world, but this would be a rash assumption. Unfortunately, the problem with the significant errors of biometrics discussed in this chapter are regularly being underestimated, for example by the European Court of Justice.[213]

[211] See www.cpdpconferences.org
[212] See also http://en.wikipedia.org/wiki/Biometrics
[213] ECJ, Case C-291/12 of 13 June 2013 (*Michael Schwarz v. Stadt Bochum*).

We saw in our discussion of the *Michael Schwarz v. Stadt Bochum* judgment (2013) in chapter four of this report that the Court had very little difficulty with error rates and mismatches, since these would only lead to human interventions by border authorities and then corrections. The question whether those human interventions are experienced as pleasant was not addressed. The question of what an error rate of 1 percent means for millions and millions of citizens remained equally unconsidered. We also saw that the EU voted an EU Regulation without properly addressing all the issues at stake (central storage or not/ function creep or not/further use by law enforcement agencies or not?). The Court has in principle acknowledged that further use might be an option, but not on the basis of article 1(2) of Regulation 2252/2004.[214] In principle there was thus no problem with the original idea in the Netherlands to create a central database of fingerprints and to allow law enforcement access to this database.

[214] We recall that with regard to the processing of fingerprints, the Court notes that fingerprints play a particular role in the field of identifying persons in general. Thus, comparing fingerprints taken in a particular place with those stored in a database makes it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly. However, the Court also notes that the regulation explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder. Moreover, the regulation does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone. The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the EU.

Chapter 7. Country responses to the questionnaire

7.1. Introduction: responses of 22 out of 47 countries

The questionnaire containing 7 important questions regarding the use of biometrics was sent to 47 countries, of which 23 responded. Portugal has been omitted from this report because it did not want its reply to be published. Therefore, this chapter contains the responses of 22 countries which are provided in alphabetical order in the following 22 sections. Each section (i.e. each country report) contains the summarised answers of the member states that provided responses to the 7 questions of our questionnaire. The most interesting information (noted as 'Information of interest') to our report is contained in boxes at the end of each section. Note that no responses were obtained from countries such as Slovakia and the Czech Republic, although existing guides on data protection law suggests that specific provisions do exist. [215] We will use these guides where appropriate to clarify some of the responses.[216]

7.2. Albania

Remark: the general data protection framework was laid down in Act No. 8517, dated July 22, 1999
On the Protection of Personal Data,[217] replaced by the Act on Personal Data Protection No. 9887, dated 10 March 2008, that implemented the 95/46/EC Directive.[218]

1. No specific legislation regarding biometrics. Biometric data are addressed in data protection legislation and considered personal data. Also, provisions on biometrics in police legislation.
2. Fingerprints are used for Albanian ID cards and biometric passports
3. Not indicated
4. Not indicated
5. Yes, a fingerprint database needed for the production and issuance of citizens' identity documents, and a central biometric database for police legislation including fingerprints, facial images, and DNA samples.
6. No report that systems or data have been attacked or corrupted.
7. No answer

Information of interest: The Albanian report underlines that the Ministry of Interior is the owner and controller of the personal data, including biometric data, needed for the issuance of ID cards and biometric passport.

7.3. Austria

Remark: The general framework is provided for by the Federal Act concerning the Protection of Personal Data (Bundesgesetz über den Schutz personenbezogener Daten (*Datenschutzgesetz*

[215] See on Czech Republic: Eva Ruhswurmová, 'Czech Republic', in DLA Pipers, *Data Protection Laws of the World*, 2013, 69-74; CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 9. See on Slovakia CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 41 & 45.
[216] We also rely on Linklaters, *Data Protected*, 2005, 116p. via www.linklaters.com; on http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.LegislationbyCountry and on http://www.ceecprivacy.org/main.php?s=2.
[217] http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.AL
[218] http://www.ceecprivacy.org/main.php?s=2&k=albania

2000") dated 17 August 1999 which was last revised on 31 March 2005 and implemented the EU Data Protection Directive 95/46/EC.[219]

1. Provisions on DNA are incorporated in police legislation and the penal procedure act. All EU regulations in this area (e.g. Eurodac regulation, and Prüm decisions) are fully implemented in different national acts.
2. The latest technical generation of identification databases, including facial images, fingerprints (AFIS – automated fingerprint identification systems) and DNA databases.
3. Only in the public sector:
   AFIS system and picture databases for police legislation and asylum
   DNA analysis and DNA database for police legislation and asylum
   Fingerprints for acquisition and storage in national passports and ID cards
4. Passports have been issued to persons who have been using a stolen identity while applying for the passport.
5. Yes, in the public sector.
6. No.
7. No such research has been conducted.

Information of interest: The Austrian report underlines that in accordance with Austrian law fingerprint images which have to be stored on the chip of the electronic passport have to be deleted from the database after issuing the document. In some cases passports have been issued to persons who have been using a stolen identity while applying for the passport. It is remarkable that the Austrian report states that this could have possibly been prevented if the fingerprints had been stored in a central database permanently and the passport authority had the right to use this data. The central storage of biometric data, namely, poses more risks for function creep or linking of data to other databases.

7.4. Denmark

Remark: Denmark implemented the EU Data Protection Directive 95/46/EC with the Act on Processing of Personal Data dated 31 May 2000.[220]

1. Only police legislation regarding DNA. New legislation being prepared regarding the processing of fingerprints, including rules on deletion of personal information within a central register of fingerprints.
2. State of the art IT-tools for DNA-comparison and fingerprint identification. The DNA register is currently being transformed to the CODIS system. The fingerprint identification system is being exchanged to an AFIS system.
3. The CODIS system for DNA, and an AFIS system for fingerprints.
4. No answer
5. Public databases on fingerprints and DNA, containing both identified persons, previously known for criminal activities, and crime scene traces.
6. No biometric systems were hacked or compromised.
7. Research is continuously being conducted on DNA, primarily by external authorities such as the Department of Forensic Medicine at the University of Copenhagen.

[219] W. Freund, 'Austria', Chapter 3 in DLA Pipers, *Data Protection Laws of the World*, 2013, 17-21; Schönherr Rechtsanwälte OEG, 'Austria', in Linklaters, *Data Protected*, 2005, 11-13
[220] E. Husum, 'Denmark', Chapter 14 in DLA Pipers, *Data Protection Laws of the World*, 2013, 75-19; G. Federspiel Kierkegaard, 'Denmark', in Linklaters, *Data Protected*, 2005, 27-28.

Information of interest: The Danish report underlines that the use of AFIS (Automated Fingerprint Identification System) will be supplemented with a number of live scanners situated around the country in specific strategic places.

7.5. Estonia

Remark: The general framework is laid down in the Personal Data Protection Act (*lsikuandmete kaitse seadus* dated 12 February 2003) and also the implementation act of Directive 95/46/EC.[221]

1. Yes, biometric data is framed by the 2003 data protection act and considered sensitive personal data. National DNA register and national fingerprint register regulated by national legislation.
2. Biometric passports and DNA sample database. Estonia has all the most commonly used biometric technologies.
3. Public sector: biometric passports, DNA register, fingerprint register
   Private sector: fingerprint and iris scans used for security and workplace entry reasons.
4. Problems with the private sector using security systems that use biometric data (like fingerprints, palm prints or iris scans) for identifying workers. According to the Estonian Personal Data Protection Act sensitive data cannot be used for performance of a contract. For the use of biometric data for security reasons the consent of the data subject is needed. The advisor of the Estonian Data Protection Inspectorate recommends using systems that don't record the biometric image but create a code from the image and use that.
5. Yes, a national DNA register and a national fingerprint register. Both are regulated by national law.
6. No information on that matter
7. No information on that matter

Information of interest: The Estonian report underlines that biometric data is considered sensitive personal data in the Estonian data protection act. Our research has not confirmed this. However, Article 4 defining personal data mentions as one of the categories of sensitive personal data as relating to genetic information (Article 4(3)).
Answer 3 mentions private sector use of biometrics (fingerprints and iris scans) for security and workplace entry reasons. The advisor of the Estonian Data Protection Inspectorate recommends the use of systems that don't store biometric images but a biometric template of that image. It can be concluded that the recommendations of Mr Haibach have been noticed in Estonia.

7.6. France

Remark: The general data protection framework in France is provided for by Act No. 78 17 of January 6, 1978 on Information Technology, Data Files and Civil Liberty (the 1978 Act). The EU Data Protection Directive 95/46/EC was implemented via an act (Act No. 2004 8021) of August 6, 2004 that amended the 1978 Act.[222]

1. The processing of biometric data is governed by the rules laid down in the 1978 Act
2. CNIL (*Commission nationale de l'informatique et des libertés*), the French Data Protection Authority), has recently assessed the use of the venous networks of the hand, speech or typing recognition, multimodal devices combining face images in two dimensions, iris scan,

[221] Raidla & Partners, 'Estonia', in Linklaters, *Data Protected*, 2005, 29-31,
[222] C. Umhoefer, 'France', Chapter 18 in DLA Pipers, *Data Protection Laws of the World*, 2013, 93-98

and speach verification. The objectives for implementing biometric processing are changing too. Apart from classical control of access to premises or to computers, venous patterns are used for bank payment, iris and voice recognition for security of information systems and fingerprints in a hospital to identify critically ill patients with certainty.

3. Technological developments make the CNIL's position necessary to change. For example, hand geometry was favoured by the CNIL so far because it leaves no trace. But the venous system has now the same qualities and its use could be reconsidered for purposes such as for recording working hours and for the security of specific protected areas. The difficulty in using fingerprints combined with a centralised database still remains, even though some changes have been made.
4. Palm printing, iris scan, and "hand venous pattern". Other technologies such as facial or voice recognition are still experimental.
5. The situation is changing regarding the public sector due to the evolution of European legislation. So far CNIL was of the opinion that storage in a centralised database is only possible for biometrics with "no trace". But these are very limited databases. Concerning fingerprints, the use of centralised databases is strictly supervised. In the private sector, the use of such databases is only allowed "for a strong security imperative" such as monitoring patients in radiotherapy in a hospital. Regarding the public sector, CNIL has always opposed to the creation of a centralised database of fingerprints by insisting on having a parliamentary debate. As a result, the government decided to give up the proposed biometric identity card, which relied on the creation of a centralised fingerprints database. The first time the French government decided to implement a centralised fingerprints database was in 2009 for the application of the European Regulation 2252/2004 (EC) of 13-12-2004 on security features and biometrics in passports. Later, the government implemented a centralised biometric database for the management of its "control return assistance" policy, which aims at giving financial assistance to foreigners wishing to go back to their countries. This fingerprints database detects any new application by a person who has already benefited from this financial assistance under another identity.
6. No information on this issue.
7. Two projects have been authorised by CNIL:
   - "Technology Vision Techno-vision" is led by the University of Evry Val d'Essonne, an independent public research organisation. It is supported by the Ministries of Research and Defense. Its aim is to create a database and conduct multimodal assessment of recognition systems developed by other research laboratories.
   - "3DFACE" is led by Sagem Défense, a private research group, coordinated by "Sagem Défense Sécurité". It is part of the IST program (Information Technology for the Information Society) of the European Commission and brings together twelve partners in the European Union.

   CNIL does not have a report so far.

Information of interest: The processing of biometric data is framed by the general data protection act. Prior checking: biometric processing needs to be authorised by the CNIL. Double check in the public sector: the implementation of biometrics is subject to a decree of the Council of State, adopted on the basis of the DPA's opinion.
Strict regulation, and since 2004, a doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. Biometric devices are categorised based on their risks to privacy and data protection:
- "with a trace": fingerprints and palm prints. The use of these devices is considered to involve significant risks in terms of privacy. CNIL has been particularly cautious about the use of fingerprints;
- "without a trace": hand geometry, finger vein patterns;
- "intermediate": voice and face recognition, iris scans.
The CNIL considers the use of "with a trace" biometric device to be legitimate if the biometric data are stored on a storage medium under the exclusive control of the data subject, as opposed to storage in a centralised database. In the private sector, the deployment of a centralised database should be linked to a "strong security imperative" that the CNIL will assess.
The doctrine evolves continuously due to new biometric developments and European legal developments such as Regulation 2252/2004 (EC) on biometrics passports.
In France, venous pattern technology is used for bank payments; iris recognition and voice recognition are used for security of information systems, and fingerprints in a hospital to identify critically ill patients with certainty.
The French Data Protection Authority CNIL is one of the few countries that apply prior checking.

7.7. Georgia

1. The processing of biometric data is regulated in the general data protection act.
2. The Civil Service Development Agency uses several biometrics. Facial images for several national documents and face recognition systems. Fingerprints for travel documents (based on the ICAO recommendations) and for the automatic border crossing system ("eGate"). The Civil Service Development Agency is currently working on a document ("Seamen's book") in which the biometric fingerprint template will be introduced as a 2D barcode, based on the ILO "Seafarers' Identity Documents Convention" 2003 (No. 185).
3. The Civil Service Development Agency is using facial images and fingerprints for biometric passports and facial images for national ID cards. Both of these documents are issued by the Ministry of Justice of Georgia. Other governmental institutions are also using biometric images for their document issuance purposes. In addition, both private and public sectors are using fingerprints for access systems.
4. The Civil Service Development Agency has not encountered any problem regarding the issue.
5. The Civil Service Development Agency has a central database of biometric data, which is primarily used for citizen identification purposes.
6. No.
7. No research regarding biometrics has been conducted.

Information of interest: the Georgian data protection act explicitly states in Article 2(b) biometric data as a special category of data. Article 2(c) defines biometric data as any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person. Article 9 paragraph 1, on the processing of biometric data by a public institution, reads as follows: "*The processing of biometric data by a public institution shall be allowed only for the purposes of the security of person and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts*." Article 10, on the processing of biometric data by a private person, includes a notification obligation for the biometric system's processor. Article 10 reads as follows: "*The processing of biometric data by a private person shall be allowed only if it is necessary for the purposes of conducting activities, for the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts. Before using biometric data, a data processor shall notify a personal data protection inspector detailed information on the processing of biometric data, including the information notified to a data subject, the purpose of the processing of data and the safeguards of the protection of data, unless otherwise provided by the law."*

7.8. Hungary

Remark: The Hungarian Act CXII of 2011 on the Right of Self-Determination in Respect of Information and the Freedom of Information ('Data Protection Act') is based on Directive 95/46/EC and sets the general framework for data protection. Apparently there is no reference to biometrics.[223] In what follows, we reproduce the responses to the questionnaire.

1. Biometrics are regulated in acts on (1) genetic research and biobanks, (2) law enforcement, and (3) travelling abroad.
2. Biometric passports, which include a chip: personal data (personal identification data, signature, and facial image of the applicant) and fingerprints (protected by special encoding) of the holder. Fingerprints are introduced due to the mandatory provisions of Regulation 2252/2004/EC.
3. Biometrics are being used in the public sector. Records of Criminal and Police Biometric Data contain fingerprint data and DNA-profile data. The main purpose of this record is the identification of potential perpetrators and suspects, deceased persons with unknown identity as well as convicted persons upon receipt into a penitentiary institution etc. Biometric passports containing digital facial images.
4. Hungary is facing increasing penetration of biometric identification systems. In this regard, petitions requesting a position on the usability of biometric entry control systems, fingerprint driven, based on cases so far, have become ever more frequent. With advances in technology, the trend of camera surveillance and using biometric entry control systems has proliferated and has already reached schools. The former Data Protection Parliamentary Commissioner emphasized in several resolutions and recommendations that instead of applying biometric entry control systems which affect the privacy of the individual, the use of other less intrusive methods (e.g. admission cards with magnetic stripes holding serial numbers or barcodes or other means as a replacement for biometric identification) of personal identification are advisable.

[223] See on Hungary CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 14-20.

5. In the public sector: the Records of Criminal and Police Biometric Data contain fingerprint data and DNA-profile data. The main purpose of this record is the identification of potential perpetrators and suspects, deceased persons with unknown identity and convicted persons upon entry into a penitentiary institution etc.
6. No information.
7. Not answered.

Information of interest: The former Data Protection Parliamentary Commissioner emphasised in several resolutions and recommendations that instead of applying biometric entry control systems which affect the privacy of the individual, the use of other less intrusive methods (e.g. admission cards with magnetic stripes holding serial numbers or barcodes or other means as a replacement for biometric identification) of personal identification are advisable.

7.9. Ireland

Remark: The core Irish data protection law is comprised in the Data Protection Act 1988 ('1988 Act') as amended by the Data Protection (Amendment) Act 2003 ('2003 Act') (together the Data Protection Acts ('DPA')). The 2003 Act implemented the EU Data Protection Directive (95/46/EC).[224]

1. The processing of biometric data is framed by the general data protection act.
2. Not answered.
3. Authentication systems: identification systems and verification systems (typically storage on a card).
4. The principal difficulty across all sectors arises from attempts to introduce biometric systems without consultation and without the consent of intended users (e.g. employees in the workplace).
5. No central database in Ireland.
6. There are no known incidents of hacking or compromising biometric data in Ireland.
7. The Data Protection Commissioner has two guidance notes on his website:

   Biometrics in the workplace:
   http://dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/bio.htm; and

   Biometrics in Schools, Colleges and other Educational Institutions:
   http://www.dataprotection.ie/viewdoc.asp?DocID=409.

Information of interest: Attempts to introduce biometric systems without the consultation or consent of data subjects (e.g. employees in the workplace).

7.10. Italy

Remark: Italy's consolidated data protection code came into force on 1 January 2004. This Code brings together all the various laws, codes and regulations relating to data protection since 1996. In particular, it supersedes the Data Protection Act 1996 (no. 675/1996), which had come into effect in May 1997.[225]

[224] See Ph. Nolan, 'Ireland', Chapter 27 in DLA Pipers, *Data Protection Laws of the World*, 2013, 142-147
[225] http://www.garanteprivacy.it/home_en/italian-legislation. See also G. Olivi, St. Baldazzi & G. Marino, 'Italy', Chapter 28 in DLA Pipers, *Data Protection Laws of the World*, 2013, 149-158

1. The processing of biometric data is framed by the general data protection act:
   - The processing of biometric data must be notified to the DPA. Under the Italian code, organisations are required to notify the DPA (Garante) when processing higher-risk categories of data. These include, in particular, genetic and biometric data, data processed for the purpose of analysing or profiling individuals, and credit-related information (see Section 37 of the code for additional details).
   - Prior checking of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects.
   - The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.

In addition, Italy implemented EU legislation concerning the processing of biometric data in specific sectors or for specific requirements. In particular, EU regulation defining specific standards for electronic passports, including the obligation to store two fingerprints (not templates thereof) in the relevant chip in order to allow identity verification and EU regulation establishing huge EU databases containing biometric data (e.g. Eurodac, and VIS).

2. The processing of graphometric data is becoming more widespread for the secure signature of documents, mainly in the banking and insurance sectors and in connection with utilities. A few biometrics-based techniques are used (not on a regular basis) in connection with IT-authentication procedures, which are envisaged as minimal security measures. Fingerprints are mostly relied upon. Hand contour and/or fingerprints are used in some cases for physical access control. The processing of video surveillance data is performed for the recognition of bodily traits for physical access control, mainly in the banking sector (anti-robbery and anti-camouflage checks). The processing and analysis of genetic data are offered also online on a 'do-it-yourself' basis.
3. Biometric systems in the workplace, in particular for the control of employees' access to workplace areas. Other cases concern the use of biometrics for access to banks, sports centres, and schools. In 2008, the Italian DPA laid down specific recommendations and measures with regard to the Ministry of Interior's 'Guidelines on the collection of fingerprints of members of the country's Roma community'. Other databases containing biometric data are those related to Eurodac and VIS. Moreover, the Italian immigration law requires the collection of fingerprints of all aliens entering the territory as well as for requiring/renewing permits of stay. Fingerprints of foreigners including those of asylum seekers are stored in the national AFIS, which is operated by the Scientific Police. Biometric systems based on fingerprints are used with regard to biometric passports in which fingerprints are stored locally on the chip.
4. The main difficulties regarding the application of data protection principles are:
   - The proportionality principle and the purpose specification principle. The Italian DPA recently found that the processing of biometric data to regulate access to a sports centre was disproportionate.
   - The criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent).

   The DPA issued several decisions regarding the use of biometrics in the workplace. The main principles of the DPA in the workplace context are as follows:
   - 1) The blanket, unrestricted use of biometric data is not permitted. On account of their nature, these data require specific precautions to be in place to prevent harming data subjects. Therefore, as a rule it is not permitted to process fingerprint data to control the number of hours worked by the employees.

- 2) Using biometric data may only be justified in specific cases by taking account of the relevant purposes and context in which data are to be processed. This is the case, for example, if access to "sensitive areas" is to be regulated through the use of biometrics.
- 3) Biometric verification and identification systems based on the reading of fingerprints stored as encrypted templates on media that are held exclusively by the relevant data subject should be preferred over centralised processing of biometric data.

5. Biometric databases set up by the police. Biometric systems in the workplace, in particular for the control of employees' access to workplace areas. Other cases concern the use of biometrics for access to banks, sports centres, and schools. Other databases containing biometric data are those related to Eurodac and VIS. Moreover, the Italian immigration law requires the collection of fingerprints of all aliens entering the territory as well as for requiring/renewing the permit to stay. Fingerprints of foreigners including those of asylum seekers are stored in the national AFIS, which is operated by the Scientific Police. Biometric systems based on fingerprints are used with regard to biometric passports in which fingerprints are stored locally on the chip.
6. No personal data breaches caused by biometric technologies.
7. Not answered.

Information of interest: (1) the processing of biometric data must be notified to the DPA. (2) Prior checking of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects. (3) The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.
The Italian DPA faces difficulties regarding the application of data protection principles, in particular the proportionality principle, the purpose specification principle, and the criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent).
The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects: (1) no unrestricted use, (2) justification grounds taking into account the relevant purposes, and (3) storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases.
In 2008, the Italian DPA laid down specific recommendations and measures with regard to the Ministry of Interior's 'Guidelines on the collection of fingerprints of members of the country's Roma community'.

7.11. Lithuania

Remark: the general framework is laid down in the Act on Legal Protection of Personal Data (adopted on 11 June 1996, last new version on 21 January 2003, came into force on 1 July 2003).[226]

1. There is no separate legal act that regulates biometric data processing. The processing of fingerprint data in a fingerprint register is regulated by the general data protection act.
2. Not answered.
3. Public and private bodies mostly use video surveillance systems. Also the Lithuanian DPA (SDPI; State Data Protection Inspectorate of the Republic of Lithuania) has encountered questions regarding the possibility to use fingerprint data in the private sector (e.g. gyms, schools, and university dormitory for entrance purposes), but after the consultation with the DPA such systems (except that of the university dormitory) were not deployed because the

[226] http://www.ceecprivacy.org/main.php?s=2&k=lithuania

DPA issued a prohibition order on the use of such systems. One firm issuing certificates for IT specialists have proved the necessity of using vein pattern in order to identify persons taking the exam for the certificate, because the certificate is widely acknowledged and for them it was important to prevent fraud. The DPA also encountered the plan of the Lithuanian State Social Insurance Fund Board to implement a voice recognition system as one of the alternatives for the identification of insured persons in order to provide personal data to him by phone. The Lithuanian DPA is still examining this plan.

4. Due to the fact that legislation does not state whether biometric data should be regarded as sensitive data, data controllers processing biometric data do not have legal certainty whether prior checking (provided in the Lithuanian data protection act) shall be carried out or not. Legal uncertainty is also caused by the lack of legislation on biometric data processing and the lack of clear requirements on such processing.
5. The Lithuanian police have only one fingerprint register. The Lithuanian DPA has no information on the existence or planning of other central biometric databases in the public or private sector.
6. The Lithuanian DPA is not aware of such situations.
7. The Lithuanian DPA is not aware of such research or reports.

Information of interest: The Lithuanian DPA has encountered questions regarding the possibility to use fingerprint data in the private sector (e.g. gyms, schools, and university dormitory for entrance purposes), but after consultation with the DPA, such systems (except university dormitory) have not been deployed because the DPA issued a prohibition order on the use of such systems. One firm issuing certificates for IT specialists, have proved the necessity to use vein pattern in order to identify persons taking the exam for the certificate, because the certificate is widely acknowledged and for them it was important to prevent fraud. Due to the fact that legislation does not state whether biometric data should be regarded as sensitive data, data controllers processing biometric data do not have legal certainty as to whether **prior checking** (provided in the Lithuanian data protection act) shall be carried out or not. Legal uncertainty is also caused by the lack of legislation on biometric data processing and the lack of clear requirements on such processing.

7.12. Former Yugoslav Republic of Macedonia[227]

Remark: the Act on the Protection of Personal Data adopted in 1994 created the original basis general data protection framework. In January 2002 this act was amended, incorporating 'partly' the principles of the legal processing of personal data, particularly special categories of personal data as established by Directive 95/46/EC. A new Act on Personal Data Protection was drafted in 2004, amended to include the EC recommendations eventually adopted on 25th January 2005.[228]

1. In the data protection act of the former Yugoslav Republic of Macedonia, biometric data is seen as a special category of personal data. Prior checking by the DPA, prior to the processing of biometric data is necessary to confirm the identity of the data subject.
2. Not answered.
3. From the received requests for obtaining the approval for processing biometric data, the national DPA concludes that the most frequent requests are for biometric systemsprocessing fingerprints.

227 As of February 2019, the official name of the country changed to North Macedonia.
228 See http://www.ceecprivacy.org/main.php?s=2&k=«Former Yugoslav Republic of Macedonia» and http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.MK

4. One of the problems encountered with regard to the processing of biometric data (in both the public and private sector) is the intention of controllers to use the biometric system to control employees – to prove the presence of the employees. This controllers' intention is due to the fact that a biometric system is one of the cheapest ways to control employees, cheaper than the system for performing video surveillance. Therefore, the DPA required the controller to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.
5. One of the central registers for biometric data in the former Yugoslav Republic of Macedonia is in the Ministry of interior and is used to provide data for issuing passports and personal ID cards.
6. The DPA is not aware of, or informed by, the Ministry of Interior on the hacking or compromising of biometric systems.
7. The DPA is not aware of research on biometrics.

Information of interest: the data protection act of the former Yugoslav Republic of Macedonia states biometric data as a special category of personal data. Prior checking by the DPA, prior to the processing of biometric data necessary to confirm the identity of the data subject. One of the problems encountered with regard to the processing of biometric data (in both the public and private sector) is the intention of controllers to use the biometric system to control employees, to prove the presence of the employees. The controllers' intention is due to the fact that a biometric system is one of the cheapest ways to control employees, cheaper than a system performing video surveillance. Therefore, the DPA required the controller to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.

7.13. Malta

Remark: Directive 95/46/EC has been implemented by the Data Protection Act 2001.[229]

1. Malta does not have regulation or legislation with regard to biometrics.
2. The latest biometric technologies available are voice, fingerprint, and hand palm recognition devices, iris scanners, and face geometry devices.
3. The devices currently being used are the fingerprint and hand palm recognition devices. In both private and public sectors these are used for time and attendance verification, payroll purposes, general administration and for access to specific designated areas. In the public sector these are also set for the issue of biometric passports.
4. No specific problems or difficulties have been encountered in both the private and public sectors with regard to biometrics. When they were first introduced trade unions voiced their concerns about the legality of the installation of such devices at places of work and to date they seek the advice of the Maltese DPA on queries on this matter.
5. One example of a central database in the public sector is 'NIDMS – National Identity Data Management System'. This records biometric data (fingerprints) for passports and the issuance of VISA purposes. The Maltese DPA is not aware of any central database in the private sector.
6. The Maltese DPA is not aware of any situations where biometric systems were hacked or compromised.

[229] Mamo TCV Advocates, 'Malta', in Linklaters, *Data Protected*, 2005, 76-78; A. Camilleri & Cl. Micallef-Grimaud, 'Malta', Chapter 33 in DLA Pipers, *Data Protection Laws of the World*, 2013, 188-195.

7. The Maltese DPA issued a paper entitled 'The Use of Biometrics Devices at the Workplace'.

Information of interest: -

7.14. Monaco

Remark: Data protection in Monaco is regulated by Data Protection Act n° 1.165 of 23 December 1993, modified by Law n° 1.353 of 4 December 2008 (the 1993 Act). The principality of Monaco is part of the Council of Europe and ratified Convention n° 108, but is not part of the EU and as a consequence did not transpose Data Protection Directive 95/46/EC.[230]

1. The processing of biometric data is regulated through the Monegasque DPA.
   Prior checking: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorisation from the Monegasque DPA (CCIN; Commission de Contrôle des Informations Nominatives).
   Penalisation: "*persons who, knowingly, collect or cause to be collected, record or cause to be recorded, store or cause to be stored, use or cause to be used personal data relating to suspected unlawful activities, offences, security measures or including biometric data that is required to check persons' identities or is intended for the purposes of surveillance without having obtained the authorization laid down in article 11-1*", "[…] *shall be punished by imprisonment for three months to one year and by a fine as described in item 4 of article 26 of the Criminal Code or only one of those two penalties".*
2. Private sector: biometric systems which can recognise the contour of the hand, the venous network of the fingers of the hand, and fingerprints.
3. Private sector: biometric systems are being used for access control and time attendance of employees. The Commission excluded the use of systems based on fingerprint recognition for the purpose of time management, time attendance of employees, and for access control at entrances and exits of companies or organisations, because they present a greater risk to individuals than systems based on recognition of the contour of the hand or finger vein patters of the hand. Biometric devices that have been analysed since 2011 by the supervisory authority raised no particular difficulty. The controllers of these systems have met the principles set out in the supervisory authority's recommendations.
   Public sector: biometric data are used in the police database AFIS. Data from DNA samples from crime scenes or suspects or defendants are included in the court records, but not contained in the database. Biometric data are used for identity cards, including two fingerprints and a digital photograph. These data are stored in the computer system used for the issuance of identity cards and cannot be interconnected with any other file. It has never been compromised.
4. Private sector: problems have been encountered regarding two biometric devices. By Resolution no. 2010-19 of 26 May 2010, published on the website of the CCIN, the Commission issued an opinion unfavourable to the implementation of systems based on fingerprint recognition with the purpose of securing access control. The system was deployed in a cloakroom. The Commission noted that the deployment was disproportionate and the system lacked security measures. During an investigation conducted on 14 March 2011, the Commission staff noted the existence of an unsecured central database for

[230] G. Pace, 'Monaco', Chapter 36 in DLA Pipers, *Data Protection Laws of the World*, 2013, 211-215

fingerprints for which no approval had been granted. The use of both biometric systems had been stopped at the request of the Commission.

5. Not answered.
6. Not answered.
7. Not answered.

Information of interest: the Monegasque DPA prohibits the use of biometric systems based on fingerprints in the workplace. The DPA supervises security requirements applicable to biometric systems and the prohibition of the further use of biometric data. Prior checking: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorisation from the Monegasque DPA. Penalty: "*persons who, knowingly, collect or cause to be collected, record or cause to be recorded, store or cause to be stored, use or cause to be used personal data relating to suspected unlawful activities, offences, security measures or including biometric data that is required to check persons' identities or is intended for the purposes of surveillance without having obtained the authorization laid down in article 11-1",* "[…] *shall be punished by imprisonment for three months to one year and by a fine as described in item 4 of article 26 of the Criminal Code or only one of those two penalties*".

7.15. Montenegro

Remark: The general framework is based on the Personal Data Protection Act No. 79/08 of 23 December 2008 and 70/09 of 21 October 2009).[231]

1. The processing of biometric data is regulated through the Montenegran DPA. Biometric data is defined as "[…] *data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly*". Prior checking: prior to the processing of biometric data, the approval of the Montenegran DPA is required, because the processing represents a particular risk for the rights and freedoms of individuals. The processing of biometric data is only allowed if it is provided for by law and in accordance with the law. Biometrics are only allowed if it is "[…] *necessary for the protection of individuals and property or for the protection of secrecy of data or business secrets* […]" when there are no other authentication methods, if is obligated by international treaties, or to establish the identity of individuals crossing state borders.
   The Montenegran Code of Criminal Procedure contains provisions regarding the 'examination, autopsy and exhumation of a corpse' and the 'physical examination and other procedures' in which the use of DNA is regulated.
2. No information provided.
3. No information provided.
4. No information provided.
5. Montenegro does not have a central database for biometric data. However, it has a database containing the fingerprints of two fingers which are collected in the context of legislation on identity cards. Additionally, the police has a database for biometric data (the answer of Montenegro does not elaborate on this issue). Montenegro does not yet have a DNA register, although required by law.
6. No problems regarding hacked or compromised biometric systems.
7. No information provided.

[231] http://www.ceecprivacy.org/main.php?s=2&k=montenegro. The act can be found on http://www.afapdp.org/wp-content/uploads/2012/01/Monténégro-Personal-Data-Protection-Law-79-08-and-70-09.pdf

Information of interest: Biometric data is defined as '[…] *data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly*". Prior checking: prior to the processing of biometric data, the approval of the Montenegran DPA is required, because the processing represents a particular risk for the rights and freedoms of individuals.

7.16. The Netherlands

Remark: The general framework is formed by the Act on the Protection of Personal Data of 6 July 2000 ('Wet bescherming persoonsgegevens') and the Exemption Decree of 7 May 2001 (vrijstellingsbesluit Wbp).[232] Sector specific regulations are contained in other acts.

1. Criminal law: yes, specific provisions regulate the collection of facial images and fingerprints.
   Travel documents: yes, the Dutch Passport Act regulates the storage of facial images and fingerprints in the passport. The Passport Act also regulates the storage of two fingerprints in a decentralised storage register, operated by the individual municipalities. The 2009 amendment of the Dutch Passport Act[233] contains a provision on the travel document administration which is intended to include the central storage of fingerprints.[234] This provision on the travel document administration has, in contrast to the provision on the storage of biometrics in passports, not yet entered into force.
   A recently proposed amendment of the Dutch Passport Act[235] aims at (1) ceasing the storage of fingerprints, (2) ceasing the storage of fingerprints in Dutch identity cards, and at (3) collecting two instead of four fingerprints when someone applies for a passport.
2. Criminal law: facial images and fingerprints are primarily being used for identification purposes during criminal proceedings.
   Travel documents: for the application and issuance of Dutch travel documents devices to collect fingerprints and devices to digitalise a facial image and signature are being used.
3. Criminal law: facial images and fingerprints to (1) identify suspects and convicts, and for (2) criminal investigation purposes.
   Travel documents: for the application and issuance of Dutch travel documents biometric devices to collect and verify fingerprints, and specific technology to digitalise facial images are being used.
4. Criminal law: problems regarding the (1) technology (e.g. stability and performance), the (2) operation of the fingerprint device, and the (3) quality of the fingerprints (e.g. technical problems and organisational problems).
   Travel documents: with regard to facial images in Dutch travel documents no major problems have been encountered. There is, however, social resistance regarding the storage of fingerprints, as there are doubts about the need to store fingerprints, and about the efficacy of using fingerprints.
5. Criminal law: yes, a national fingerprint database (called HAVANK) for criminal investigation purposes (the identification of suspects, convicts, and witnesses) operated by the Dutch police. The facial images collected for the same purposes are processed in the

[232] R. Van Schalk & J. Kabel, 'Netherlands', Chapter 38 in DLA Pipers, *Data Protection Laws of the World*, 2013, 221-226; De Brauw Blackstone Westbroek, 'the Netherlands', in Linklaters, *Data Protected*, 2005, 79-81.
[233] *Staatsblad* 2009, 252. The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published.
[234] The intention to include, *inter alia*, fingerprints in a central database is noted in the Explanatory Memorandum, see *Kamerstukken II* 2007/08, 31 324, No. 3, 34. The *Kamerstukken* are Parliamentary Documents. 'II' refers to the Second Chamber. The document referred to can be found at https://zoek.officielebekendmakingen.nl/, by searching the series number, in this case 31324. The article referred to in the Explanatory Memorandum and containing the provision on the travel document administration ('*reisdocumentenadministratie*') is Article 4a of the amended Dutch Passport Act [Staatsblad 2009, 252].
[235] *Kamerstukken II* 2012/13, 33 440, No. 2.

database operated by the Dutch criminal courts. Facial images and fingerprints being used in Dutch prisons and institutions for people, who committed a crime and suffer from a mental disorder, are processed in a biometric database.
Travel documents: no.

6. Criminal law: no, but there have been situations in which users tried to spoof a biometric system.
   Travel documents: no.
7. Criminal law: several Dutch universities, including Tilburg University, have conducted research on biometrics.
   Travel documents: attached a 2012 report on the decision making process of the Dutch government with regard to biometrics in Dutch travel documents.

   The Dutch independent foundation Privacy First recently presented its 2012 annual report.[236] Privacy First's aim is to preserve and promote the right to privacy and a free society with a central focus on biometrics. Its 2012 annual report shows the issues Privacy First is concerned about, such as privacy issues about biometrics regarding the Dutch Passport Act and the access to centralised and decentralised fingerprint databases by Dutch and foreign secret services.

Information of interest: The 2009 amendment of the Dutch Passport Act[237] contains a provision on the travel document administration, which is intended to include the central storage of fingerprints.[238] This provision on travel document administration has, in contrast to the provision on the storage of biometrics in passports, not yet entered into force.
With regard to facial images in Dutch travel documents, no major problems have been encountered. There is, however, social resistance regarding the storage of fingerprints, as there are doubts about the need to store fingerprints, and about the efficacy of using fingerprints. A recently proposed amendment of the Dutch Passport Act[239] aims at (1) ceasing from the storage of fingerprints, (2) ceasing from the storage of fingerprints in Dutch identity cards, and at (3) collecting two instead of four fingerprints when someone applies for a passport. Problems with biometric systems used in the context of criminal law enforcement have been encountered regarding the (1) technology (e.g. stability and performance), the (2) operation of the fingerprint device, and the (3) quality of the fingerprints (e.g. technical problems and organisational problems).

7.17. Niger

1. Niger does not have any legislation on biometric data, although by 2015 Niger hopes to have introduced biometric passports and hopes to have a biometric electoral roll.
2. Not answered.
3. Not answered.
4. Not answered.
5. Not answered.
6. Not answered.
7. Not answered.

[236] The 2012 Annual Report (in Dutch), Privacy First Foundation, Amsterdam, 29 March 2013, http://www.privacyfirst.nl/images/stories/PDFs/jaarverslag_privacyfirst_2012.pdf.
[237] *Staatsblad* 2009, 252. The *Staatsblad* is the official journal in which all Dutch laws and most decrees are published.
[238] The intention to include, *inter alia*, fingerprints in a central database is noted in the Explanatory Memorandum, see *Kamerstukken II* 2007/08, 31 324, No. 3, 34. The *Kamerstukken* are Parliamentary Documents. 'II' refers to the Second Chamber. The document referred to can be found at https://zoek.officielebekendmakingen.nl/, by searching the series number, in this case 31324. The article referred to in the Explanatory Memorandum and containing the provision on the travel document administration ('*reisdocumentenadministratie*') is Article 4a of the amended Dutch Passport Act [Staatsblad 2009, 252].
[239] *Kamerstukken II* 2012/13, 33 440, No. 2.

Information of interest: -

7.18. Poland

Remark: Directive 95/46/EC has been implemented by the 1997 Act on Personal Data Protection ('Data Protection Act'). It sets the general framework for the protection of personal data in Poland.[240] In what follows, we reproduce the responses to the questionnaire.

1. No general regulation/legislation with regard to biometrics. Biometric databases are set up on the basis of specific provisions, which specify the tasks and powers of particular authorities (e.g. border guards and military police). Access to biometric data collected by such entities is possible only for authorised, strictly specified authorities, in connection with the conducted proceedings. Poland has two acts in which biometrics are regulated: the Act on Passport Documents and the Act on the Police, which contains provisions on a fingerprint database (CRD; Central Dactyloscopic Registry) and on a DNA database.
2. In Poland, the latest biometric technologies solutions are being implemented. Bank PBS (Bank Polskiej Spółdzielczości) has already exchanged over 90 per cent of its cash machines for devices in which finger vein scan is a transaction confirmation. Wincor-Nixdorf biometric cash machines using Hitachi Finger Vein technology have been used. The Institute of Mathematical Machines issued an official opinion on innovation in relation to the Finger Vein solution destined for cash machines and bank affiliates. The opinion concerns a solution based among others on Finger Vein (HOTS 609) bank readers and FVS software. Thanks to this opinion a bank in Poland which purchases Finger Vein solution will be able to apply for a tax refund to the sum of 50 per cent of the cost of purchased solution. Finger Vein is the only biometric technology to have warranted such an opinion.
3. In Poland the following biometric identification systems are applied:
   - Automated Fingerprint Identification System (AFIS) - kept by the Police;
   - Cash machine authorisation systems, where biometric data are used to scan finger vein as authentication system in cash machines. This technology is used e.g. by the bank "Bank Polskiej Spoldzielczosci S.A."
   - CRD (Central Dactyloscopic Registry) – information in the form of fingerprints collected and obtained by the Police is processed in this central data filing system;
   - Central Register of Issued and Annulled Passports – in this data filing system among others the following data are processed: face images (photographs) and fingerprints;
   - Passport System of the Ministry of Foreign Affairs – in this data filing system among others the following data are processed: face image and fingerprints;
   - Eurodac module within the IT system "Residence" – in this module fingerprints are processed, in connection with the need to identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the European Union;
   - DNA Database, kept by the Police – in this data filing system among others the following data are processed: data revealing directly, or in context, the genetic code;

   Please, note that automated exchange of DNA data from fingerprint databases and DNA databases also takes place through the agency of INTERPOL as well as within the framework specified by the Prüm Decision (Council Decision 2008/615/JHA of 23 June

[240] See on Poland CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 21-27

2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime).

- Moreover, biometric data are used (contrary to the Polish law) in the working time monitoring systems employed by some entities (see point 4 as regards this problematic issue); or in buildings', or rooms', access control systems;

4. One of the problems related to implementation of biometric technologies is a closed catalogue containing employee data that can be processed by an employer in connection with employment. The catalogue does not include biometric data and therefore there is no legal basis for using biometric technologies in working time monitoring systems. In a few cases solutions applied for this purpose were reported by employees as illegal, and court decisions were issued ordering the removal of these solutions.

   Another problem connected with implementation of biometric technologies is the lack of official definition of biometric data and distinguishing biometric data processed in the form of electronic records, which are used in IT solutions, from traditional ones, such as personal signature, face image photograph or voice.
5. Yes, a Central Dactyloscopic Registry (CRD), containing fingerprints collected by the police, and an Automated Fingerprint Identification System (AFIS), operated by the police.
6. No situations of hacking or compromising are known. However, there were cases of unauthorised use of biometric data in the work place setting to monitor working time.
7. In Poland, research regarding biometrics is conducted by the Warsaw University of Technology (Biometrics and Machine Learning Group at the Faculty of Electronics and Information Technologies) and Research and Academic Computer Network (NASK Biometrics Laboratory). The activity of the Biometric Laboratory of NASK is centered on the security of biometric applications, original biometrics technologies, biometrics applications in identity recognition, remote biometrics authentication, and biometric-related smart cards.

   The original solutions include access control systems based on iris recognition algorithms, as well as payment transaction verification systems based on handwritten signature analysis. Biometrics security research is centred on testing the aliveness detection level of biometric equipment, development of presentation attacks detection methods, as well as in combining cryptography and biometrics to protect biometric templates. NASK's original combination of biometrics, smart card technology and remote authorisation methodology allows the creation of secure remote authorisation mechanisms. The expertise extends also to equipment selection procedures depending on the required level of security and reliability, as well as on the given target environment.

   The lab holds a US patent related to iris aliveness detection. It also developed the world's only multimodal database containing measurements of numerous biometric characteristics (iris, fingerprint, face, palm geometry and handwritten signature) collected over a long period of time (over 7 years) from several hundred individuals. The NASK Biometrics Laboratory actively participates in biometric standardisation, being a member of Polish Committee on Standardisation and ISO/IEC SC37.

   The research conducted at the Warsaw University of Technology and NASK are managed by Prof. Andrzej Pacut. There are other research centres in Poland involved in the research, including:

   - Lodz University of Technology - Prof. Krzysztof Ślot (with a team),
   - AGH University of Science and Technology - Prof. Khalid Saeed (with a team),
   - Silesian University of Technology - Prof. Andrzej W. Mitas (with a team),
   - Institute of Mathematical Machines - Mr Krzysztof Dzik (with a team)

Information of interest: the Polish bank PBS has exchanged over 90 per cent of its cash machines for devices in which a finger vein scan is a transaction confirmation. Poland has encountered problems with regard to the deployment of biometric systems in work place settings, while there is no legal basis for using these systems to monitor working time. Other problems encountered are the lack of an official definition of biometric data and the difficulty in distinguishing biometric data from other personal data. In Poland, research is conducted on: access control through iris recognition, payment transaction verification systems based on handwritten signature analysis, aliveness detection, combining cryptography and biometrics to protect biometric templates, smart card technology, and remote authorisation methodology. The NASK Biometrics Laboratory holds a US patent on iris aliveness detection, and actively participates in biometric standardisation, being a member of the Polish Committee on Standardisation and ISO/IEC SC 37.

7.19. Portugal

Portugal has been omitted from this report because it did not want its reply to be published.

7.20. Romania

Remark: Act no. 677 regarding the protection of individuals with regard to processing their personal data and the free movement of such data of 2001 ('Data Protection Act') is based on Directive 95/46/EC and sets the general framework for data protection in Romania.[241] In what follows, we reproduce the responses to the questionnaire

1. Biometrics are regulated in legal instruments on travel documents. Romanian passports contain the facial image and two fingerprints of the data subject.
2. Not answered.
3. Not answered.
4. Not answered.
5. In the public sector, a central biometric database is used for the issuance of travel documents.
6. No information on compromised biometric systems was registered.
7. No research on biometrics has been conducted.

Information of interest: There is not much to be found in the report received by the authors. In a commercial guide to data protection laws in Central and Eastern Europe we also find that Romania has created a specific notification obligation to the Romanian DPA, if the personal data to be processed fall under the category of 'special data', as listed under article 8.1 of Directive 95/46/EC, or is related to an individual's genetic, biometric or geographical location.[242]

7.21. Senegal

1. No legislation specifically relating to biometrics. However, legislation regarding ID cards regulates the use of biometrics (i.e. fingerprints and facial images). These biometrics are used to identify citizens, and in electoral matters, to prevent multiple entries on the electoral

[241] See CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 28-33
[242] CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, (56p.), 32.

roll. The Senegalese data protection act regulates the processing of personal data in general, and the processing of biometric data in particular, which is under the control of the Senegalese DPA.
2. Biometric recognition systems for fingerprints, facial images, iris scans, and hands/fingers.
3. Biometrics in the public sector are only be used for the purposes of the identity card and the biometric passport.
4. Not answered.
5. The Senegalese Ministry of the Interior holds a database of digital passports. In addition, a foreign company (Securiport LLC) has set up a database of passengers in Senegalese airports.
6. Not answered.
7. Not answered.

Information of interest: fingerprints and facial images are used in electoral matters, to prevent multiple entries on the electoral roll.

7.22. Serbia

Remark: Law on personal data protection **(**The Official Gazette of the Republic of Serbia, number 97/08).[243]

1. No specific regulation regarding biometrics. The processing of biometric data is addressed in legislation on identity documents, state border protection legislation, police law, and criminal procedure law.
2. Facial images (FIIS; Face Image Identification System), fingerprints (AFIS; Automated Fingerprint Identification System), signature biometrics, voice identification and DNA.
3. Public sector: the Ministry of Interior operates an AFIS system, FIIS system, and DNA database. At border crossings and checkpoints Serbia employs devices able to read biometric identification documents.
   Private sector: biometric systems are used in the workplace to monitor the number of hours worked by the employees. However, due to the violation of data protection legislation the further processing of biometric data was prohibited.
4. Due to the lack of regulation concerning biometrics, many controllers in the private sector deploy fingerprint identification systems to monitor the number of hours worked by the employees. However, the Serbian DPA observed that this type of processing is disproportionate to its purpose and issued warnings to several data controllers.
5. Yes. Biometric records are located in two separate databases.[244]
6. No information.
7. No information.

Information of interest: in addition to biometric data such as facial images, prints of all fingers, palm prints and other biometric characteristics of perpetrators – such as tattoos and scars – are being collected.

[243] See http://www.ceecprivacy.org/main.php?s=2&k=serbia. English version of the act: http://www.poverenik.org.rs/images/stories/dokumentacija-nova/zakon-o-zastiti-podataka-o-licnosti_en.pdf
[244] The answer does not clarify what kind of databases is meant.

7.23. Slovenia

Remark: basis of the framework is the Personal Data Protection Act (ZVOP-1), which was adopted by the National Assembly of the Republic of Slovenia at its session of 15 July 2004.[245]

1. Yes. The use of biometrics in both the public and private sector is regulated in the Slovenian data protection act, and with regard to biometric passports in specific legislation on passports.
2. The vast majority of biometrics used in Slovenia processes fingerprints, probably exceeding 95 % market share. Given that the Slovenian data protection act requires **prior checking** before biometric measures are introduced, there were only a few examples where other methods were used, i.e. face recognition and palm recognition. All in all, the Information Commissioner has issued roughly 80 decisions about biometric measures since 2005, around three out of four were positive. Cases where applicants were not given permission were mostly because the applicants could not meet the legal preconditions and wanted to use biometric measures only for ease of use or economic benefits. In terms of passports, the Republic of Slovenia introduced second generation biometric passports in June 2009 (first generation passports that used biometric images were introduced in 2006). Second generation passports require both biometric images and fingerprints.
3. Most implementations use centralized storage of biometric templates, very few were encountered where templates are stored on portable media in the possession (only) of the individual. In the case of biometric passports, it has to be noted that there is no centralised database – biometric data are stored **only in the passport**.
   In terms of purposes biometrics are mostly used for access control, e.g. to protect access to server rooms, vaults, premises with confidential information and valuable equipment or resources. There are, however, significant tendencies to use biometric measures for the purposes of timing attendance in both the private and public sectors due to the fact that biometric equipment has become easily available and affordable. Such use, however, does not meet the legal preconditions. The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures **may only be introduced 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*.** Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.
   In terms of biometric passports, biometric measures may be provided for by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.
4. In administrative procedures of applying for a decision to allow biometric measures several applicants underestimate the strictness of legal conditions. Many want to introduce biometric measures just for ease of use or economic reasons. Many applicants have in the past also been misled by biometric resellers about the effectiveness and downsides of use of biometric measures, where only the perceived benefits were presented. Resellers obviously tend to see the existing regulations as too strict. The opinion of the Information Commissioner is contrary to this and supports the legislator's decision to limit the use of biometric measures to situations where this is absolutely necessary and where milder measures are not possible.

[245] https://clientsites.linklaters.com/Clients/dataprotected/Pages/Slovenia.aspx. See for an English version: http://ec.europa.eu/justice/policies/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf

There have been very few implementations where privacy-enhancing technologies were used, e.g. use of template-on-card solutions etc.

5. There is no such database. Regarding biometric passports there is no centralised database; biometric data are stored only in the passport. In terms of DNA there were some proposals by some political parties in 2006 to introduce a nation-wide DNA database, but these plans were not taken on board.
6. We have not been informed of such cases. On the other hand, in some cases there were reports of:
   problems with enlisting all employees (e.g. workers with damaged fingerprints)
   problems with malfunctioning equipment (false acceptance/false rejections)
   complaints and resistance by employees to be subjected to such measures.
7. Unfortunately, we are not aware of such research on a national level.

Information of interest:

The questionnaire does not contain detailed responses on this point, but further analysis reveals some of the interesting features of the data protection act (ZVOP). Article 6.21 defines biometric characteristics as such physical, physiological and behavioral 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. Biometrical data are included under Article 6.19 on sensitive data under specific circumstances: "*Sensitive personal data - are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, the entry in or removal from criminal record or records of minor offences that are kept on the basis of a statute that regulates minor offences (hereinafter: minor offence records); biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances*".

The Slovenian data protection act also imposes a range of additional restrictions that apply to video surveillance, biometric information, access control information and connecting systems. The Slovenian data protection act requires **prior checking** before biometric measures are introduced. The Information Commissioner has issued about 80 decisions about biometric measures since 2005, around three out of four were positive. Cases where applicants were not given permission to use biometrics were mostly because the **applicants could not meet the legal preconditions and wanted to use biometrics measures only ease or economic reasons, not for improving their security mechanisms**. Many applicants have also been misled in the past by biometric resellers about the effectiveness and downsides of the use of biometric measures, where only the perceived benefits were presented to them. Resellers tend to see the existing regulations as too strict. The opinion of the Slovenian DPA is contrary to this and it supports the legislator's decision to **limit the use of biometric measures** to situations where this is absolutely necessary and where milder measures are not possible.

With regard to biometric passports, the **biometric data to be used are stored only in the passport; there is no central biometric database**. Biometrics are mostly used for **access control** (e.g. to protect access to server rooms, vaults, premises with confidential information and valuable equipment or resources), but there is a tendency to use biometric measures also for the purposes of **timing attendance** in both the private and public sectors, due to the fact that biometric equipment has become easily available and affordable. Such use, however, does not meet the legal preconditions.

The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures may only be introduced 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*. Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.**

7.24. Switzerland

Remark: The processing of personal data is mainly governed by the Federal Act on Data Protection of 19 June 1992 (the 1992 Act) and its ordinances, i.e. the Ordinance to the Federal Act on Data Protection ("DPO") and the Ordinance on Data Protection Certification ("ODPC"). Additional regulation can be found in other laws, mainly with regard to the public sector and regulated markets.[246]

1. Private sector: no specific regulation regarding biometrics. Biometric data must be processed in accordance with the 1992 Act.
   Public sector: yes, several legislative instruments.[247]
2. The 1992 Act does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the current state of technology.
3. The 1992 Act does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the current state of technology.
4. Today, biometric systems are available at low costs. Therefore, in the private sector the technology is often used without the need for a strong identification or any other serious reason. Subsequently, the Swiss DPA is often confronted with questions concerning the proportionality of the use of such systems; especially if a central database is part of the system. Furthermore, it is our observation that serious tensions between employer and employee can arise as soon as the employer collects the biometric data of his employees, even against their will.
5. Private sector: the 1992 Act does not contain a provision for a formal authorisation of biometric systems. Therefore, the Swiss DPA has no information on the use of central databases.
   Public sector: yes, two biometric databases. One database is set up in accordance with regulation on 'police identification'.[248] Another database 'serves as a basis for the biometric passport'.[249]
6. Unknown.
7. Unknown.

Information of interest: in the private sector biometric technology is often used without the need of identification or any other serious reason. The Swiss DPA is often confronted with questions about the proportionality of the use of biometric systems, especially if a central database is part of the system. The Swiss DPA notices the possibility of serious tensions between employer and employees if the employer collects the biometric data of his employees, even against their will. Switzerland has two central biometric databases in the public sector.

[246] Chr. Beusch-Liggenstorfer & N. Schwibs, 'Switzerland', Chapter 54 in DLA Pipers, *Data Protection Laws of the World*, 2013, 318-323
[247] The Swiss response does not elaborate on the content of their reported legislative instruments.
[248] It is not clear what exactly is meant by 'police identification'.
[249] Although it is not clear what exactly is meant by 'serves as a basis for the biometric passport', Switzerland seems to have a central biometric database in which biometric data needed for the biometric passport is stored.

7.25. Main results from the questionnaire

The authors of this report have drafted 7 significant questions about the current legislation and regulation on biometrics and regarding the current state of biometric technology, (central) biometric databases, and problems arising from the deployment of biometric systems. The questionnaire was sent to 47 countries of which 22 responded. The responses differ considerably in the amount of information provided and the way in which the countries have made progress in legislation and regulation specifically aimed at the protection of biometric data. This section discusses the most interesting information in the country responses.

7.26. Countries that have adopted legislation and regulation specifically aimed at the protection of biometric data

Only a few countries have adopted legislation specifically aimed at the protection of biometric data. These countries are:

- **Estonia:** biometric data is considered **sensitive personal data** in the Estonian data protection act. (An interesting opinion comes from the Estonian DPA: the advisor of the Estonian Data Protection Inspectorate recommends the use of systems that don't store biometric images but a biometric template of that image). A similar situation exists in **the Czech and Slovak Republic** (although no response to the questionnaire was sent).[250] Under the **Slovenian** data protection act sensitive personal data includes not only the standard types of sensitive personal data, but also biometric information if it can be used to identify sensitive personal data about a data subject. This understanding of biometrics is also echoed in a **Belgian** DPA opinion from 2008.[251]

- **France:** France is pioneering the field of data protection in general and biometric data in particular. The processing of biometric data is regulated in the French 1978 data protection act which contains a provision on **prior checking**: biometric processing needs to be authorised by the French DPA (CNIL). In the public sector a double check has to be carried out: the implementation of biometrics is subject to a decree of the Council of State, adopted on the basis of the DPA's opinion.
  France has adopted in 2004 a strict doctrine on the use of biometrics: seeking a balance (proportionality) between the purpose of processing and the risks in terms of privacy and data protection. Biometric devices are categorised upon their risks for privacy and data protection:
  - "with a trace": fingerprints and palm prints. The use of these devices is considered to involve significant risks in terms of privacy. CNIL has been particularly cautious about the use of fingerprints;.
  - "without a trace": hand geometry, finger vein patterns;
  - "intermediate": voice and face recognition, iris scans.

  The CNIL considers the use of "with a trace" biometric devices to be legitimate if the biometric data are stored on a storage medium under the exclusive control of the data subject, as opposed to storage in a centralized database. In the private sector, the deployment of a centralised database should be linked to a "strong security imperative" that the CNIL will assess.

[250] We rely on Eva Ruhswurmová, 'Czech Republic', in DLA Pipers, *Data Protection Laws of the World*, 2013, 69-74; CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, 9 and on the Slovak Republic M. Stessl, 'Slovak Republic', in Chapter 49 in DLA Pipers, *Data Protection Laws of the World*, 2013, 284-290.

[251] Avis d'initiative relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017), via http://www.privacycommission.be/sites/privacycommission/files/documents/avis172008_1.pdf

The doctrine evolves continuously due to new biometric developments and European legal developments such as Regulation 2252/2004 (EC) on biometrics passports.

- **Georgia:** Georgia is particularly pioneering the field of biometric data protection.
  The Georgian data protection act explicitly states in article 2(b) biometric data as a **special category of data**.
  Article 2(c) defines biometric data as any physical, mental or behavioural feature (fingerprints, iris scans, retinal images, facial features, and DNA), which is unique and permanent for each natural person and which can be used to identify this person.
  Article 9 paragraph 1, on the processing of biometric data by a public institution, reads as follows: "*The processing of biometric data by a public institution shall be allowed only for the purposes of the security of person and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts*."
  Article 10, on the processing of biometric data by a private person, includes a notification obligation for the biometric system's processor. Article 10 reads as follows: "*The processing of biometric data by a private person shall be allowed only if it is necessary for the purposes of conducting activities, for the security of persons and protection of property, as well as for avoiding the disclosure of secret information, if it is impossible to achieve these objectives by other means or it involves disproportionately huge efforts. Before using biometric data, a data processor shall notify a personal data protection inspector detailed information on the processing of biometric data, including the information notified to a data subject, the purpose of the processing of data and the safeguards of the protection of data, unless otherwise provided by the law."*

- **Italy:** several strict provisions are contained in the Italian data protection act:
  - The processing of biometric data must be notified to the DPA
  - **Prior checking** of the DPA in case of biometric databases set up by the police, as these are explicitly considered to carry higher risks of harming data subjects.
  - The use of biometrics is mentioned among the authentication credentials applying to any person in charge of processing data by electronic means.

  (An interesting opinion is given by the Italian DPA: the Italian DPA faces difficulties regarding the application of data protection principles, in particular the proportionality principle, the purpose specification principle, and the criteria for making the processing of biometric data legitimate (e.g. based on the data subject's consent). The Italian DPA is of the opinion that biometric data require **specific precautions to prevent harming data subjects**: (1) no unrestricted use, (2) justification grounds taking into account the relevant purposes, and (3) storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases.)

- **Former Yugoslav Republic of Macedonia:** biometric data is considered a **special category of personal data** in the data protection act of the former Yugislav Republic of Macedonia. **Prior checking** by the DPA, prior to the processing of biometric data necessary to confirm the identity of the data subject. The DPA required the controller of biometric systems to submit special analyses as well as written procedures in addition to the request for approval for the processing of biometric data, in order to decide whether the processing of biometric data is justified and necessary.

- **Monaco: prior checking**: the automated processing of biometric data required to check persons' identities, carried out by controllers other than judicial and administrative authorities, is only allowed with prior authorization from the Monegasque DPA.

- **Montenegro:** in Montenegran legislation, biometric data is defined as '[…] *data on physical or physiological features intrinsic to every natural person, which are specific, unique and unchangeable and capable of revealing the identity of an individual either directly or indirectly*". **Prior checking**: prior to the processing of biometric data, the approval of the Montenegran DPA is required, because the processing represents a **particular risk for the rights and freedoms of individuals**.

- **Slovenia:** the use of biometrics in both the public and private sector is regulated in the Slovenian data protection act. The Slovenian data protection act requires **prior checking** before biometric measures are introduced. The main reason that the Slovenian DPA did not give permission to use biometrics is that applicants for such systems **could not meet the legal preconditions** and wanted to use biometrics measures only for their **ease of use or economic reasons**, and not for improving their **security mechanisms**. The opinion of the Slovenian DPA is to **limit the use of biometric measures** to situations where they are absolutely necessary and where milder measures are not possible.
  The provisions for the introduction of biometric measures contain rather strict conditions and biometric measures may only be introduced 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***. Unless one of these conditions is fulfilled the Information Commissioner will not allow the introduction of biometric measures and will issue a negative administrative decision.

8 out of 22 member states which responded to our questionnaire have adopted legislation specifically aimed at the protection of biometric data. These countries are: **Estonia**, **France**, **Georgia**, **Italy**, **the former Yugoslav Republic of Macedonia**, **Monaco**, **Montenegro**, and **Slovenia**. The provision included most often in data protection legislation of these member states concerns prior checking. **Prior checking** is contained in data protection legislation of the following Member States: **France**, **Italy**, **the former Yugoslav Republic of Macedonia**, **Monaco**, **Montenegro**, and **Slovenia**.[252] The member states addressing biometric data as a **special category of personal data** are: **Georgia** and , **the former Yugoslav Republic of Macedonia**. In **Estonia** and other countries such as **Russia,** the **Czech** and **Slovak Republics** (although no response to the questionnaire were received) biometric data is considered **sensitive personal data.**[253] In Russia, consent needs therefore to be obtained in writing and a special regulation identifies specific security measures for carriers of biometrical information and biometrical information. Member states which adopted a **definition of biometric data** are: **Georgia** and **Montenegro**.
A quick scan of the available guides on data protection law around the world,[254] teaches us that the categorisation of biometrics as 'sensitive data' also occurs in countries such as India and Australia (the new act).

[252] See on prior checking in Luxembourg (unreported): A. Schmitt, G. Arendt & A. Grosjean, 'Luxembourg' in Chapter 31 in DLA Pipers, *Data Protection Laws of the World*, 2013, 173-183
[253] See on Romania (unreported): M. Dinu, C. Simion & L. Leanca, 'Romania', in Chapter 46 in DLA Pipers, *Data Protection Laws of the World*, 2013, 267-273, See on Russia (unreported): M. Malloy, P. Arievich, E. Golodinkina & M. Biryukova, 'Russia' in Chapter 47 in DLA Pipers, *Data Protection Laws of the World*, 2013, 274-279; on the Czech Republic (unreported): Eva Ruhswurmová, 'Czech Republic', in DLA Pipers, *Data Protection Laws of the World*, 2013, 69-74 and CMS Cameron McKenna, *CEE Guide to data protection*, London, 2013, 9 and on the Slovak Republic (unreported): M. Stessl, 'Slovak Republic', in Chapter 49 in DLA Pipers, *Data Protection Laws of the World*, 2013, 284-290.
[254] DLA Pipers, *Data Protection Laws of the World*, 2013, 366p.

7.27. Biometrics in the contexts of sports, school and workplace

The country responses show that the main difficulties of using biometrics are being encountered in the contexts of sports, school and workplace. The countries referring to these contexts are addressed hereinafter.

Sports

In **Italy** biometrics, including a biometric database, are being used for access to sports centres. The Italian DPA encounters difficulties regarding the proportionality principle and the purpose limitation principle. It recently found that the processing of biometric data to regulate access to a sports centre was disproportionate.

School

In **Hungary** camera surveillance and biometric entry control systems[255] are being used in schools. The DPA of **Ireland** published on its website guidance notes regarding 'Biometrics in Schools, Colleges and other Educational Institutions'. In **Italy** biometrics, including a biometric database, are being used for access to schools.[256] The DPA of **Lithuania** encountered questions regarding the possibility to deploy biometric systems using fingerprints in schools. The Lithuanian DPA issued a prohibition order on the use of such systems. Although **Belgium** did not report back, we note that biometric systems are also used in some Belgian schools. *De Liga voor Mensenrechten/Ligue des droits de l'homme* (League for Human Rights) nominated the practice of collection of biometric identifiers at schools for its yearly 'Big Brother Awards'. At a school in Gent, each student needed to register on the basis of his or her fingerprint, both upon arrival and when leaving the school. It is presumed that biometric identifiers have been used in schools in other Belgian cities such as Brussels, Liège and Mechelen. In the opinion of the *Liga voor Mensenrechten/Ligue des droits de l'homme,* fingerprint registration is stigmatising in itself, since it is based on the assumption that children lie. The same motive is also put forward to justify the use of biometrics during counter-terrorism operations. While a certain amount of suspicion in the fight against terrorism is warranted, in the eyes of the *Liga voor Mensenrechten/Ligue des droits de l'homme* the same suspicion cannot be condoned when it comes to school children. It creates an atmosphere of distrust in an environment where children are supposed to learn the value and attitude of mutual trust. One of the arguments in favour of biometric verification is that it prevents the loss of paper and plastic access badges. However, the *Liga voor Mensenrechten/Ligue des droits de l'homme* asserts that children have to acquire a sense of responsibility while growing up and learn that the loss of possessions entails consequences. An excessive pursuit of efficiency through the use of biometric identifiers takes away some essential growth and learning opportunities from children. Furthermore, it decreases possible forms of human interaction. Where physical access control or student registration still require some form of interaction between student and teachers, biometric identifiers aim to reduce this interaction to a minimum. This is detrimental within a school context where children are supposed to acquire interaction and communication skills. In sum, the *Liga voor Mensenrechten/Ligue des droits de l'homme* asserts that the use of impersonal, automated biometric identifiers deprives the educational system substantially of aspects of its human dimension.[257]

[255] The Hungarian response does not specify what kind of biometrics is being used.
[256] The Italian response does not specify what kind of biometrics is being used.
[257] Belgium, *Liga voor Mensenrechten/Ligue des droits de l'homme* (2013), *Big Brother Awards (2013) – Vingerafdrukken op school*, Liga voor Mensenrechten/Ligue des droits de l'homme.

Workplace

In **Estonia** the private sector makes use of fingerprints and iris scans for security and workplace entry reasons. In **Ireland** the principal difficulty across both the public and private sector arises from attempts to introduce biometric systems without the consultation or consent of intended users – such as employees in the workplace. The Irish DPA published guidance notes on its website regarding biometrics in the workplace. In **Italy,** biometrics systems, including biometric databases, have been deployed in the workplace, in particular for the control of employees' access to workplace areas. The Italian DPA issued several decisions regarding the use of biometrics in the workplace: (1) the blanket, unrestricted use of biometric data is not permitted. On account of their nature, these data require specific precautions to prevent harming data subjects. Therefore, as a rule it is not permitted to process fingerprint data to control the number of hours worked by employees; (2) using biometric data may only be justified in specific cases by taking account of the relevant purposes and context in which data are to be processed. This is the case, for example, if access to "sensitive areas" is to be regulated through the use of biometrics; (3) biometric verification and identification systems based on the reading of fingerprints stored as encrypted templates on media that are held exclusively by the relevant data subject should be preferred over centralised processing of biometric data. The DPA of **Malta** issued a paper entitled 'The Use of Biometrics Devices at the Workplace'. The DPA of **Monaco** prohibits the use of biometric systems based on fingerprints in the workplace. The private sector in **Serbia** makes use of biometric systems in the workplace to monitor the number of hours worked by the employees. Due to the violation of data protection legislation the further processing of biometric data was prohibited.[258]

The country responses show that the main difficulties of using biometrics are being encountered in the contexts of **sports, school and workplace**. The DPA in **Italy** encounters problems concerning the proportionality principle and the purpose limitation principle and recently found that the processing of biometric data to regulate access to a sports centre was disproportionate. While biometric systems are deployed in schools in **Hungary** and **Italy**, the DPA of **Lithuania** issued a prohibition order on the use of biometric systems based on fingerprints in schools. Biometric systems are deployed in the workplace (in the private sector) in the following Member States: **Estonia**, **Ireland**, **Italy**, and **Serbia**. The Italian DPA issued several decisions containing the requirements for using biometrics in the workplace. **Monaco** prohibits the use of biometric systems based on fingerprints in the workplace.

[258] The Serbian response is not clear as to whether the processing of biometric data in the workplace had been prohibited at all, or only the *further* processing of biometric data for other purposes than initially intended, which is a significant difference.

Chapter 8. Conclusions and recommendations

The overview of country reports shows that previous recommendations made by the Council of Europe (in the Council of Europe's 2005 progress report and the Parliamentary Assembly's 2011 report) have not lost their relevance. A coherent legal framework on biometrics is still lacking at each level – the level of the Council of Europe, the level of the European Union and the member state level. A small step forward is the relevant provisions on biometrics in the modernised convention 108 and the proposed EU Data Protection Regulation. The authors conclude and recommend (in bold) the following:

1. **In the opinion of the authors, the 2011 Parliamentary Assembly's report on biometrics captures all the main issues of the current legal debate on biometrics. The report contains many creative policy ideas regarding the regulation of biometrics. The central message is that additional regulatory measures, either soft law or hard law, need to be implemented in order to keep pace with developments in biometric technology and to harmonise the legal framework on biometrics across the CoE Member States. Data protection legislation should for example include the requirement to use biometric templates whenever possible, as it decreases the risk of abuse and misuse of biometric data.**

2. The 2005 progress report of the Council of Europe's Consultative Committee and the Parliamentary Assembly's report of 2011 both recommend the use of templates instead of raw biometric data. Unfortunately, the country reports show that only Estonia and Italy have noticed and implemented this recommendation. **Regulatory initiatives should also include a correct and useful definition of 'biometric data'.** The country responses show that very few countries have adopted legislation specifically aimed at the protection of biometric data. Georgia and Montenegro are the only two countries which have adopted a definition of biometric data. France and Georgia are pioneering the field of data protection in general and biometric data in particular.

3. In the 2012 modernisation proposal of Convention 108, drafted by the Council of Europe's Consultative Committee of Convention 108, the new Article 6 on the processing of sensitive data includes a provision concerning biometrics. By means of this proposal the Committee categorises biometric data as sensitive personal data. The 2013 draft explanatory report of the Consultative Committee includes the same categorisation, although it is not clear what the consequences of such a categorisation are. **More reflection is warranted about defining biometric data as sensitive personal data as it may imply that a distinction can no longer be made between more and less intrusive types of biometric processing.**

4. The European Court of Human Rights noted in its *Marper* judgment that "[…] *all three categories of the personal information retained by the authorities in the present cases, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of [Convention 108] as they relate to identified or identifiable individuals*." Therefore, all biometric data allowing the identification of an individual is protected by Article 8 of the European Convention on Human Rights (ECHR), according to the Court. The Court, however, recognised in its *Marper* judgment that fingerprints need to be distinguished from cellular samples and DNA profiles. The Court states that because of the information they contain, the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints. **In the Court's judgment one can find an argument not to label all biometric data as sensitive personal data. It**

is not clear what the consequences of such a categorisation are. Biometric data as a category of sensitive personal data implies that a stringent data protection regime is applicable to biometric data, meaning that a distinction can no longer be made between more and less intrusive types of biometric processing. The Court also considers that states which claim to be pioneers in the development of new technologies bear special responsibility for striking the right balance between biometric data retention and the right to respect for private life. **In the opinion of the authors of this report, it can be construed from the Court's statement that it should be obligatory to subject biometric projects to a privacy impact assessment. Such an obligation is provided in the proposed regulation, but it is not mentioned in the proposed directive.**

5. The European Commission, unlike the Council of Europe, does not define biometric data as sensitive personal data or even as a special category of personal data. The Council of Europe steers another course. In the modernisation proposal of the Consultative Committee regarding Convention 108 and the Consultative Committee's 2013 draft explanatory report of the modernised version of Convention 108 biometric data is considered sensitive data. **The European Commission and the Council of Europe's Consultative Committee both acknowledge the importance of a standardised definition of biometric data. The authors of this report endorse this acknowledgment.** The Committee's 2013 draft explanatory report contains the following definition of biometric data: "*data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter*". The European Commission and the Council of Europe are aware of the necessity to implement the requirement of a privacy impact assessment (sometimes called a data protection impact assessment). The Proposed Regulation contains such a requirement in Article 33, and the 2012 Modernisation Proposal of the Council of Europe's Consultative Committee includes such a requirement in Article 8bis(2). The country reports show that no Member State has yet implemented in their data protection legislation an obligation to perform a privacy impact assessment. However, France, Italy, the former Yugoslav Republic of Macedonia, Monaco, Montenegro and Slovenia incorporated the requirement of prior checking into their data protection legislation.

6. The Eurodac system, operational since 15 January 2003, enables European Union (EU) countries to help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union. The 2006 Commission Staff Working Document of the Commission of the European Communities shows that in 2005 the EURODAC Central Unit gave very satisfactory results in terms of speed, output, security and cost-effectiveness. However, the Eurodac system has also attracted considerable criticism because it requires the mandatory disclosure of biometric information by people who have not committed a crime. The following data are registered: the member state of origin, the digital fingerprint, the gender and the reference number used by the member state of origin. **The registration of biometric data and other additional information of the data subject may pose risks such as function creep, particularly because the disclosure of biometric data is mandatory. The risk for function creep is especially present when access is given to law enforcement agencies, as proposed by the Commission. Such access should only be possible in exceptional and well-defined circumstances. Special care should also be taken to avoid the use of biometric data as the key to link databases.**

7. The Schengen Information System (SIS) is used by border guards as well as by police, customs, visa and judicial authorities throughout the Schengen Area. Work on a new, more advanced version of the system, known as the second generation Schengen Information system (SIS II), is currently in progress and is assumed to become operational in April 2013. SIS II will have enhanced functionalities, such as the possibility to use biometrics (e.g. photos, fingerprints and, if necessary, even DNA profiles), the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries to the system. As soon as SIS II becomes operational it will increasingly be used by police crime investigation units. There are questions about the clarity of the rules governing collection and access to data in SIS II, including the desirability of granting access to immigration data to police and asylum authorities. The criticisms focus on loosely defined access criteria to subject data where access is for a purpose other than SIS II. **The use of (biometric) data for another purpose than that for which it was originally collected – called function creep – poses serious risks for the individual's rights and freedoms, particularly if more authorities are granted access to SIS. The inclusion of biometric data in SIS II threatens to change the purpose of this database from border control into criminal investigation. This demands a thorough evaluation of the legal framework to assure respect for necessity and proportionality principles, both for the inclusion of personal data into SIS II and for access to that data. Independent oversight by the data protection authorities should be foreseen, while special care should also be taken to avoid the use of biometric data as a key to link databases.**

8. The VIS system, operational since 11 October 2011, is a large-scale information system for visa requests to enter Schengen area countries. The VIS database will include information about personal identification of visa applicants (including biometrical data such as facial image and fingerprints), status of visa, authority that issued the visa, and record of persons liable to pay board and lodging costs. **Because the disclosure of biometric data and other additional information is mandatory, its registration may pose risks such as function creep. Special care should be taken to assure respect for the necessity and proportionality principles in the access to the data, while also avoiding the use of biometric data as a key to link databases. Independent oversight by the data protection authorities should be foreseen.**
9. The Council of European Justice and Home Affairs ministers adopted Regulation (EC) No 2252/2004 ('Regulation on standards for security features and biometrics in passports and travel documents issued by Member States') on 13 December 2004 without taking into account amendments proposed by the European Parliament. Unlike Eurodac, SIS and VIS, the European biometric passport is applicable to all European citizens. Biometric systems used in the context of the European biometric passport therefore pose risks to the rights and freedoms of all European citizens. The decisions to include mandatory facial images as well as finger scans, and the idea of a centralised database, were not questioned. Furthermore, little attention was paid by the EU institutions to meeting the requirements of proportionality and necessity. **It can be concluded that the EU does not always pay adequate attention to privacy issues regarding biometrics. The EU should reconsider the proportionality of the amount of biometric data to include in passports and the necessity of a central database. Independent oversight by the data protection authorities should be foreseen, while also avoiding the use of biometric data as a key to linking databases. The country reports show that only few countries incorporate privacy protecting provisions in legislation concerning biometrics. Regulation on biometrics should not be left to member states. The EU and the Council of Europe themselves should propose regulation.**

10. Second generation biometrics aims to identify a person on the basis of his or her behaviour or activities. Second generation biometrics comprises a new type of biometric features such as gait (manner of walking), voice, body odour, ECG (brainwave pattern), EEG (electrical activity of the heart), body temperature, and pupil dilation. These biometric characteristics can sometimes be collected from a distance whilst the data subject is unaware. This makes it more difficult to monitor whether biometric controllers comply with data protection legislation (e.g. informed consent by the data subject prior to biometric data processing). Due to second generation biometrics, an incremental change from visible to invisible data collection may occur. Biometric data may be originally collected for one specific purpose, but subsequently used for another purpose (function creep). Accordingly, it becomes more difficult to exercise the right to object to certain types of data processing. Moreover, biometric data may be used for profiling activities, while it is not clear whether and when profiling falls directly under the Convention. The Council of Europe concludes in its 2010 Recommendation that it is necessary to regulate profiling because profiling poses significant risks for the individual's rights and freedoms. Second generation biometrics can be used for profiling, meaning that individuals can be categorised. Unjustified selection due to profiling may result in discrimination and stigmatisation. **In the opinion of the authors the debate about the future legal framework on data protection should include a discussion about concerns regarding second generation biometrics, such as function creep, profiling, discrimination, and stigmatisation. This legal framework should clarify which profiling activities falls under its scope, limit the further use of biometric data and assure the respect of the rights of transparency and access.**

11. All biometric systems (without exception) have some intrinsic errors which can have a negative effect on the system's performance and accuracy (i.e. efficacy). The main error rates are the failure to enrol (FTE), failure to acquire (FTA), false accept error (FAR) and false reject error (FRR). All four intrinsic errors negatively affect the efficacy and efficiency of a biometric system. The FTE can often be reduced by means of assistance of trained personnel (human intervention) to the individuals who need to provide their biometric. The FAR and FRR can be reduced (although not to zero) by increasing the quality of biometric images. The FTA furthermore (but also the FTE, FAR and FRR) can be reduced by employing multimodal biometric systems, which make use of several biometric modalities. Two design modes offer best accuracy: (1) multiple biometrics from the same individual (e.g. fingerprint and iris), and (2) multiple units of similar biometrics (e.g. fingerprints from more than one finger). It can be concluded that the biometric systems' performance and accuracy depend on error rates, which can, for example, be reduced by human intervention, multimodal biometric systems and higher quality of biometric images. **The European legal framework on data protection should include provisions aiming to reduce the error rates of biometric systems such as provisions on human intervention, multimodal biometrics, high quality images and fall-back procedures. The principles of accuracy and transparency suggest a need for information duties concerning the accuracy of biometric systems in use and technical standards, especially when the results are used in legal proceedings and decisions affecting the data subject. In case of errors, alternative methods of identification and verification should be offered (see also the 2011 Parliamentary Assembly report).**

12. Biometric systems are susceptible to several threats, such as impostor threats (e.g. identity fraud, biometric database attack, enrolment fraud, spoofing and Trojan horse attacks) and additional threats (e.g. function creep, tracking and tracing, linking of biometric data to

other personal information, system failures and leakage of biometric data). Mechanisms to overcome vulnerabilities in biometric systems include human intervention, human supervision, liveness detection and multimodal biometrics. A major problem, however, is considered to be compromised biometric templates, as they can be reverse engineered to generate the original image of a biometric. Template protection methods proposed in the literature, which possess the four properties concerning template protection, can be categorised in feature transformation and the employment of a biometric cryptosystem. Both are effective methods to protect biometric templates. Although biometric templates as such are significantly safer compared to the use of raw biometric data, the country reports show that very few countries address the need to use templates. The Council of Europe's 2005 progress report and the 2011 Parliamentary Assembly's both recommend the use of templates instead of raw biometric data, but Mr Haibach's recommendations (in the 2011 report) regarding the use of templates have been noticed only in Estonia and Italy. The Estonian report underlines the importance to use biometric templates instead of raw biometric data. The Italian DPA is of the opinion that biometric data require specific precautions to prevent harming data subjects. For example, the storage of encrypted templates exclusively held by the data subject should be preferred over storage in central databases. **In the opinion of the authors, data protection legislation should include the requirement to use biometric templates whenever possible, as this decreases the risk of abuse and misuse of biometric data. Currently, data protection legislation lacks such a requirement.**

13. 8 out of 22 member states which responded to our questionnaire have adopted legislation specifically aimed at the protection of biometric data. These countries are Estonia, France, Georgia, Italy, the former Yugoslav Republic of Macedonia, Monaco, Montenegro, and Slovenia. The provision included most often in data protection legislation of these member states concerns prior checking. Prior checking is contained in data protection legislation of the following member states France, Italy, the former Yugoslav Republic of Macedonia, Monaco, Montenegro, and Slovenia. The member states addressing biometric data as a special category of personal data are Georgia and the former Yugoslav Republic of Macedonia. In Estonia biometric data is considered sensitive personal data. The member states which adopted a definition of biometric data are Georgia and Montenegro. Currently, neither Convention 108 nor the applicable European legislation specifically address biometrics. Provisions on prior checking have been adopted by several member states but are not (yet) addressed in legislation from the Council of Europe or the European Union.

14. The country responses show that the main difficulties of using biometrics are encountered in the contexts of sports, school and workplace. The DPA in Italy encounters problems concerning the proportionality principle and the purpose limitation principle and recently found that the processing of biometric data to regulate access to a sports centre was disproportionate. While biometric systems are deployed in schools in Hungary and Italy, the DPA of Lithuania issued a prohibition order on the use of biometric systems based on fingerprints in schools. Biometric systems are deployed in the workplace (in the private sector) in the following member states: Estonia, Ireland, Italy, and Serbia. The Italian DPA issued several decisions concerning the requirements for using biometrics in the workplace. Monaco prohibits the use of biometric systems based on fingerprints in the workplace. **Both the Council of Europe and the EU should propose hard and/or soft law to regulate the legal issues in the contexts of sports, school and workplace.**

Annex

The Council of Europe's 2005 progress report contains 12 recommendations:

Recommendation 1: Biometric data are to be regarded as a specific category of data as they are taken from the human body, remain the same in different systems and are in principle inalterable throughout life. They might be altered, however, for instance through aging, illnesses or surgical interventions.

Recommendation 2: Before having recourse to biometrics, the controller should balance the possible advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand, and consider possible alternatives that are less intrusive for private life.

Recommendation 3: Biometrics should not be chosen for the sole sake of convenience. Human dignity might be affected by the use of biometrics. Socio-cultural aspects and possible reluctance towards the instrumental use of the human body should be taken into account.

Recommendation 4: The biometric data and any associated data generated by the system must be processed for specific, explicit and legitimate purposes and should not be processed further for purposes that are incompatible with these.

Recommendation 5: The data should be adequate, relevant and not excessive in relation to these purposes. A technical system using biometric data should be configured to exclude the possibility to collect more biometric or associated data than is necessary for the purposes of the processing. Where templates are sufficient, the collection or the storage of the picture should be avoided.

Recommendation 6: In choosing the system architecture, the controller should balance the advantages and disadvantages for the data subject's private life on the one hand and the envisaged purposes on the other hand. A reasoned choice should be made between storage solely on an individual storage medium, a decentralised database or a central database, bearing in mind the aspects relating to data security.

Recommendation 7: The architecture of a biometric system should not be disproportionate in relation to the purpose of the processing. Therefore, if verification suffices, the controller should not develop an identification solution. Biometric data that are solely used for verification purposes preferably should be stored only on a secured individual storage medium, e.g. a smart card, held by the data subject only.

Recommendation 8: The data subject should be informed about the purposes of the system and the identity of the controller unless he or she already knows, and about the personal data that are processed and the persons or the categories of persons to whom they will be disclosed as far as the information is necessary to guarantee the fairness of processing.

Recommendation 9: The data subject has a right of access, rectification, blocking and erasure of the data relating to him or her. These rights extend to the biometric data undergoing automatic

processing attached to his identity, possibly associated data (such as date and place of use of the system) and to whom they have been communicated.

Recommendation 10: The controller should foresee adequate technical and organisational measures that aim to protect biometric and associated data against accidental or deliberate deletion or loss, as well as against illegal access, alteration or communication to unauthorised persons or any other form of illegal processing.

Recommendation 11: A procedure of certification and monitoring and control, if appropriate by an independent body, should be promoted, particularly in the case of mass applications, with regard to the quality standards for the software, the hardware and the training of the staff in charge of enrolment and matching. A periodic audit of the system's performance is recommendable.

Recommendation 12: If, because of a biometric system, a data subject is rejected, the controller should, on his or her request, re-examine the case and should, where necessary, offer appropriate alternative solutions. Procedures should be in place and made known to the data subject in the case of an allegedly false result of the system.