# The privacy legal framework for biometrics

Sprokkereef, A.C.J.; Cehajic, S.

*Publication date:*
2009

*Document Version*
Publisher's PDF, also known as Version of record

# FIDIS

Future of Identity in the Information Society

| | |
|---|---|
| Title: | "D13.4: The privacy legal framework for biometrics" |
| Authors: | WP13.4 |
| Editors: | Els Kindt (K.U.Leuven, Belgium), Lorenz Müller (AxSionics, Switzerland) |
| Reviewers: | Jozef Vyskoc (VAF, Slovakia), Martin Meints (ICCP, Germany) |
| Identifier: | D13.4 |
| Type: | Deliverable |
| Version: | 1.1 |
| Date: | 8 May 2009 |
| Status: | Final |
| Class: | Public |
| File: | |


***Summary***

The present report reviews the fundamental right to privacy and data protection which shall be assured to individuals and the Directive 95/46/EC which provides more detailed rules on how to establish protection in the case of biometric data processing. The present framework does not seem apt to cope with all issues and problems raised by biometric applications. The limited recent case law of the European Court of Human Rights and the Court of Justice sheds some light on some relevant issues, but does not answer all questions. The report provides an analysis of the use of biometric data and the applicable current legal framework in six countries. The research demonstrates that in various countries, position is taken against the central storage of biometric data because of the various additional risks such storage entails. Furthermore, some countries stress the risks of the use of biometric characteristics which leave traces (such as e.g., fingerprint, face, voice…). In general, controllers of biometric applications receive limited clear guidance as to how implement biometric applications. Because of conflicting approaches, general recommendations are made in this report with regard to the regulation of central storage of biometric data and various other aspects, including the need for transparency of biometric systems.




*The FIDIS NoE receives research funding from the Community's Sixth Framework Program*

# Copyright Notice:



***PLEASE NOTE:*** This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

# Members of the FIDIS consortium

| | |
|---|---|
| ***1. Goethe University Frankfurt*** | Germany |
| ***2. Joint Research Centre (JRC)*** | Spain |
| ***3. Vrije Universiteit Brussel*** | Belgium |
| ***4. Unabhängiges Landeszentrum für Datenschutz (ICPP)*** | Germany |
| ***5. Institut Europeen D'Administration Des Affaires (INSEAD)*** | France |
| ***6. University of Reading*** | United Kingdom |
| ***7. Katholieke Universiteit Leuven*** | Belgium |
| ***8. Tilburg University***[1] | The Netherlands |
| ***9. Karlstads University*** | Sweden |
| ***10. Technische Universität Berlin*** | Germany |
| ***11. Technische Universität Dresden*** | Germany |
| ***12. Albert-Ludwig-University Freiburg*** | Germany |
| ***13. Masarykova universita v Brne (MU)*** | Czech Republic |
| ***14. VaF Bratislava*** | Slovakia |
| ***15. London School of Economics and Political Science (LSE)*** | United Kingdom |
| ***16. Budapest University of Technology and Economics (ISTRI)*** | Hungary |
| ***17. IBM Research GmbH*** | Switzerland |
| ***18. Centre Technique de la Gendarmerie Nationale (CTGN)*** | France |
| ***19. Netherlands Forensic Institute (NFI)***[2] | The Netherlands |
| ***20. Virtual Identity and Privacy Research Center (VIP)***[3] | Switzerland |
| ***21. Europäisches Microsoft Innovations Center GmbH (EMIC)*** | Germany |
| ***22. Institute of Communication and Computer Systems (ICCS)*** | Greece |
| ***23. AXSionics AG*** | Switzerland |
| ***24. SIRRIX AG Security Technologies*** | Germany |

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

# Versions

| *Version* | *Date* | *Description (Editor)* |
|---|---|---|
| **0.1** | 11.01.2008 | • Suggested Table of Contents for Country Contributions (Els Kindt) |
| **0.2** | 15.03.2008 | • First draft of privacy legal framework and country reports for Belgium and France (Els Kindt and Fanny Coudert) |
| **0.3** | 15.05.2008 | • Updated draft of privacy legal framework for biometrics in the European Union (Els Kindt) |
| **0.4** | 16.02.2009 | • Updating draft and country reports for Belgium and France and integration of draft country report for Switzerland (Els Kindt) |
| **0.5** | 12.03.2009 | • Collection of country reports for Germany and United Kingdom and providing comments (Els Kindt) – Drafting introduction, conclusions and recommendations (Els Kindt) |
| **0.6** | 24.03.2009 | • Finalizing first draft and internal posting (Els Kindt) |
| **0.7** | 01.04.2009 | • Collection of the country report for the Netherlands and providing comments (Els Kindt) and integration of country reports for Germany, the Netherlands and the United Kingdom |
| **0.8** | 04.04.2009 | • Finalizing first completed draft ; review and finalizing introduction, conclusions, and recommendations (Els Kindt)<br>• Internal posting for review and input contributors on recommendations (Els Kindt) |
| **0.9** | 22.04.2009 | • Finalizing completed draft and internal posting for internal review (Els Kindt) |
| **1.0** | 08.05.2009 | • Final draft including comments of reviewers and submitted to the Commission for external review (Els Kindt) |

# Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

| *Chapter* | *Contributor(s)* |
|---|---|
| **Executive Summary** | Els Kindt (K.U.Leuven) |
| **1 Introduction** | Els Kindt (K.U.Leuven) |
| **2 The Privacy Legal Framework** | Els Kindt (K.U.Leuven) ; Suad Cehajic & Annemarie Sprokkereef (TILT) (section 2.3 (pp. 28-29) and section 2.4) |
| **3. Belgium** | Els Kindt (K.U.Leuven) |
| **4. France** | Els Kindt (K.U.Leuven), Fanny Coudert (K.U.Leuven) (section 4.3.4 and section 4.5 (p.63)) |
| **5. Germany** | Suad Cehajic & Annemarie Sprokkereef (TILT) |
| **6. The Netherlands** | Paul De Hert & Annemarie Sprokkereef (TILT) |
| **7. Switzerland** | Emmanuel Benoist (VIP) |
| **8. The United Kingdom** | Suad Cehajic & Annemarie Sprokkereef (TILT) |
| **9. Conclusions and Recommendations** | Els Kindt, Jos Dumortier (K.U.Leuven), with review and input by Lorenz Müller (AxSionics, Switzerland) and Emmanuel Benoist (VIP) |
| **Bibliography & Glossary** | Els Kindt (K.U.Leuven) |

# Table of Contents

# Executive Summary

Biometrics is a high tech identification technology that has grown in maturity over the last years and that is increasingly used for authentication in public and private applications.

While the focus of debate about biometrics was in the past in many cases on technical aspects of security and privacy, often in relation with the introduction of biometrics in the electronic passport (epass), decisions on a regulatory framework for the use of biometrics in general are hardly taken.

The present Fidis Deliverable D13.4 reviews the fundamental right to privacy and data protection which shall be assured to individuals because these principles are laid down in binding international conventions and national constitutions. The application of these fundamental rights upon new technologies, such as the processing of unique human characteristics for the verification or identification of individuals, however, is not self-explanatory. The Directive 95/46/EC provides more detailed rules on how to establish protection in case of personal data processing but seems not apt to cope with all issues and problems raised by biometric applications. The limited recent case law of the European Court of Human Rights and the Court of Justice sheds some light on some relevant issues, but does not answer all questions.

The report further analyses the use of biometrics and the applicable current legal framework for the processing of biometric data in various countries. Six country reports confirm that biometrics are not only introduced and deployed in government controlled wide scale deployments but are gradually entering our day to day lives, mainly for access control type of applications. In many countries, the national DPAs have issued (sometimes also technical (e.g., Switzerland)) guidelines and advice for the use of biometrics. The report demonstrates that in various countries, position is taken against the storage of biometric data in (central) databases because of the various additional risks such storage entails (e.g., unintended use for law enforcement purposes, other use without knowledge and function creep, ….). There is in that case a clear preference for local storage of the biometric data, for example, on a card or token. Only in exceptional cases, the position against central storage is confirmed in some specific national legislation, e.g., on the use of biometric identifiers in passports (e.g., Germany). However, the DPAs do not exclude all storage in central databases, and sometimes provide criteria (e.g., France, Belgium, …) which shall be applied in order to evaluate whether central storage could be acceptable. Furthermore, some countries stress the risks of the use of biometric characteristics which leave traces (such as e.g., fingerprint, face, voice, …). In other countries, such as in the Netherlands and the United Kingdom, there is a preference for storage in a central database for government controlled ID applications.

In general, controllers of biometric applications receive limited clear guidance as to how implement biometric applications. Because of conflicting approaches, general recommendations are made in this report with regard to the regulation of central storage of biometric data. Such legislation shall also address various other aspects, including the need for transparency of biometric systems and shall address the errors and technical failures of biometric systems.

This report aims at feeding the discussion about the regulation of the wider use of biometric data and the enactment of appropriate remedies for individuals subject to biometric technologies. The research, which contains a limited number of country reports, may need to be completed with additional research in other countries and further recommendations.

# 1 Introduction

Biometrics is a high tech identification technology that has grown in maturity over the last years and that is increasingly used for authentication in public and private applications.

The research on biometrics in general has been concentrated on the improvement of the technology and of the processes to measure the physical or behavioural characteristics of individuals for automated recognition or identification. Biometric technology has also been the subject of research of the NoE Fidis at regular intervals as an important factor of the future of identity. Previous Fidis work has analysed the state-of-the-art techniques, the technical strengths and weaknesses as well as privacy aspects as set out in the Fidis deliverables 3.2, 3.6 and 3.10. In these deliverables, various approaches of the use of biometrics were analysed from a multi-disciplinary perspective. The biometric methodologies and specific technologies have been analysed and described[4] and the deployment of biometrics in various contexts, such as in a PKI structure[5] or in Machine Readable Travel Documents[6] researched and presented. In these deliverables, various security and privacy aspects of biometrics were discussed as well.

In Fidis Deliverable D3.2, attention was given to the recommendations for the processing of biometric data of the Article 29 Data Protection Working Party contained in their working document on biometrics of 2003.[7] In Fidis Deliverable D3.6, an overview of the current European initiatives regarding the large scale deployment of biometrics, such as in Eurodac (the EU central fingerprint database in connection with asylum seekers), the Visa Information System (VIS – the EU central database set up to create a common visa policy) and the European Passport (requiring fingerprints and facial images as biometrical identifiers) was provided. The legal basis for these systems was analysed and critically discussed, as well as the compliance with the data protection Directive 95/46/EC and fundamental human rights.[8]

In Fidis Deliverable 3.10, the technical details of a biometric authentication process were described and illustrated in detail.[9] It was also convincingly argued and demonstrated that biometric data become an increasingly used key for interoperability of databases, without an appropriate regulation. To facilitate the discussion on biometrics, it was further proposed to make a classification of applications models which use biometrics, depending on differences in control, purposes, and functionalities. The application types that were introduced are the Type I – government controlled ID applications, the Type II – security and access control applications, the Type III – public/private partnership applications, the Type IV Convenience and personalisation applications and the Type V - Tracking and tracing (surveillance)

---

[4] M. Gasson, M. Meints, *et al*., (eds.), *D.3.2. A study on PKI and biometrics*, FIDIS, July 2005, ('Fidis Deliverable D3.2'), p. 62 *et seq*.
[5] *Ibid.*, p. 120 *et seq.*
[6] M. Meints and M. Hansen (eds.), *D.3.6. Study on ID Documents*, FIDIS, December 2006, 160 p. ('Fidis Deliverable D3.6').
[7] Article 29 Data Protection Working Party, *Working document on biometrics, WP 80*, 1 August 2003, 12 p. ('WP 29 Working Document on Biometrics'). The Article 29 Data Protection Working Party was set up under Article 29 of the Directive 95/46/EC as an independent European advisory body on data protection and privacy and consists of representatives of the national Data Protection Authorities of the EU.
[8] M. Meints and M. Hansen (eds.), *o.c.*, p. 40 *et seq.*
[9] E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, FIDIS, December 2007, 130 p. ('Fidis Deliverable D3.10').

applications.[10] The distinction of the use of biometrics for verification and identification purposes was stressed and the research also showed that various technical aspects of biometric systems are not taken into account in the legal treatment of biometrics. This results in a considerable 'margin of appreciation' of the national Data Protection Authorities (hereafter 'DPAs') in their opinions on biometric systems, whereby the proportionality principles plays an important role.[11]

The present Fids Deliverable D13.4 contains various country reports from a legal point of view which illustrate that biometrics are not only deployed in wide scale deployments but are gradually entering our day to day lives. The use of biometric applications, however, is often debated and criticized. Biometric data are in most cases personal data to which article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the data protection legislation apply, but this legislation does not mention biometric data explicitly. As a result, the legislation does not provide an adequate answer to many questions in most cases. This deliverable aims at analyzing the gaps in the present legal framework which shall tackle the issues of the increasing use of biometric data in various identity management systems.[12] This deliverable will hereby make further use where possible of the classification proposed in Fidis Deliverable D 3.10 and mentioned above in order to facilitate the discussion.

Six country reports discuss the spreading of biometric applications and the applicable legislation. The reports - by tackling similar key aspects of biometrics - illustrate how the gaps in the general legal framework are handled and may provide useful suggestions for an appropriate legal framework for biometric data processing. The country reports have been prepared on the basis of legal research. However, in order to describe the domains in which biometrics are used and debated, additional sources have been taken into account, including reports with a broader focus than only legal aspects and press releases. The use of biometric data also raises ethical questions, but these will not be discussed in this report.[13] The present deliverable will conclude with some specific recommendations to policy makers and the legislator.

The content of the research for this deliverable is updated until the end of March 2009.

The views expressed in this report represent the opinion of the authors only and do not bind their organisation, other Fidis members or the EU institutions.

---

[10] *Ibid.*, p.60 *et seq.*
[11] *Ibid.*, p. 37 *et seq.*
[12] Only for specific large-scale biometric databases in the European Union, such as Eurodac, VIS, SIS II and the epass, regulations containing specific but incomplete requirements for biometrics were enacted.
[13] About the ethical questions, we refer to the Biometric Identification Technology Ethics project (BITE), an EU project N°. SAS6-006093. Information is available at www.biteproject.org. About ethical aspects, see also the Commission de l'Ethique de la Science et de la Technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Québec (Canada), 2005, 42 p. and the National Consultative Ethics Committee for Health and Life Sciences, *Opinion N° 98. Biometrics, identifying data and human rights*, France, April 2007, 22 p.

# 2 The privacy legal framework for biometrics in the European Union

## 2.1 Introduction

At the end of the 1970s, some realized that a new 'information age' was commencing in which the processing of information would play a major role. Because some of this information related to individuals, the Organisation for Economic Cooperation and Development ('OECD') issued upon initiative of the United States the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These OECD Guidelines in fact stressed the need to ensure the free flow of data. This free flow was threatened by the at that time increasing – by some perceived as redundant and annoying[14] – concern for privacy. Soon thereafter, however, the Council of Europe issued Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[15] The Convention was opened for signature in January 1981 in Strasbourg and was – contrary to the OECD Guidelines - really concerned about privacy: it attempted to reconcile the right to privacy with the transfer of personal data. The Convention was the first legally binding international instrument in the data protection field. It imposed upon the Member States of the Council of Europe an obligation to issue legislation which would enforce various declared principles, such as there were the data minimization and the purpose specification principle. The Convention further intended to harmonize the at that time existing but fragmented legislation relating to data protection.[16]

About fifteen years later, the 1980 Guidelines and the Convention No. 108 were further completed with the Directive 95/46/EC (the 'Data Protection Directive' or 'Directive 95/46/EC') and, some years thereafter, with the Directive 2002/58/EC (the 'ePrivacy Directive').

In the meantime, more than a decade has lapsed since the adoption of Directive 95/46/EC and privacy has become an increasingly important concern. In this period, telecommunication networks and the Internet have introduced a new 'communication age': online electronic communications and the collection and use of (personal) data will never be what they were before. New legal rules have been introduced, for example for e-commerce, such as relating to the liability of information service providers and for making online contracts legally valid and binding. But the privacy legislation – apart for electronic communications – has barely been changed or completed. At the same time, the technology is further developing, including technologies for the authentication of persons.

---

[14] See e.g., H. Lowry, 'Transborder Data Flow: Public and Private International Law Aspects', *Houston Journal of International Law*, 1984, (159-174), p. 166 : 'As the reader can see, very little of this information is about individuals. Most transborder data flows are by organizations and about their operations. *Privacy plays a very minor part* of the import and export of this type of information. Certainly some data, such as payroll or personnel files, should be protected. *But often privacy is just a convenient club with which to beat to death the freedom to exchange information'* (stress added).

[15] Council of Europe, ETS No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, available at http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm

[16] See P. Miller, 'Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information : An Introduction to the Arrival of the New Information Age', *Columbia Journal of Law and Social Problems*, 1986, (89-14), p. 120.

Biometrics is an authentication technology which is very promising. Biometric systems are implemented for various purposes by various actors, whether private or public. However, many agree that privacy risks are one of the important factors which reduce the willingness to fully engage biometric methods. Another aspect is that the current privacy legal framework does not provide clear answers to many issues relating to the processing of biometric data. The legislation is not adapted to cope with biometric authentication methods. The general principle of the right to privacy as laid down in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 ('Article 8 ECHR'), Article 7 and Article 8 of the EU Charter of 2000 and the general Data Protection Directive 95/46/EC need to solve the various (privacy) issues of biometrics, but do not provide legal certainty because many questions remain unsolved. It seems therefore that this new wave of the 'communication age' challenges the existing legal framework again.

In this first chapter, the application of the present privacy and data processing provisions which are relevant for biometrics and the difficulties of the application of these provisions will be demonstrated and discussed.

At the same time, biometric data is already increasingly used in specific, often large scale public sector systems, such as in the European epassport, but also in Eurodac, VIS and SIS II. As set out in Fidis Deliverable D3.6, specific regulations were made for these large-scale systems. To the extent relevant, some of these systems will herein be briefly touched, but the legal aspects of the processing of biometric data in these large-scale biometric systems will not be discussed in depth. This deliverable D.13.4 aims principally at discussing the legal aspects of the processing of biometric data in general, in particular in 'civil' applications (hereby excluding applications used for public or national security or for law enforcement purposes). The Directive 95/46/EC is moreover not applicable in these cases.

The Article 29 Data Protection Working Party and the European Data Protection Supervisor (hereafter the 'EDPS') have over the last five years issued numerous opinions and recommendations with regard to the use of biometric data.[17] These opinions provide valuable guidelines since the existing legal framework is too general compared to the need for clarification imposed by the processing of biometric data. Some of these significant opinions of the Article 29 Data Protection Working Party and the EDPS are therefore in this deliverable recapitulated (see section 2.5).

The Consultative Committee of the Convention No. 108 of the Council of Europe has also issued in 2005 a so-called 'progress report' on the application of the data protection principles on the processing of biometric data.[18] This deliverable will refer to this report, but as it is intended to revise or complement the progress report, it will not be discussed in depth herein.

---

[17] These opinions were necessary mainly because some political developments have resulted in a consensus to introduce biometrics in various applications on EU level, in particular the introduction in passports and travel documents, in the related Visa Information System (VIS), and in the second generation Schengen Information System (SIS II) (see *above*).

[18] Consultative Committee of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data [CETS No. 108] (T-PD), *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, Council of Europe, CM(2005)43, March 2005 ('*Progress report*, Council of Europe'), available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)43&Language=lanEnglish&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=

## 2.2 Fundamental rights in the European Union: Right to respect for privacy and the right to data protection

The right to respect for privacy (Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 of the EU Charter) and the right to data protection (Article 8 of the EU Charter) are fundamental rights in the Member States of the European Union.[19]

While the right to respect for privacy is already recognized for a long time as a human right, the explicit recognition of the right to data protection as a fundamental right is far more recent. The fundamental right to data protection was listed in the Charter of Fundamental Rights of the European Union (Charter) which was proclaimed and published in 2000.

### 2.2.1 Article 8 of the European Convention on Human Rights

*The concept of private life and the recording and storage of information relating to identity*

The right to respect for one's private (and family) life is one of the human rights and fundamental freedoms that was listed in 1950 in the European Convention for the Protection of Human Rights and Fundamental Freedoms concluded in the framework of the Council of Europe (hereinafter the 'Convention').[20] The notion of one's private life is 'a broad term not susceptible to exhaustive definition' and the European Court of Human Rights in Strasbourg (hereinafter the 'Court') has continuously interpreted the concept of 'private life'. As a result, private life does not merely cover the physical and psychological integrity of a person, but also embraces multiple aspects of a person's identity.

In recent case law, the Court has repeatedly stated that the concept of private life *extends to aspects of a person's physical and social identity*, and includes protection of a person's name and a person's right to his image.[21] The Court stated that Article 8 of the Convention protects *a right to identity* and a right to personal development, also in interaction with other persons, even in a public context.[22]

The concept of private life has known a continuing evolution in the case law of national courts and of the Court, also in view of threats posed by new technologies. Because of the increasing processing of information, the Court also gradually included a right to data protection in article 8 of the Convention.[23]

---

[19] For other human rights that may be involved, such as the freedom of movement and the human right to a fair trail, we refer to M. Meints and M. Hansen (eds.), *o.c.*, pp. 54 – 55.

[20] Council of Europe, ETS no. 005, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, 4 November 1950, available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm This Convention is to be distinguished from Convention No. 108 discussed *above*.

[21] ECHR, *Sciacca v. Italy*, no. 50774/99, 11 January 2005, § 29 ('*Sciacca v. Italy*').

[22] ECHR, *Peck v. U.K.*, no. 44647/98, 28 January 2003, §57 ('*Peck'*).

[23] The Court, however, hereby initially did not interpret the right to data protection in the same way as the right as laid down in the data protection legislation, for example in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1981. The Court for example made a distinction between privacy sensitive information and non privacy sensitive information. See on this issue, P. De Hert, 'Grondrechten die bijna niet verdedigd kunnen worden; De bescherming van persoonlijke gegevens op het Internet', *De rechten van de mens op het internet*, Maklu, Antwerpen – Apeldoorn, 2000, (21), p. 33.

The Court, for example, stated that private life considerations may arise when, taking into account a person's reasonable expectations as to privacy, systematic or permanent *records* are made from a public scene.

The Court also decided that a *recording*, for example of *voices*, for further *analysis*, was regarded as the processing of personal data and was of direct relevance to identifying that person when considered in conjunction with other personal data, amounting to an interference with the right to respect for their private life.[24] The *unforeseen use* of *photographs* may also amount to an invasion of privacy.

The fact that a person is an 'ordinary person' (as compared with a public figure, such as a politician, etc) enlarges the zone of interaction which may fall within the scope of private life. This distinction between ordinary persons and public figures, however, seems to disappear in more recent case law of the Court.

A person's reasonable expectations as to privacy are significant but not necessarily a conclusive factor. The fact *that a person is subject of criminal proceedings* does *not curtail* the scope of the protection of Article 8 of the Convention either.

There is hence increased attention for interference with aspects of a person's identity in recent case law of the Court, which it finds to be in breach of Article 8 of the Convention especially when the recording and storage of data is involved.

This is a contrast with the case law of the Court of the nineties, when the Court or the Commission[25] paid *less attention to possible threats* posed by the recording of identity information. In a case of 1995, *Friedl v. Austria*, Mr. Friedl who participated in a demonstration in Vienna, complained that the police took video recordings of the public demonstration, noted down personal data and took photographs individually of him. In that case, which resulted in a friendly settlement, the Commission expressed the opinion that there had been no breach of Article 8. The Commission hereby gave importance to the fact that no names were noted down and hence in its view the photographs taken remained anonymous, the personal data recorded and photographs taken were not entered into a data-processing system and *no action had been taken to identify the persons photographed on that occasion by means of data processing*.[26] This decision was in line with another case of that decade, Reyntjes v. Belgium[27] of 1992, where the Commission did not find that the registration of identity data of an ID card was in breach of Article 8 of the Convention.

In these (earlier) cases, more attention was paid to the *actual* use that is made of the data in the particular case, rather than *the possible uses* that could be made of the identity data recorded for deciding on interference of the private life right.

Video monitoring or the use of photograph equipment which does not record visual data as such, however, is considered by the Court to fall outside the application field of Article 8 of the Convention. In *Pierre Herbecq and Ligue des droits de l'homme v. Belgium*[28] of 1998, the Commission found that video surveillance did not automatically come within the scope of Article 8 unless specific criteria were fulfilled. In the decision *Peck*, the Court reminded of its

---

[24] ECHR, *P.G. and J.H. v. U.K.*, no. 44787/98, 25 September 2001, §59-60.
[25] In previous cases, not only the Court but also the competent Commission made decisions.
[26] ECHR, *Friedl v. Austria*, 31 January 1995, §§ 49-51, Series A no.305-B.
[27] *F. Reyntjens v. Belgium*, Commission decision, 9 September 1992.
[28] *Pierre Herbecq and Ligue des droits de l'homme v. Belgium* , nos. 32200/96 and 32201/96, Commission decision, 14 January 1998, *A.J.T.*, 1998 with note of P. De Hert and O. De Schutter, pp. 501-511.

position and stated that (only) the *recording* of the data and the systematic or permanent nature of the record may give rise to the application of Article 8.[29]

Although the decisions referred to above do not explicitly refer to automated recognition or identification by biometrics, the judgements and decisions do warn for the processing of personal data, such as of images and of voices, which would permit identification or allow additional uses which the person in question did reasonably not foresee.

In various decisions, the Court stressed that 'increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data'.[30] Because of the privacy (and security) risks, such vigilance is in our opinion also required for biometrics.

In the significant recent case *S. and Marper v. the United Kingdom*, that is also considered important by the Court because the 'Grand Chamber' decided it, and that pertains to the retention of DNA and fingerprint, the Court continued its general approach as in respect of photographs and voice samples. The Court noted that 'fingerprint records constitute personal data (…) which contain external identification features much in the same way as, for example, personal photographs or voice samples'.[31] The Court stated that 'fingerprint objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances' and that the 'retention of fingerprints on the authorities' records (…) may in itself give rise (…) to important private-life concerns'.[32] In this case, the Court further concluded that the retention of cellular samples and DNA profiles disclosed an interference with the right to respect for private life within the meaning of the Article 8 §1 of the Convention.

Future decisions will shed further light on how the right to private life and Article 8 of the Convention shall be interpreted in the case of the use of biometric characteristics and data.

*Restrictions*

Fundamental rights, including the right to respect for one's private life, are not always absolute. It means that it is possible to interfere with them and to restrict them, but only in specific circumstances and if the restriction and the means used are in proportion with the objectives sought.[33] Article 8 §2 of the Convention stipulates the conditions under which interferences with this right to respect for private life are possible as follows:

> *'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.'*[34]

[29] *Peck*, §59.
[30] ECHR, *Von Hannover v. Germany*, no. 59320/00, 24 June 2004, § 70.
[31] ECHR, *S. and Marper v. United Kingdom* [GC], no. 30562/04, 4 December 2008, § 80 ('*S. and Marper*').
[32] *Ibid.*, §§ 84-85.
[33] See E. Kindt and L. Müller (eds.), *o.c.*, p. 72 *et seq.*
[34] Art. 8 §2 Convention.

Because of the privacy risk of the use of biometric technologies, such as unobserved and non-interactive authentication, use of biometrics for tracking and surveillance purposes, direct identify ability, link ability and profiling, use of additional information contained in biometric characteristics, but also violation of the purpose binding principle, problems regarding revocability and risks of identity theft, all and more as described in the previous Fidis deliverables as mentioned above, biometrics could lead to an interference with the right to privacy.

Hence, any interference that biometric systems impose with the right of privacy must, in the light of Article 8 of the Convention and of the case law related thereto, be adequately based and provided for in a law in a clear and generally comprehensible way (interference 'in accordance with the law') and pursuing 'a legitimate aim', both being tested as being 'necessary in a democratic society' to achieve that aim and in so far the restriction is relevant and proportionate. These three steps test for interference with private life are hereunder further illustrated by some selected decisions of the Court where possible which involve the processing of personal data, such as images or voice.

*a. 'In accordance with the law'*. The deployment of biometric systems is because of the privacy risks only permitted if there is a law which provides for the use of the biometrics. Biometric systems of Type 1 government controlled ID (whether or not with central database(s))[35] are therefore only possible if there is a law providing for a legal basis for such identity control.

The law shall have in addition particular qualities. The phrase 'in accordance with the law' requires, according to the Court,

> (1) that the impugned measure should have some *basis in domestic law*,
>
> (2) the law in question should be *accessible* to the person concerned,
>
> (3) the person *must be able to foresee its consequences,*
>
> (4) the law is *compatible with the rule of law*, and
>
> (5) the impugned measure *complies with the requirements* laid down by the domestic law providing for the interference.[36]

In *Sciacca v. Italy*, the Court found that there was no law governing the taking of photographs of people under suspicion or arrested, but rather a practice which had developed, and that the interference was therefore not 'in accordance with the law'. In *Perry v. United Kingdom*, the Court found that there was a legal basis for the use of access control video taping images for identification (and prosecution) purposes of a person who had refused the so-called 'Oslo confrontation', but that the police did not comply with the requirements laid down in that law, in particular failed to inform the person and to ask his consent.[37] This requirement is set out because a law must provide sufficient guarantees against the risk of abuse and arbitrariness.

The question arises whether without a legal basis, use of images or fingerprint for identification purposes by the government (see Type 1 Government controlled ID applications) or any other controller could also possibly be lawful if one would consent with

---

[35] For the various types of biometric applications , see E. Kindt and L. Müller (eds.), *o.c.*, section 3.3.3.
[36] See ECHR, *Perry v. United Kingdom*, no. 63737/00, 17 July 2003, § 45 ('*Perry*').
[37] *Perry*, §47-49. In the case, the Court held unanimously that there had been a violation of Art. 8 of the Convention for lack of compliance with the requirement 'in accordance with the law'.

such control.[38] Consent is also often relied upon for Type 2 access control applications. However, in such case, some Data Protection Authorities have already stated that in case the processing is not proportional (see hereunder step 3), such consent will not be sufficient.

*b. Legitimate aim.* The deployment of biometric systems is because of the privacy risks only permitted if there is a legitimate aim[39] which provides for the use of the biometrics. A legitimate aim can be the prevention and prosecution of crime.

In *S. and Marper v. United Kingdom*, the Court *agreed* with the government of the United Kingdom that the retention of fingerprint and DNA information pursues *the legitimate purpose of the detection and the prevention of crime*. It further distinguished the original taking of the information for linking a person to a particular crime from the retention of it and clarified that the retention as such pursues the broader purpose of assisting in the identification of future offenders. In its analysis, the Court implicitly seems to accept that the use of retained samples for identification of future offenders still remains within this legitimate aim as it does not further elaborate as to whether identification of future offenders falls with the general legitimate aim of the prevention or detection of crime. As a result, some will defend that the registration in connection with the investigation of an offence and the keeping of identifying biometric data by police authorities for the prevention or detection of crime even in the future is a legitimate aim.

*c. 'Necessary in a democratic society'.* Any interference, *even for a legitimate aim* and with a legal basis, however, shall be 'necessary in a democratic society'.

Case law of the Court explains that 'necessary in a democratic society' means that

> (1) the interference shall be justified by 'a *pressing social need'*,
>
> (2) the interference shall be *proportionate* to the legitimate aim pursued, and
>
> (3) the reasons adduced by the national authorities to justify it shall be '*relevant and sufficient'*.

The proportionality principle in the strict sense involves the need of a check of the proportionality of the *means* used which interfere with private life with the legitimate *aims*. For biometrics, it means that one shall check in particular whether the deployment of biometrics is an appropriate and necessary means to reach the goal.

In the fore-mentioned case *S. and Marper*, the Court found that the retention of fingerprint, cellular samples and DNA profiles of persons suspected but not convicted, as applied in the case at hand, including the retention of such data of a minor, failed to strike a fair balance between the competing public and private interests.[40] The Court hereby considered that it is

---

[38] See and compare also with the explicit reference to consent in Article 8 of the EU Charter (see *below*).

[39] A legitimate aim as set forth in Article 8 of the Convention includes the prevention of crime, for example, of 'look alike' fraude with international passports and travel documents.

[40] See also the web commentary on the Marper case by B.-J. Koops and M. Goodwin, *Strasbourg sets limits to DNA databases*, available at www.tilt.nl. The authors have written this commentary immediately following the GC's decision. With regard to the balance between private and public interests, the authors stated the following: 'Having established that privacy was at stake, the next question for the Court was to decide whether the retention was necessary within a democratic society. The Court was 'struck' by the blanket and indiscriminate nature of the powers of retention, powers which are not time-limited and do not distinguish between suspected offenders on the basis of the gravity of the crime of which they are suspected. Moreover, the Court was particularly critical of the failure to distinguish between adult and minor offenders and noted the need to pay special attention to the privacy needs of minors within the criminal justice system. Further, it noted the ability of ethnicity to be deduced

acceptable that the database of the case at hand may have contributed to the detection and the prevention of crime. The final review that was made for the proportionality test however is in our view factual and will therefore vary from case to case.

Based on the review made in *S. and Marper*, one could conclude for the time being that the specific provisions of the legal basis which provide for the interference will have to be taken into account and when they provide for the processing of personal data, they will have to be reviewed as to what *safeguards* are built in for the protection of private life. Questions which may be raised may include whether (i) the data collected are not excessive but minimal in relation to the purposes envisaged, (ii) the data are preserved in a form which permits identification for no longer than is required, (iii) there are adequate guarantees to efficiently protect the data against misuse and abuse[41], but also whether there is (iv) an indiscriminating element in the power of decision on the processing of the data, (v) an age minimum of persons whose personal data are collected and retained, (vi) a time period for retention, and (vii) a right to object of the data subject and independent review of the data processing.[42]

The level of interference may also differ in view of the nature or the category of personal data processed. The processing of cellular samples, for example, is particularly intrusive given the wealth of genetic and health information contained therein.[43] As stated in Fidis deliverable D3.10, other biometric data may also contain information relating to health. Such 'sensitive information' will differ for each kind of biometric data.

One shall note that national authorities will enjoy a *certain margin of appreciation* when assessing whether an interference with a right protected by Article 8 of the Convention was necessary in a democratic society and proportionate to the legitimate aim pursued. Nevertheless, the Court will give the final ruling whether the measure is reconcilable with Article 8. In *S. and Marper,* the Court stated however that 'where a particular important fact of an individual's existence or identity is at stake, the margin allowed to the State will be restricted'.[44] The Court further said that it considers the protection of personal data of fundamental importance to a person's enjoyment of his or her right to privacy, especially in case of automatic processing'.[45]

It is expected that the courts will further elaborate relevant criteria to be used in order to assess whether the use of biometric data is necessary in a democratic society and proportionate to the legitimate aim pursued. One important element will be whether the aim of the processing could not be reached with other means which interfere less with the right to respect for privacy. The weight to be attached to the respective criteria *will however vary according to the specific circumstances of each case.*

---

from DNA samples and restated its position that an individual's ethnic identity falls within the meaning of privacy within Article 8; however, it did not elaborate on this element within its reasoning. For these reasons, the GC found that the balance between private and public interests had not been well met and the UK had overstepped its margin of appreciation.'

[41] *S. and Marper,* §103.

[42] These criteria were mentioned in *S. and Marper*, §119.

[43] *S. and Marper* § 120.

[44] *S. and Marper* § 102. In the same case, the Court discovered a consistent approach in most Council of Europe Member States towards the collection and retention of DNA samples and profiles in the police sector, i.e., only collection from individuals suspected of offences of a minimum gravity and destruction immediately or within a limited period after acquittal or discharge, with only a limited number of exceptions (*S. and Marper* §§ 108-110). Therefore, because of a strong consensus amongst Contracting States, the margin of appreciation is narrowed in the assessment of permissible interference with private life in this context.

[45] *S. and Marper* § 103.

The fore mentioned requirements under Article 8 of the Convention are also reflected to some extent in Directive 95/46/EC.[46] While the Directive 95/46/EC imposes similar requirements for the deployment of biometric systems, other requirements of the Directive 95/46/EC impose additional conditions and concerns, which will be discussed *below*.

### 2.2.2 Articles 7 and 8 of the EU Charter

The Charter of Fundamental Rights of the European Union (EU Charter) contains various human rights provisions, and includes the explicit right to respect for privacy (Article 7) and an explicit right to protection in case of personal data processing (Article 8).

The Charter was proclaimed and published in December 2000.[47] Subject to the ratification of the Treaty of Lisbon, the provisions of the Charter will become legally binding in (most of) the EU Member States (see Article 6.1 of the Lisbon Treaty).

Article 7 of the EU Charter is stated as follows :

> *'**Respect for private and family life***
>
> *Everyone has the right to respect for his or her private and family life, home and communications.'*

This Article 7 of the EU Charter does not list the conditions under which interference with this right would be possible.

Since it is explicitly stated that the Charter reaffirms the specific fundamental rights and freedoms as already set forth in the constitutions of the Member States and international treaties, in particular in the European Convention for the Protection of Human Rights and Fundamental Freedoms and that these provisions shall be applied in conformity with the interpretation of such rights, it is expected that the same exceptions as stated in Article 8 of the Convention would apply.

Article 8 of the EU Charter is stated as follows:

> *'**Protection of personal data***
>
> *1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3. Compliance with these rules shall be subject to control by an independent authority.'*

This Article 8 of the EU Charter refers to some specific data subject's rights such as the requirement that the data shall by fairly processed for specified purposes on a legitimate basis and the right of access and correction. One could wonder on what basis these rights where explicitly chosen amongst various other rights of the data subject (including the right to information) as already laid down in previously enacted data protection legislation.

---

[46] See E. Kindt and L. Müller (eds.), o.c., p. 73.
[47] *O.J.* C 364, 18 December 2000, p. 1.

The choice of the data subject's rights in Article 8 may be relevant for the processing of biometric data. The reference to consent, however, may confuse, as the Article 29 Data Protection Working Party and various DPAs have already indicated that consent is in some particular situations biased (e.g., in the relationship employer-employee).

## 2.3 The Data Protection Directive 95/46/EC

*Scope of Directive 95/46/EC*

The Data Protection Directive 95/46/EC[48] is applicable to the processing of personal data, including the processing of biometric data. Biometric systems which process voice or images of persons, however, will not always fall under the provisions and obligations of the Directive.[49] In general, the Directive 95/46/EC is limited to the processing of personal data *other than concerning public security, defence, State security* (including the economic wellbeing of the State when the processing operation relates to State security matters) and the activities of the State in areas of *criminal law*.[50] For the processing of voices, images and other personal data by justice and home affairs authorities for these purposes, specific data protection rules are being set up, but the attempt to install an adequate protection seems not very successful.[51] Biometric data is often (intended to be) used for one or more of the above mentioned purposes, including the prevention and prosecution of criminal offences. In that case, the Directive 95/46/EC does not provide any rules.

In addition, Member States can *restrict* specific obligations and rights under the Directive 95/46/EC, such as the right to be informed, if necessary to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, important economic or financial interests of a Member State (such as monetary and taxation matters), the exercise of an official authority for such purposes or the protection of rights and freedoms of others (Article 13 of the Directive).

The processing of biometric data by a natural person for *purely personal or household activities* (e.g., for access to a laptop used for other than professional activities, or for access to someone's home) does also not come within the scope of the Directive.[52]

In all other circumstances, biometric systems fall within the application field *ratione materiae* of the Directive, whether operated by a public or private data controller, if they are used in the

---

[48] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23 November 1995, pp. 31-50.

[49] Recital 16 of the Directive 95/46/EC reiterates that the processing of sound and image data for purposes of public security, defence, national security or processed in the course of State activities for criminal law purposes or other non community matters, is not subject to the provisions of the Directive.

[50] Art. 3.2 of the Directive 95/46/EC.

[51] This results in a multitude of legislative proposals. See E. Kosta, F. Coudert and J. Dumortier, 'Data protection in the third pillar : in the aftermath of the ECJ decision on PNR data and the data retention directive', *Bileta*, Annual Conference, 2007, published and available at http://www.bileta.ac.uk/Document%20Library/1/Data%20protection%20in%20the%20third%20pillar%20-%20in%20the%20aftermath%20of%20the%20ECJ%20decision%20on%20PNR%20data%20and%20the%20data%20retention%20directive.pdf. See also the recently adopted Framework decision of the Council on the processing of personal data in the third pillar discussed in section 2.4. According to article 34 §2 of the EU Treaty, framework decisions are adopted to align law and regulations of the Member States.

[52] Compare with the Type IV convenience model type of application, as defined in E. Kindt and L. Müller (eds.), *o.c.*, p. 60 *et seq.*

context of activities of an establishment of such controller on the territory of an EU Member State or if equipment is used on such territory (other than for transit purposes).

*The Directive 95/46/EC and biometric data*

It is generally accepted that the Directive 95/46/EC applies to the processing of biometric data because biometric data is generally considered as 'information relating to an identified or identifiable natural person' (Article 2 (a) of the Directive). Biometric data, however, comes in various formats (raw data or template form), protected or unprotected, and therefore the question as to whether biometric information remains personal data is still raised from time to time.

The Article 29 Data Protection Working Party has also looked into this issue. In its working document on biometrics, it stated that '*measures of biometric identification or their digital translation in a template form in most cases are personal data'*. In a footnote, however, the Article 29 Data Protection Working Party left open the possibility that '[i]n cases where biometric data, like a template, are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject, those data should not be qualified as personal data'.[53] It was, however, not clear how these 'reasonable means' shall be understood. In a more recent opinion of 2007 on the concept of personal data, the Article 29 Data Protection Working Party stated that for assessing *all the means likely reasonably to be used to identify* a person, all relevant factors shall be taken into account, including not only the cost of conducting identification, but also the intended purpose, the way the processing is structured, the advantages expected by the controller and the interests of the data subjects.[54]

In addition, the test is a dynamic test, and shall not only take the state of the art in technology at the time of the processing into account, but *also the possibilities of future technologies* during the *period of the processing* of the data.[55] This clarification is significant for biometrics. Biometric technologies are in constant development. For example, images taken by a satellite system or a video surveillance camera system may not (yet) allow sufficient details to automatically identify or permit the automatical identification of persons, but other technology may do so (in the future).[56] The same applies to the storage of biometric information, for example in databases, which – as some argue - does not at first sight or with reasonable means permit the identification of the data subjects, but may do later.

Finally, if the *purpose* of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means likely reasonably to be used to identify the data subject. The Article 29 Data Protection Working Party stated that 'in fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms'.[57] This clarification is for the processing of biometric data applicable and useful, but also raises questions. While biometrics can be used for identification, it can also be used for the verification of the identity. In the latter case, the identity will not always be established by the system in the sense of providing name etc. of the data subject, but it will be checked whether it is the same person or one of the group of persons that are authorized, for example to enter a

[53] WP 29 Working document on biometrics, p. 5. About this important opinion, see also below, section 2.5.1.
[54] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, 26 p. ('WP 29 Opinion on personal data').
[55] WP 29 Opinion personal data, p. 15.
[56] See also *Progress report*, Council of Europe, § 103.
[57] *Ibid.*, p. 16.

place, and as such - one could argue - the individuals are not identified. However, in view of existing and future technology, we esteem that it will remain possible to identify the individuals in this case, even if the biometrics would be locally stored, and hence, that the Directive 95/46/EC applies.

*The provisions of Directive 95/46/EC and the processing of biometric data*

The application of the provisions of the Directive 95/46/EC, which does not explicitly mention biometrics, raises various questions. Some of these questions and uncertainties are hereunder briefly described.

*- Obligation to process data fairly and lawfully (Art. 5 and Art. 6.1.a)*

The Directive 95/46/EC requires that Member States shall state that personal data must be processed 'fairly and lawfully'. The national laws that implement the Directive repeat mostly this general principle. This principle is because of its general wording apt to cope with a variety of situations. Judges will decide upon a case by case basis whether the processing of personal data is 'fairly and lawfully'.

On the other hand, the principle remains vague and gives little guidance when and how data, in our case biometric data, are processed fairly and lawfully. The Article 29 Data Protection Working Party applies the principle in the WP 29 Working document on biometrics in connection with the *collection* of biometric data (only) and states that the data subject shall be *informed* of the purposes and the identity of the controller. However, this requirement to inform is always applicable to any data processing and does not add much to fair processing.

The observation in the second paragraph on the same issue in the WP 29 Working document on biometrics however clarifies what the Article 29 Data Protection Working Party probably intends to communicate and is more significant: it is stated that *the collection of data without the knowledge of data subjects must be avoided*. In fact, several biometric data can be collected and processed without the knowledge of the person concerned, such as facial images for facial recognition, fingerprint and voice (and DNA). Such data processing present more risks, according to the Article 29 Data Protection Working Party. Does this comment of the WP 29 Data Protection Working Party mean that such data processing of facial images, fingerprint or voice is *not* allowed? Or does it mean that such processing shall only be *limited* and subject to *specific requirements* in order to be fairly and lawfully, while the processing of other biometric characteristics, such as for example hand veins, will be less restricted? In the absence of clear legislation on this issue, this remains uncertain.

Very few countries have enacted general legislation regulating the processing of biometric data. Some countries have (more recently) enacted legislation regulating the use of camera surveillance. Article 5 of the Directive 95/46/EC states as a general rule that Member States shall determine 'more precisely the conditions under which the processing of personal data is lawful'. In the absence of such legislation and conditions laid down therein for biometric systems, which exist in a large variety and modalities, this principle of 'fair and lawful' processing remains for biometric systems therefore vague and in our view difficult to enforce.[58]

[58] See, as an example of legislation which attempts to lay down (some limited) conditions for the lawful use of biometric data, the VIS Regulation (EC) N° 767/2008 (see *below*) which refers to lawful processing '*in particular that only duly authorized staff have access to the data processed in the VIS for the performance of*

It is of particular interest for all citizens that biometric data such as facial images are not collected secretly (for example in public places). However, to the extent that such processing would be done for the prevention of crimes or in the case of activities of the State in criminal matters, this principle of fair and lawful processing of the Directive 95/46/EC would not apply because the Directive would not be applicable. Note that this principle of 'fairful processing', however, has been chosen to be repeated in Article 8 of the EU Charter. Article 8 of the EU Charter could in such situations where the Directive 95/46/EC would not apply, such as in case of processing for prevention of crime, hence have a more significant role.

- *Purpose specification and limitation (Art. 6.1.b)*

Article 6 1 (b) of the Directive 95/46/EC requires that biometric data must be collected for specified, explicit and legitimate purposes and shall not be processed in a way incompatible with those purposes. The Article 29 Data Protection Working Party links this principle of purpose specification to the proportionality principle in the WP 29 Working document on biometrics. Although both principles are connected (because the proportionality will have to measure the means used in relation with the purposes envisaged), they are very different and deserve a distinct review.

The purpose limitation principle aims at setting the limits within which personal data may be processed. It also determines how and to what extent data collected for one purpose may be used for other purposes.

The purposes of biometric systems are often indicated in a general way, such as 'for security of access control'. Biometric systems, however, can be used in either the verification or identification mode, which are two very different functionalities[59] with different risks. The specification of the functionality which will be applied (identification or verification), the information as to whether the data will be stored in a central database or not and information about the related risks is in fact therefore necessary in order to duly specify the purposes.

The specification of the purpose of 'increasing security' will not adequately reflect the purpose of a biometric system in operation. The error rates, such as the FRR and the FAR can be set by the controller/operator according to the purpose of the system. For commercial viable systems, these rates are often set for a fluent use. Such adapted error rates however could (invisibly) decrease the security which one would expect from a biometric system. A general purpose specification is therefore misleading without specification of the effects of the tuned FRR and FAR.

The purpose specification and limitation principle of the Directive 95/46/EC in fact implies for biometric systems that due information is provided about these error rates and their effects.

- *Obligation to process personal data which are adequate, relevant and not excessive in relation to the purposes*

The Directive 95/46/EC does not provide any guidance as to which (biometric) data could be considered adequate, relevant and not excessive for a given application.

---

*their tasks in accordance with this Regulation*' (Article 29). Compare also with legislation enacted in several member states relating to camera surveillance.

[59] See E. Kindt and L. Müller (eds.), *o.c.,* p. 11 *et seq.*

*- Obligation to process data on a legitimate ground (Art. 7)*

The Court of Justice has recently clarified its position in a particular case upon request for preliminary questions by the Higher Administrative Court for the *Land* North-Rhine Westphalia (*Oberverwaltungsgericht für das Land Nordrhein-Westfalen*)[60] before which proceedings were brought.[61] The German court asked the Court of Justice whether the processing of personal data of the kind undertaken in the centralised register is compatible with Community law. On the 16th December 2008, the European Court of Justice rendered a judgment in the Case C-524/06 *Heinz Huber* v *Germany*.[62]

The Court of Justice held, first of all, that the data in question constitute personal data within the meaning of the Directive 95/46/EC. The Directive provides that such data may lawfully be processed only if it is necessary to do so for the *performance of a task carried out in the public interest* or in *the exercise of official authority*. The Court noted also that the right of residence of a Union citizen in a Member State of which he is not a national is not unconditional but may be subject to limitations. Thus, it is, in principle, legitimate for a Member State to have relevant particulars and documents relating to foreign nationals available to it and to use a register for the purpose of providing support to the authorities responsible for the application of the legislation relating to the right of residence, provided that there is compliance with the requirement of necessity laid down by the Directive. The Court concluded that such a system for processing personal data complies with Community law *if it contains only the data which are necessary for the application by those authorities of that legislation* and *if its centralised nature enables that legislation to be more effectively applied* as regards the right of residence of Union citizens who are not nationals of that State.

As regards the storage and processing of those data for statistical purposes, the Court then observed that Community law does not exclude the power of Member States to adopt measures enabling the national authorities to have an exact knowledge of population movements affecting their territory. Those statistics presuppose that certain information will be collected by those States. However, the exercise of that power does not, of itself, mean that the collection and storage of individualised personal information of the kind undertaken in the register at issue is, of itself, necessary. Consequently, the Court decided that such processing of personal data *does not satisfy the requirement of necessity* laid down by the Directive**.**

Finally, as regards the question of the use of the data contained in the register for the purposes of fighting crime, the Court held that that objective involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators. The register at issue does not contain personal data relating to nationals of the Member State concerned. Consequently, use for the purposes of fighting crime is contrary to the principle of non-discrimination and hence contrary to Community law.

---

[60] http://www.ovg.nrw.de/presse/index.php

[61] The facts of the case were as follows : Mr Huber, an Austrian national, moved to Germany in 1996 in order to carry on business there as a self-employed insurance agent. On account of the fact that similar information on German nationals was not kept, Mr Huber requested deletion of the information. His request was refused and he filed a claim for discrimination.

[62] *O.J.* C 44 21.2.2009: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:044:0005:0005:EN:PDF ; see als ECJ Press Release 90/08: http://www.statewatch.org/news/2008/dec/ecj-databases-huber=prel.pdf

This ruling has hence clarified two points: (1) a centralised register of foreign nationals may contain only those data which are strictly necessary for the application of the rules relating to the right of residence; and (2) the processing and storage of those data relating to EU citizens for statistical purposes or with a view to fighting crime is contrary to Community law.[63]

*- Obligation to process accurate data, kept up to date (data quality) (Art. 6.1.d)*

Because of the various error rates, including the fact that a biometric comparison is a calculation of a probability, the processing of biometric data and the resulting decisions are never 100 % accurate.[64] This is even more problematic for the possible use of biometric information as an identification key.[65] In addition, factors such as age, but also light conditions will not only influence the accuracy of the processing, but also the resulting scores, decisions and records. In the case of false rejection, the system will for example produce a record showing that a person intended to access a secured area, while this person may have such rights. In general, the scores of biometric systems intended to be deployed, are sometimes not satisfactory.[66]

Therefore, the use and processing of biometric data present a problem under the present principle of data quality as formulated in the Directive 95/46/EC.

The Directive does not provide an adequate answer in this respect.

*- Prohibition of processing of data revealing racial or ethnic origin and of data concerning health (Art. 8.1)*

Fidis deliverables 3.2 and even more 3.10 have described the additional information that biometric '*raw data*' may contain, specifically concerning health.[67] But 'raw data', such as face images, could in some cases also reveal racial or ethnic origin. In addition, very little research has been made as to what extent *templates* may contain similar information while in some cases, it is likely that templates may also contain such information (e.g., in case of deformation of the face due to a stroke or deformation of a hand due to arthritis). Directive 95/46/EC states clearly that the processing of personal data revealing racial or ethnic origin, and of data concerning health shall be prohibited by the Member States (Article 8). Only in exceptional cases, such as if the processing of such data is *necessary* under employment law or for the protection of vital interests, or if the data subject has given *explicit consent*, or *by law* or *decision* of the supervisory authority '*for reasons of substantial public interest*', such prohibition may be lifted.

---

[63] ECJ Press Release 90/08: http://www.statewatch.org/news/2008/dec/ecj-databases-huber=prel.pdf

[64] For a detailed analysis of the various error scores and their meaning, see E. Kindt and L. Müller (eds.), *o.c.*, p. 26 *et seq.*

[65] See also EDPS, Comments on the Communication of the Commission on interoperability of European databases, Brussels, 10 March 2006, 3, available on http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

[66] See the study of the United Kingdom Passport Service, *Report of Biometrics Enrolment Trial*, May 2005, pp. 8 and 9, available on http://dematerialisedid.com/PDFs/UKPSBiometrics_Enrolment_Trial_Report.pdf. In this report, the results of the trial (for finger, one out of five false rejections and for face, one out of three) were far below the expectations on the basis of previous lab testing; See also the test end of 2006-early 2007 in Germany by the *Bundeskriminalamt* which showed that in a real life environment (in a train station), face recognition at a *FAR* of 0,1 % could only successfully recognize about 60 % at day light conditions, while only 10 up to 20 % at night : Bundeskriminalamt, *Forschungsprojekt. Gesichtserkennung als Fahndungshilfsmittel. Foto-Fahndung. Abschlussbericht*, February 2007, 5 and 27.

[67] E. Kindt and L. Müller (eds.), *o.c.*, p. 83 *et seq.*

This prohibition under the Directive 95/46/EC is too easily disregarded. *All* biometric systems capture during the enrolment process (but also during the comparison phase) raw data from the data subjects for feature extraction and further processing, even if such systems would only store the templates. Because biometric systems capture *always* first 'raw data' which may contain information revealing racial or ethnic origin, or revealing the health condition, which are further processed in one way or another, additional legal safeguards should protect the legitimate interests of the data subject, for example by explicitly prohibiting any use of such additional information deduced from biometric data (whether 'raw data' or templates). The general prohibition in the Directive 95/46/EC and the exceptions thereto (for example, the consent of the data subject, which is often not explicit or not valid in view of the proportionality principle) is not fit for biometric systems and in many cases even not complied with.

The specific characteristics and risks of the biometric process for the processing of these so-called 'sensitive data' needs to be taken fully into account in the legislation in order to provide appropriate safeguards for the individuals.

> *- Right of data subject to obtain communication in an intelligible form of the data undergoing processing and knowledge of the logic involved in any automatic processing at least in case of automated decision (Art.12 a)*

Biometric systems are complex to understand. The processing of biometric data involves transformations of the data, various parameters, scores, algorithms and results, and in some cases automated decisions (see *hereunder)*. Data subjects are rarely informed of all these processes and of the data processed (raw data versus templates) and receive no insight in the logic of the automated decisions. The Directive 95/46/EC states that Member States shall guarantee these rights. So far, there is to our knowledge no specific national legislation which guarantees and enforces such rights upon data controllers.

*The provisions of Directive 95/46/EC do not provide a global international legal framework*

It shall also be noted that the Directive 95/46/EC does not provide data protection rules for data processing outside the EU (and the EEA). It does not provide for a legal framework for processing of data exchanged between players situated in various countries around the globe.

This poses problems for systems which are controlled by multilateral parties, in particular biometric multilateral controlled systems. [68]

Another problem is where EU citizens carry biometric enhanced documents, such as travel documents, where the biometrics can be read and used in third countries (for example, by the immigration services).

The Directive only states that the transfer of personal data to countries which do not provide for an adequate level of protection is in principle prohibited (Art. 25). Various exceptions apply, such as transfer with the unambiguous consent of the data subject or the necessity of the transfer for the performance of a contract (e.g., for a hotel reservation). A transfer could also be authorized under the 'safe harbor' system or by the DPAs involved if adequate safeguards result from appropriate contractual clauses.

[68] E. Kindt and L. Müller (eds.), *o.c.*, p. 59 *et seq.*

However, these provisions of the Directive 95/46/EC only restrict or regulate the transfer and do not provide, for example for biometrics, for a global legal framework.

## 2.4 The Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters

The Framework Decision on the protection of personal data in the field of police and judicial cooperation in criminal matters is the first general data protection instrument in the EU third pillar.[69] Since various data processing in this third pillar (i.e., Justice and Home Affairs (JHA)) include biometric data, this Framework Decision is herein briefly discussed.

In a reaction to its adoption, the EDPS reminded the EU Institutions that it had repeatedly called for significant improvements of the proposal to ensure high standards in the level of protection offered and warned against a dilution of data protection standards.[70] The current decision was not amended to meet the criticisms of the EDPS. The EDPS reiterated its position that besides the inclusion of domestic data in the scope of the decision,

> 'further work was needed with regard to the following main points:
>
> • the need to distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards;
> • ensuring an adequate level of protection for exchanges with third countries according to a common EU standard;
> • providing consistency with the first pillar's Data protection Directive 95/46/EC, in particular by limiting the purposes for which personal data may be further processed.'[71]

This Framework Decision is further in general criticized as that it regulates mainly the transmission and exchange of data between Member States and competent authorities/systems in the framework of police and judicial cooperation in criminal matters and not the data processing in the third pillar by the Member States as such.

Furthermore, rules and guidelines have been issued that specifically relate to the processing of personal data for law enforcement purposes. These include, in particular, Council of Europe (CoE) Recommendation R(87)15 Regulating the Use of Personal Data in the Police Sector (1987) of the Committee of Ministers to Member States.[72] This Recommendation has become the effective standard on the issue: it is expressly referred to in various European police co-operation instruments, including the Schengen and Europol treaties and associated

---

[69] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ* L 350, 30.12.2008.

[70] European Data Protection Supervisor, *EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step*, available at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-11_DPFD_EN.pdf>, last consulted 11 March 2009. p. 1.

[71] *Ibid.*, p. 1. The application to domestic data and the need to distinguish between data subjects are issues that potentially affect the UK more than other EU states because the UK is one of the member states with the largest biometric (including DNA) databases.

[72] Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector, available at http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf , last consulted 11 March 2009.

regulations, and is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, as well as by the European Parliament.
The following broad guidelines can be derived from the judgments of the European Court of Human Rights, and are reflected in the case-law of the European Court of Justice, and in Recommendation R(87)15 :

> '1. There must be a legal basis for any collection, storing, use, analysis, disclosure/sharing of personal data for law enforcement and anti-terrorist purposes. A vague, broad general statutory basis is not sufficient; rather:
> 2. Such processing must be based on specific legal rules relating to the particular kind of processing operation in question; these rules must be binding, and they must lay down appropriate limits on the statutory powers such as:
> - a precise description of the kind of information that may be recorded;
> - a precise description of the categories of people against whom surveillance measures such as gathering and keeping information may be taken;
> - a precise description of the circumstances in which such measures may be taken;
> - a clearly set out procedure to be followed for the authorisation of such measures;
> - limits on the storing of old information and on the time for which new information can be retained;
> - explicit, detailed provisions concerning:
>
> the grounds on which files can be opened;
> the procedure to be followed [for opening or accessing the files];
> the persons authorised to consult the files;
> the nature of the files;
> the use that may be made of the information in the files.
>
> It follows from the above:
> (1) that the collection of data on "contacts and associates" (i.e. on persons not suspected of involvement in a specific crime or of posing a threat), the collection of information through intrusive, secret means (telephone tapping and email interception etc.; "bugging"; informers; agents), and the use of "profiling" techniques, and indeed "preventive" policing generally, must be subject to a particularly strict "necessity" and "proportionality" test (.....);
> (2) that "hard" (factual) and "soft" (intelligence) data should be clearly distinguished; and that data on different categories of data subjects (officially indicted persons, suspects, associates, incidental contacts, witnesses and victims, etc.) should likewise be clearly distinguished;
> (3) that the nature of information and intelligence coming from private parties such as businesses or credit reference agencies requires additional safeguards, *inter alia* in order to ensure the accuracy of this information since these are personal data that have been collected for commercial purposes in a commercial environment; and
> (4) that access should only be allowed on a case-by-case basis, for specified purposes and under judicial control in the Member States.
> 3. Such rules can be set out in subsidiary rules or regulations - but in order to qualify as "law" in Convention terms, they must be published.'[73]

These principles also apply to the processing of biometric data.

[73] As quoted from the Commissioner for Human Rights, *Protecting the right to privacy in the fight against terrorism*, available at https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679, last consulted 11 March 2009.

## 2.5 A selective overview of opinions of the Article 29 Working Party and the EDPS on biometrics

In this section, some selected opinions of the Article 29 Working Party and the EDPS on biometrics are discussed. It should be noted that because of the growing complexity of the privacy and data protection issues, especially in recently set up large scale EU systems, also a special Working Party on Police and Justice ('WPPJ') was mandated by the European conference of the DPAs to follow up on the privacy and data protection issues of specific EU wide databases and to provide advice in this regard. The WPPJ started its activities in June 2007.[74]

### 2.5.1 Opinions and comments on the processing of biometrics in general

In 2003, the Article 29 Data Protection Working Party issued an opinion on biometrics because of the 'rapid progress of biometric technologies and their expanded application in recent years' to contribute to the effective and homogenous application of the data protection legislation.[75] One of the major concerns expressed by the Article 29 Data Protection Working Party is, after collection and processing of biometric data for routine applications, their fear of the *potential re-use* by third parties for their own purposes, *including by law enforcement* agencies. One aspect of its fear is also that the public may become desensitised to the effect that the processing of biometric data may have on their daily lives, especially when biometric data are collected from young children.

The WP 29 Working Document on Biometrics of 2003 focuses on biometric systems used for authentication and verification purposes and contains a clarification of the general principles of the Directive 95/46/EC and its application to the processing of biometric data.[76] The opinion, although not clearly stated, is also restricted to use of systems for other than law enforcement or border control purposes. The Article 29 Data Protection Working Party first points briefly in the more technical description of biometric systems *to the problem of collection of so called 'sensitive' data* and *the risk of collection of some biometric characteristics without the knowledge of the individual* involved. Thereafter, it stresses that a clear determination of the purpose shall be made.

In view of the proportionality principle, the Article 29 Data Protection Working Party recommends that (1) characteristics that *do not leave traces shall be used,* or (2) if such other characteristics are used (such as fingerprint), they *should be stored on an object* exclusively available to the user, and that (3) proportionality has to be in general assessed for each category of biometric data in relation with the intended purposes.

If local storage of characteristics which leave traces would not be possible, the Article 29 Data Protection Working Party hints to the possibility that Member States would provide in their *national law* for the requirement of *prior checking* with the data protection authorities before one could start such processing. It further states that 'all measures must be taken to

---

[74] See Working Party on Police and Justice, *Activity Report 2007-2008,* available at http://www.privacycommission.be/nl/static/pdf/working-party-on-police-and-justice-ar-nl.pdf

[75] WP 29 Working Document on Biometrics, 11 p.

[76] These guidelines and the principles, such as fair collection, information to the data subject, security of the processing, etc have been described in earlier Fidis work in M. Gasson, M Meints, *et al.* (eds.), *o.c.,* p. 102 *et seq.*. These will therefore not be repeated here. We herein limit our analysis to some positions which the Article 29 Data Protection Working Party takes for specific problems.

prevent […] incompatible re-use' and implicitly states that *local storage* could maybe solve this problem as well, while this could also solve the risk of the use of biometric data as a key (or identifier of general application) for interconnecting databases.

'*Mathematical manipulations*' are also mentioned as desirable in the case of central storage, to avoid that biometrics are used as a key, *in addition to legislation* as to the conditions of such processing by the Member States.[77] As a conclusion, the importance for *the data subject to exercise better control* over its personal data is stressed.

The Article 29 Data Protection Working Party also briefly mentions the possibility to use biometrics as a privacy enhancing technology (hereafter 'PET').[78] Biometrics is here mentioned as a way to reduce the need for the processing of other personal data, such as name or address. In addition, the use of PETs in general is reminded as a way to minimise data collection and to prevent unlawful processing. How this has to be done in case of biometric data processing, is not clarified.

The opinion, although legally not binding, is an important document as it provides some keys in the complex discussion about biometrics. It gives some insights in how national data protection authorities may look at the issues (for example, as to their preference for characteristics which leave no traces). In opinions of DPAs, a similar point of view as set out in this WP 29 Working Document on Biometrics is sometimes repeated.

In the context of biometrics, the *interoperability* of the systems is also received attention as one major concern.[79] The EDPS has in his comments on the Commissions' Communication on interoperability of European databases expressed his concern in this regard. The EDPS stated that 'making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for the facto acceding or exchanging these data'.[80] This fear only is reinforced with the pronouncement of the principle of availability proclaimed in the The Hague Programme and since then adopted.[81]

Finally, another interesting opinion of the Article 29 Data Protection Working Party is the opinion on the Green Paper on Detection Technologies.[82] Although the opinion does not specify (yet) concrete guidelines on *detection technologies*, biometrics is mentioned several

---

[77] See section 3.8 of the WP 29 Working Document on Biometrics.

[78] This point has been referred too many times and interpreted in various ways. The use of biometrics as a PET has been sometimes described as a way to control and limit access to persons to data in large systems by controlling who they are. The Article 29 Data Protection Working Party separately mentions also the possibility to use biometrics as encryption keys.

[79] See also P. De Hert and A. Sprokkereef, 'Regulation for biometrics as a primary key for interoperability ?' in earlier Fidis work, in particular E. Kindt and L. Müller (eds.), *o.c.*, section 3.2.3. pp. 47 -55.

[80] EDPS, Comments on the Communication of the Commission on interoperability of European databases, Brussels, 10 March 2006, 2, available on http://www.edps.europa.eu/EDPSWEB/_webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

[81] The principle of availability was elaborated in the aftermath of 11 September 2001. The principle of availability is aimed at allowing national law enforcement agencies within the EU full access to all the data in national and European databases. The principle was embedded in the so-called the Hague Programme. The 'The Hague Programme' also introduced the idea of the use of biometric identifiers for passports and of a visa information system. As part of anti-terrorist measures, the Commission emphasised the need of improving exchanging information as means for strengthening the cooperation between law enforcement services. About the The Hague Programme, see also section 6.1.

[82] The Article 29 Data Protection Working Party, Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities, available on http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp129_en.pdf

times as an example of a detection technology (together with CCTV and RFID tags) for which appropriate data protection solutions need to be found.[83] It is stressed that a *clear determination of the purposes* of the data processing is a key issue. Only then, data protection authorities are able to determine whether the collected data are adequate, relevant and not excessive.

### 2.5.2 The use of biometrics in specific large scale systems in the EU

*Biometric identifiers in epassports and travel documents*

The legal basis for the inclusion of biometric identifiers in passports and travel documents of EU nationals is the Council Regulation 2252/2004/EC.[84] The biometric features in the passports shall only be used for the verification of the authenticity of the document and the identity of the holder when the document has to be produced by law (Article 4, 3). At the time of the Regulation, the new technologies of inserting chips with biometric data, however, had not yet been applied or tried out.

In the meantime, there is a proposal for amending the Regulation (EC) 2252/2004.[85] Insufficient quality of fingerprint in some situations for one-to-one verification made the proposed amendments necessary. The proposal is complementing the Regulation and aims at defining harmonised exceptions: children under 6 years and certain persons who are physically unable to provide fingerprints for travel documents are exempt from the requirement to provide fingerprints. The proposal also introduces the principle of 'one passport-one person' as an additional security measure, recommended by the International Civil Aviation Organisation (ICAO). This would ensure that the passport and the biometric features are only linked to the person holding the passport and could help combat child trafficking by requiring children to have their own passport with their own biometric identifiers. Finally, some minimum technical security measures are imposed set out in the Annex.

The EDPS stated in his opinion of 2008 on this proposed amendment that while the introduction of these exemptions were welcomed, these exemptions remain unsatisfactory, because they *fail to address all the possible issues* relevant to the inherent imperfections of biometric systems.[86] Furthermore, the EDPS stated that the Commission should also propose further *harmonization measures in order to implement only the decentralized storage* of biometric data for the Member States' passports and that the Commission should *propose common rates* for the enrolment and matching process completed by fallback procedures.

---

[83] *Ibid.*, 4.

[84] Council Regulation No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 385, 29 December 2004, p.1 ('Regulation (EC) 2252/2004'). This Regulation has been extensively discussed and analysed in earlier Fidis work, in particular M. Meints and M. Hansen (eds.), *o.c.*, p. 49 *et seq.*

[85] Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, COM (2007) 619 final, 18 October 2007, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0619:FIN:EN:PDF

[86] Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, *O.J.* C 200, 6 August 2008, p.1, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:200:0001:0005:EN:PDF

In a resolution of 14 January 2009, the European Parliament has adopted the proposal, as amended (including raising the age from six to twelve).[87]

*VIS*

In June 2004, the Council of Ministers of the EU decided to establish a Visa Information System (VIS).[88] The VIS system is an information system intended, according to the Decision of 2004, to enable national authorities to enter and update visa data of third country nationals and to consult these data electronically (Article 1). Measures necessary for the development of VIS were to be adopted, including the '*development of security measures, including biometrics*' (Article 4). The Decision needed further implementation at the EU and national level. Regulation N° 767/2008 of 9 July 2008 provides for such further implementation (VIS Regulation').[89]

The VIS system aims at providing border guards all necessary information to verify whether the entry conditions for third country nationals are fulfilled at the external borders.[90] Personal data of third country nationals to be recorded in the central database of VIS include not only a list of alphanumeric data, such as surname and first name, but also photographs and fingerprint data (Article 5 1. (a), (b) (c) of the VIS Regulation).

According to the VIS Regulation, competent authorities (at the borders and within the national territory) have access to a search facility using the number of the visa sticker in combination with the verification of fingerprints of the visa holder (which will be stored in the VIS central database (and not in the visa sticker)) for purposes of *verifying the identity* of the visa holder and/or the authenticity of the visa and/or as to whether the conditions for entering the Schengen area or the stay on the territory are fulfilled (Article 18 and 19). Access for *identification purposes* is also regulated (Article 20), as well as access for determining responsibility for asylum applications (Article 21).

The Article 29 Data Protection Working Party expressed already in August 2004 as one of its major concerns, the *storage of biometric data in a central database* for the purpose of carrying out subsequent checks with regard to proportionality. It referred also to the risks for

---

[87] See http://www.europarl.europa.eu/sides/getDoc.do;jsessionid=E97F79F84DA75D9ABD3654A8B43D23B5.node2?pubRef=-//EP//TEXT+TA+P6-TA-2009-0015+0+DOC+XML+V0//EN

[88] Council Decision of 8 June 2004 establishing the Visa Information System (VIS), 2004/512/EC, *O.J.* L 213, 15 June 2004, pp. 5-7. The Council provided hereby the legal basis for the invitations for tenders for this system which were already under way and for the inclusion in the general budget of the EU. This decision was taken after a so-called 'extended impact assessment' submitted by the Commission to the public. See European Commission, JHA, *Your views on the future EU Visa Information System (VIS)*, available at http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_vis_en.htm This public consultation was decided by the Commission in its Annual Work Programme 2004. See also about impact assessment in general, COM(2002) 276 of 5 June 2002.

[89] Regulation (EC) N° 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, *O.J.* L 218, 13 August 2008, p. 60 ('VIS Regulation'). About the draft of the Regulation, see M. Meints and M. Hansen (eds.), *o.c.*, p. 45 *et seq.*

[90] VIS should hence improve the implementation of the common visa policy of the European Union. One should note that the recitals to the Decision mention the option of a common technical platform with the second generation Schengen Information System (SIS II, see *below*) (recital 2).

the persons concerned in case of a *hijacked identity* and the *problem* of such large-scale database *of the reliability* of checks.[91] The Article 29 Data Protection Working Party questioned what *studies revealed compelling reasons of public safety or public order* that would justify such central storage, and whether alternative approaches which do not involve such risks have been studied.[92]

The Article 29 Data Protection Working Party repeated this concern in its opinion in 2005 relating to VIS and the exchange of data.[93] It stated that an 'assessment of the principle of *proportionality* (…) therefore begs the *question of the fundamental legitimacy* of collecting these data (...). (…) An extremely careful *analysis of the lawfulness* of the processing of such data *for identification purposes* is necessary, given the possible prejudicial effects to the persons concerned if they are lost or used for purposes other than those for which they were intended' (stress added).

The EDPS, requested to issue an opinion on a proposal concerning access for consultation of VIS, warned in 2005 that while VIS is an information system developed for the *European visa policy* and *not as a law enforcement tool*, routine access by law enforcement authorities would not be in accordance with this purpose. Only access on a case by case basis, under strict safeguards, shall be granted, provided the consultation will 'substantially contribute' to the prevention, detection or investigation of a serious crime.[94]

The VIS Regulation has to some extent taken the remarks and comments of the Article 29 Data Protection Working Party and the EDPS into account.[95] However, this did not prevent that, notwithstanding the original purpose of VIS, by decision of the Council of 23 June 2008, designated authorities of Member States and Europol have obtained access to VIS for purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

It is remarkable that a new Regulation (EC) N°81/2009 of 14 January 2009 already provides a derogation to the use of the biometric data in the central database when the waiting lines are too long. It is stated that '*where traffic of such intensity arises that the waiting time at the border crossing point becomes excessive, all staff and facilities resources have been exhausted and based on an assessment there is no risk* related to internal security and illegal immigration', *VIS may be consulted using the visa sticker number only, leaving out the*

---

[91] Article 29 Data Protection Working Party, *Opinion N° 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*, WP 96, 11 August 2004, pp. 4-5.
[92] *Ibid.*, p. 5.
[93] Article 29 Data Protection Working Party, *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*, WP 110, 23 June 2005, p. 12.
[94] EDPS, *Opinion on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences*, *O.J.* C97, 25 April 2006, p. 6.
[95] See, for example, Article 3 which confers access for investigation of terrorist offences and other serious criminal offences '*if there are reasonable grounds to consider that consultation (…) will substantially contribute'*. The VIS Regulation, for example, also makes a distinction between the use of the biometric data for verification and identification purposes, and restricts the access to the data.

*verification of fingerprints* (Article 1,1(ab)) (stress added)'.[96] It may be feared that such kind of provision could lead to the arbitrary use of the biometric data in VIS.

*The second generation Schengen Information System (SIS II)*

On 31 May 2005, the European Commission made proposals for replacing the original Schengen Information System ('SIS'), which was a system at both central (C-SIS) and national (N-SIS) level for allowing access to alerts on persons and property for the purposes of border checks and other police and customs checks, as detailed in Title VI of the Schengen Convention (later incorporated in the EU Treaty), by a *fully central* system with *centralised database* with new categories of data, in particular photographs (in the form of digital images) and fingerprints alongside an alert, for the broad purpose of 'exchanging information for the control of persons and objects' (Article 1).[97] Regulation (EC) N° 1987/2006 of 20 December 2006 has adopted the proposal for SIS II.[98]

The Article 29 Data Protection Working Party deplores in its opinion of November 2005 that 'without any proper assessment of the necessity' for such new categories of data, the biometric data will be added to the system. The Article 29 Data Protection Working Party also points out that no clarification is given about the *enrolment procedure* for the biometric data, the *rules for access* and the specific *security measures* to be introduced.[99] Because of the sensitivity of the data, which fall within the scope of article 6 of the Convention No 108, the Article 29 Data Protection Working Party states that the data should be safeguarded by adequate standards at international levels and that *search functions based on these data should be ruled out*.[100] It concludes by repeating that the use of biometrics for identification purposes must be strictly limited to specific cases where this information is really necessary, including in the interests of the data subject, and that the circumstances and purposes for biometric searches shall be defined, as well as appropriate guarantees by law in order to limit or reduce function creep.[101]

---

[96] Regulation (EC) N°81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) N° 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Border Code, *O.J.* L 35, 4 February 2009, p. 56 - 58.

[97] Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II), COM(2005) 236 final.

[98] Regulation (EC) N° 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *O.J.*L 381, 28 December 2006, p. 4 ('SIS II Regulation'). In addition, access by services for issuing vehicle registration certificates to SIS II is also regulated by Regulation (EC) N° 1986/2006 of the European Parliament and of the Council of 20 December 2006, *O.J.* L 381, 28 December 2006, p. 1-3 ; See also Regulation (EC) N° 562/2006 of 15 March 2006 established a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code) and lays down the detailed rules on border crossing checks, including checks in the Schengen Information System.

[99] The Article 29 Data Protection Working Party, *Opinion 6/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM(2005) 236 final) and a Council Decision (COM(2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)*, WP 116, 25 November 2005, p. 15.

[100] *Ibid.*, p.15.

[101] *Ibid.*, p.23.

The EDPS proposed in his opinion on SIS II a non exhaustive list of common obligations and requirements which need to be respected when biometric data are used in a system, in order to avoid that the data subject is to carry the burden of system imperfections.[102]

The status of SIS II is for the moment however somewhat unclear, as some say it is delayed.

*Eurodac*

EURODAC is an EU wide database with *centrally* stored biometric data and which allows checking asylum applicants on double requests.[103] Eurodac is operational.

The Working Party on Police and Justice (WPPJ) stated in a position on a proposal for access by law enforcement agencies to the Eurodac data, to assess first the necessity of such new item of legislation. In their view, Eurodac is set up in the frame of evaluating asylum applications and cannot be seen as 'an ordinary fingerprint database' which can be used for other purposes.[104] WPPJ estimates that there is no pressing need to take the risk of turning the Eurodac data base into a criminal law investigation tool.

*European Border Surveillance System and Frontex*

The EU Commission started in 2008 a discussion on the next steps on border management, the creation of an European Border Surveillance System and the evaluation of Frontex.[105]

The Article 29 Working Party, together with the WPPJ declared in 2008 that they make serious reservations as to the necessity and the proportionality of the proposals for the set up of the European Border Surveillance System and Frontex. They stated in a declaration that they regret that it is not evaluated first whether existing legal measures are properly implemented and proved to be inefficient which is needed to motivate the need for new systems. The inclusion of biometric data increases those risks. The WPPJ hereby underlined that '*not everything that is technically feasible is also ethically acceptable or legally permissible*' (stress added).[106]

## 2.6 The role of the National Data Protection Authorities

The National Data Protection Authorities ('DPAs') are in principle *independent* public authorities established in each of the Member States which are responsible for the *development* of relevant guidelines, the *monitoring* of the application of the data protection legislation and, if necessary, for its *enforcement*.

The Directive 95/46/EC sets out in detail which powers shall be conferred by the legislator to the national DPAs (Article 28). The implementing national legislation shall observe that their national DPA shall as a minimum have the powers described in Article 28. These powers

---

[102] EDPS, Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II).
[103] Eurodac has also been analysed in M. Meints and M. Hansen (eds.), *o.c.*, p. 41 *et seq.*
[104] WPPJ, *o.c.*, p. 5-6.
[105] See COM (2008) 69 final, COM (2008) 68 final,and COM (2008) 67 final.
[106] Declaration adopted on the Spring Conference of European Data Protection Authorities, Rome, 17-18 April 2008, available at http://www.ip-rs.si/index.php?id=272&tx_ttnews%5Btt_news%5D=367.

include (i) the obligation to be *consulted* when administrative or legislative measures or regulations are being taken and which affect the right to data protection, (ii) *investigative* powers, including audit and discovery powers on the premises, (iii) rendering *opinions in case of prior checking*, or in case of (iv) ordering the *blocking, erasure or destruction* of data or a (temporary or definitive) *ban* on the processing, (v) imposing (sometimes substantial) *fines* and (vi) power to *engage in legal proceedings* or to *refer cases* to the judicial authorities.

In areas of new technologies, where legislation does not yet take such technologies into account, the DPAs play an important role. For new types of data processing, such as biometrics, the application of the law is not always clear, and the DPAs often provide guidance on the interpretation of the law to biometric applications *in opinions, advice and recommendations*. Although these are in principle not binding, they are of a great authoritative importance since in case of non-compliance, the DPA could use its powers conferred as described above. Some active DPAs further provide *information in various ways* and assist in creating *awareness*, by participating in debates on the use of biometrics, for example in parliament (e.g., the CNIL) or during scientific meetings, and by referring to such new technologies and the questions they may raise in the public (annual) reports they need to provide about their activities.

The DPAs are also involved in *advising on the enactment of national legislation* and the implementation of European legislative initiatives, such as on the use of biometrics in passports and travel documents, in a national context.

The number of processing, new technologies and resulting problems, which require the attention of the national DPAs[107], however, are increasing rapidly. The DPAs have therefore *difficulties in terms of person power and financial means* to fulfil their tasks and responsibilities. Sometimes, the required independence has also been revealed a problem, but is being resolved in some countries.[108]

The DPAs will also hear *complaints* of data subjects or representative organisations. The right to file a claim with the DPA appears very important in case of the use of biometrics in the employment context. Examples of claims brought by employees or labor organisations against the installation of a biometric access control systems can be found in countries such as Greece and Belgium. The decisions of the DPAs, however, can be appealed before the courts.

The national DPAs are only competent to use their (interpretative, investigative and enforcement) powers on their own territory. For biometric systems, implemented in various places, for example of a multinational company, this could lead to different positions and approaches by the DPAs. Nevertheless, national DPAs can ask the DPAs of other countries to *exchange* useful *information* and could even request such other DPAs to exercise their powers (Article 28 (6)).

Representatives of the national DPAs will also participate in *international* initiatives and working groups, in particular the Article 29 Data Protection Working Party. This international cooperation is important for biometrics, since positions of the DPAs are there discussed, information exchanged, which sometimes results in joint declarations. In 2005, the national data protection authorities stressed in a joint resolution made at the occasion of their 27th

[107] For example, the use of RFID technology, of GPS and location data, of electronic surveillance, of camera surveillance and identity systems.

[108] In Belgian, for example, the DPA is no longer within the organisation of the Minister of Justice, but an independent commission receiving its funds from and reporting to the national parliament.

annual conference in Montreux, that the widespread use of biometric data will have a considerable impact on society and called for *effective safeguards* in an early stage in order to limit the risks inherent to biometrics.[109] Most importantly, they also called for a *strict distinction* between biometric data collected and stored for *public purposes* on the basis of *legal obligations* and for *contractual purposes on the basis of consent*. While the resolution was specific on passports, they also called for *technical restrictions* of the use of biometrics therein to verification purposes. The resolution has no binding legal effect. However, it is an important indication of the common view of the national DPAs on the processing of biometric data.

Such international cooperation may have a positive effect on a more common approach of the DPAs towards biometric systems. However, the latter is not yet a fact and DPAs will have their own position towards biometric systems (e.g., in relation to the biometric characteristic to be used or central storage). This creates problems for transnational use and implementation of biometric systems.

## 2.7 Preliminary conclusion

The national Member States are compelled in assuring the fundamental right to privacy and data protection to individuals because these principles are laid down in binding international conventions and national constitutions.

In view of new technologies and data processing, such as the processing of unique human characteristics for the verification or identification of individuals, the application of these fundamental rights is not self-explanatory. The Directive 95/46/EC provides more detailed rules on how to establish a protection in case of personal data processing but seems not apt to cope with all issues and problems raised by biometric applications, as described in section 2.3. Specific legislation could address the risks and problems with biometrics. Alternatively, the existing provisions of the Directive 95/46/EC could be further interpreted by the DPAs.

The limited recent case law of the European Court of Human Rights and the Court of Justice sheds some light on some relevant issues, but does not answer all questions.

The Article 29 Data Protection Working Party and the EDPS clearly point out in their opinions on large scale EU databases that for the processing of biometric data in the proposed specific systems (VIS, SIS II,….) that they have reviewed, and for the processing of biometric data in general, that appropriate legal specifications are lacking, including for the decision about the *proportionality* of the collection and central storage of biometric data, the *data quality (*such as low false rejection rate requirements*)*, the *enrolment procedure*, subsequent *access by law enforcement authorities*, and the *safeguards for the individuals*. These large scale databases also illustrate that the initial objective for establishing a central database (e.g., for VIS, for establishing a common visa policy) is often changed and access is granted for law enforcement purposes (e.g., for VIS, access is granted to for example Europol).[110]

---

[109] The resolution was presented by Germany and was on the use of biometric data in passports, ID cards and travel documents. See 27th International Conference of Data Protection and Privacy Commissioners, *Resolution on the use of biometrics in passports, identity cars and travel documents*, 16 September 2005, available at http://www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf

[110] The same is happening with regard to Eurodac, where developments indicate that the database, initially only for evaluating asylum applications, may be turned into a criminal investigation tool.

The country reports that follow will highlight how delicate questions in relation to biometrics are tackled in the selected countries. DPAs hereby have an important role in the interpretation and enforcement of the existing legislation. It is therefore necessary to review how these national authorities cope with such new technology as biometrics and how each country is in search of a comprehensive approach.

# 3 Belgium

## 3.1 Introduction

Biometric applications are being introduced in an increasing tempo in various domains of public and private life in Belgium. The plan of *schools* to introduce biometrics for access control and administration purposes has retained quite some press and media attention, while the introduction of biometrics on the *work floor* has raised concerns by employee(representative)s. Official *institutions of the EU* have also installed enhanced access control applications, for example the EU parliament based in Brussels which collects and registers detailed pictures of visitors upon entrance of the EU parliament premises. But also *fitness clubs* request members to provide their fingerprint. Besides these trends, more and more *consumer goods* sold in Belgium also include biometric functions, such as laptops.

The introduction and use of biometrics in combination with the national *electronic identity card* was subject of further *scientific research*[111], but research about biometrics was also done in demonstrators and research projects, such as for securing banking applications and networks.[112] The introduction of fingerprints on the epassports is in principle scheduled to start in 2009.

The data protection legislation does not refer explicitly to biometric data. Cases about the use of biometrics are pending before court. The uncertainty about the legal and privacy risks of the use of biometrics have lead to various questions posed to the Belgian Data Protection Authority ('CBPL'). Initially, the CBPL referred to some of these questions in its annual reports only. However, and more importantly, the CBPL issued *upon its own initiative in April 2008 an opinion* on the subject of the processing of biometric data for authentication purposes. This opinion contains the view of the CBPL on various aspects of the processing of biometric data and promulgates several guidelines on the subject matter.[113] This opinion will be further discussed in section 3.4.

In the field of law enforcement, it should be noted that Belgium has signed in 2005 the Prüm Treaty in which signatories agree to share *access to fingerprint* (and motor vehicle registration) databases.

## 3.2 The spreading of biometric applications

### 3.2.1 Fields in which biometric applications are implemented

Various *schools* are introducing biometrics for the administration of their students and for access control, for example to keep undesired persons outside the premises. These schools are located in the French speaking Community[114] (Luik), Brussels or the Flemish speaking

---

[111] See, for example, the research in the IDEM project (an IBBT project 'IDEntity Management for eGovernment') of the Belgian and Flemish government (see https://projects.ibbt.be/idem/index.php?id=126 )

[112] For example, the use of fingerprints of bank employees to secure access to systems.

[113] Commission for the Protection of Privacy, *Opinion upon own initiative concerning the processing of biometric data in the framework of the authentication of persons*, Opinion N° 17/2008 of 9 April 2008, 22 p., available at www.privacycommission.be (in French or Dutch) ('CBPL Opinion on biometrics').

[114] See also a question of a Walloon parliament member to the Education Minister of the Walloon community, Maria Arena of February 6, 2007 as to the use of biometric access control in schools, available at http://www.lecdh.be/docparlement/pa4896.htm . The Minister answered that the data shall not be used outside the school or for purposes other than school objectives.

Community (Mechelen, Opwijk, …).[115] These schools request the consent of parents and sometimes refer to the use of the biometric technology in their internal rules. The purposes for which they use the fingerprint technology include ensuring the security of the students and control of their presence. Sometimes, the use of instantaneous registration of the students is also defended for use in case of evacuation in emergency situations (e.g., a fire). The implementation in schools, however, are sometimes done in the form of a pilot and hence supplier driven. For avoiding the use of the data by police authorities, the school in Luik declared to use only a *part of a fingerprint.*[116]

Biometrics are also being reflected upon and being implemented in the context of *access control of employees*. Because of a complaint of the employee representatives, the CBPL has conducted an investigation on the matter, and, based on its investigation, has considered the use of biometrics as an important new technology, for which it issued guidelines in its opinion of 2008, as mentioned above.

In *public places and closed places* which are *open to the public* (for example shops), camera surveillance has been introduced massively in Belgium. This has even resulted in a new legislation on the use of camera surveillance. A new and more recent trend, however, is to replace the existing camera surveillance systems with *intelligent camera surveillance systems*, which are digital and which can perform additional automated functions. At the Belgian coast, various cameras which allow the recognition of faces, have been installed since 2005.[117] After the successful pilot with 9 cameras, about 60 cameras were planned to be installed in various communes along the Belgian coast. The system was promoted as a system that would allow relocating young children who got lost on the boardwalk or on the beach, by scanning a picture provided by the parents which would be recognized by the system. However, the system would in addition also be used to find criminals.[118] In and around Brussels, a new cooperation amongst various police zones would result in the installation and the operation of new camera surveillance systems and techniques observing the traffic on the belt around Brussels and taking down the license plates of the vehicles, to be compared with those of stolen or uninsured cars. These camera surveillance systems are examples of the use of biometrics as Type V surveillance applications or if they would be used in a specific context by a mix of public and private organisations, of Type III public – private applications.[119]

Biometrics is also increasingly used in *law enforcement* services. Police services are investing in new systems which allow the digital collection of fingerprints of persons who have been arrested.[120] The fingerprints can in such application instantaneously be compared with central

---

[115] See X., Scholen gebruiken vingerafdruk voor leerlingenregistratie', *Maks*, 18 April 2008, available at http://www.maks.be/nieuws.php?id=8439

[116] See S. Danneels, 'Vingerafdrukken garanderen veiligheid in Luikse school', *Niewsblad.be*, 18 April 2008, available at http://www.nieuwsblad.be/Article/Detail.aspx?ArticleID=SA1QVC6H

[117] Y. Naesen, 'Nooit meer verloren kinderen aan de kust', *Nieuwsblad.be*, 26 July 2005, available on http://www.nieuwsblad.be/Article/Detail.aspx?articleID=gktgko78

[118] X., 'Speciale apparatuur in Vlaamse badplaatsen zoekt zelf naar criminelen of vermiste kinderen', Elsevier, available on http://www.elsevier.nl/login/login_preview_e.asp?strretpath=http%3A%2F%2Fwww%2Eelsevier%2Enl%2Fmagazine%2Fartikel%2Easp%3Fartnr%3D60423%26jaargang%3D61%26week%3D33

[119] About these suggested classes of biometric systems, see E. Kindt and L. Müller, (eds.), *D.3.10. Biometrics in identity management* , Fidis, December 2007, p. 60 *et seq.*

[120] See *Questions & Answers* Chamber 2008-09, 16 February 2009, p. 1129 (Question of 2 February 2009 n° 229 Van Biesen): On December 2, 2008, the final approval for the purchase of the AFIS-system was given which shall replace the present 10 year old system. Local Lifescan systems and systems for the electronic sending of 'ink fingerprints' will be connected to the central system; see also X., 'Digitaal vingerafdrukken

databases in Brussels for checks on persons who were arrested before and may have committed crimes. Fingerprints may also be taken from asylum applicants (see *below*). While such prints may in principle not be used for law enforcement purposes, access to the fingerprints of asylum seekers may be asked by a magistrate in the case of an investigation of a crime.

The fields which were described above are only examples of situations in which biometrics are implemented. Other illustrations which demonstrate the increasing role of biometrics are therefore not excluded.

### 3.2.2 National studies and debate about biometrics

Unisys Corporation, a main IT system supplier, has opened in Brussels, Belgium, a Biometrics Centre of Excellence to serve its clients established in EU countries in 2006.[121] The centre publishes at regular intervals studies conducted by Unisys or its partners on biometrics. In one of these studies, consumers in fourteen countries were randomly surveyed. The survey found that two-thirds of the respondents favoured biometrics as an ideal way to combat fraud and identity theft.[122] For the survey, 436 Belgians were questioned out of a total of 3669 persons. Not less than 89% of the Belgians involved had no objection if banks would use voice recognition or fingerprints to control their identity. The main reason that was given was the *ease of use*: because of the use of biometrics they hoped that it would not be required any longer to memorize pin codes and passwords. 42% thought that the biometrics would increase the *security* of the information and 35% stated that the verification of the identity would be *faster*. In general, one out of five of the Belgians described the Belgian banks as the 'most trustable industry'.[123]

The cryptography research team of the French Catholic University of Louvain (Louvain-la-Neuve) has also studied the storage and the use of biometrics, in particular (so far) the digital picture stored on the RFID chip in the international passport. The research group made in an announcement of mid 2007 public that they made a study and discovered that Belgian passports of the first generation (issued from 2004 until July 2006 (and valid through 2011)) did not possess any security mechanism to ensure the protection of personal data. They demonstrated that the *data stored on the chip of these biometric passports can be read at a distance in a few seconds* without the owner's notice. The biometric passports issued after July 2006 do benefit from a security mechanism, but these are insecure. Anyone with an easy to purchase electronic reading device can acquire all the data on the chip, including picture and signature, without authorization and without the owner knowing it.[124] The weakness has already been revealed for passports of other countries, including German and Dutch biometric

---

nemen kan in Hasselt', available at http://www.hasseltlokaal.be/Item/tabid/55/seqAxNewsItem/2672/Default.aspx; X, 'Mechelse politie krijgt digitaal systeem voor vingerafdrukken', available at http://www.hln.be/hln/nl/957/Belgi/article/detail/635931/2009/01/23/Mechelse-politie-krijgt-digitaal-systeem-voor-vingerafdrukken.dhtml

[121] W. Gardner, 'Unisys opens Brussels Biometric Centre', Techweb Network, 26 April 2006, available at http://www.techweb.com/wire/security/showArticle.jhtml?articleID=186701106

[122] X., 'Consumers Worldwide Overwhelmingly Support Biometrics for Identity Verification, Says Unisys Study', 26 April 2006, available at http://www.unisys.com/about__unisys/news_a_events/04268651.htm

[123] K. Van der Stadt, 'Belgen hebben geen bezwaar tegen biometrie', *Data news*, nr. 35.

[124] G. Avoine, K. Kalach & J-J. Quisquater, *Belgian Biometric Passport does not get a pass… Your personal data are in danger'*, available on http://www.dice.ucl.ac.be/crypto/passport/index.html ; zie hierover ook E. Kindt, 'Belgisch biometrisch paspoort onveilig', *Computerrecht* 2007, pp. 221 – 223.

passports. The weakness of Belgian biometric passports, however, is considered worse, because the information needed to read the chip, the two coded lines at the bottom of the first page, containing birth date, expiry date and passport number, can be guessed in about one hour with a search of all possible combinations if the data of birth and the date of expiry are known. The reason is that the passports numbers are given in an increasing order, are linked to the language and that the passports are only valid for five years, thus limiting the possible combinations to be 'guessed'.

At the occasion of that study, parliament questioned the Minister of the Interior and the Minister of Foreign Affairs in 2007 as to whether the Belgian biometric passports were sufficiently safe. The Minister of Foreign Affairs replied by referring to the technical specifications of the International Civil Aviation Organisation, in particular the Basic Access control and the Active Authentication, which are implemented in the passports and hereby concluded that the Belgian passport is secure.[125] In general, the competent ministers are regularly questioned in parliament about the introduction of the biometric passports, but one can hardly say that there is a real debate with defenders and opponents of biometrics in parliament.[126]

In communications with the press in 2008, the CBPL however has warned for the generalized use of biometrics.[127] The Belgian Data Protection Authority hereby attempted to clarify its position taken in its opinion on the subject (see *below*, section 3.4). At this occasion, various articles appeared in the press on biometrics. These articles warned that biometric systems shall be carefully considered, but one cannot say that there was a debate in the press on the topic with opponents and defenders at the occasion of the newly issued opinion by the Belgian Data Protection Authority.

## *3.3 Legislation regulating the use of biometric data*

### 3.3.1 General and specific privacy legal framework for biometrics

The collection and processing of biometric data is subject to the general data protection legislation, the Law of 8 December 1992[128] (as modified by the Law of 11 December 1998[129]) which was completed with a Royal Decree of 13 February 2001[130] (hereinafter together the 'Law of 1992'). The Law of 1992 implements the Data Protection Directive 95/46/EC. The Law of 1992 applies to the processing of biometric data. There are however no specific

---

[125] *Questions and Answers*, Chamber 2006-07, 9 January 2007, 17-20 (Questions no 13251 of Arens and no. 13421 of Maene), also available at http://www.lachambre.be/doc/CCRI/pdf/51/ic1146.pdf ; see also *Questions and Answers*, Chamber 2006-07, 22 January 2007, 112-114 (Question no 420 of Bex), also available at http://www.dekamer.be/QRVA/pdf/51/51K0150.pdf.

[126] See for example question nr. 584 in which the Minister was asked whether the negative study of the London School of Economics on the electronic identity card in the United Kingdom was also relevant for the Belgian eID, *Questions and Answers*, Chamber 2004-05, 23 May 2005, 79-85 (Question no 584 of Di Rupo), also available at http://www.dekamer.be/QRVA/pdf/51/51K0079.pdf

[127] See Belgian Data Protection Authority, *Privacy commissie schetst kader voor verwerking van biometrische gegevens*, 6 june 2008, available at the website of the CBPL at http://www.privacycommission.be /nl/press_room/pers_bericht6.html ; See also M. Justaert, 'Te veel misbruik van biometrische gegevens. Wildgroei gebruik vingerafdrukken en scans in bedrijven', *De Morgen*, 17 april 2008, 1.

[128] *Belgian State Gazette*, 18 March 1993.

[129] *Belgian State Gazette*, 3 February 1999.

[130] *Belgian State Gazette*, 13 March 2001.

provisions in this general data protection legislation which tackle the issues of the collection and use of biometric data.

Article 22 of the Constitution, introduced in the 1990's, confers the fundamental right to respect for private life.

### 3.3.2 Legal provisions for government controlled ID biometric applications (passports, other civil ID biometric applications and law enforcement)

*Passports*

The Belgian Act of 1974 on the issuance of passports states in article 5 that Belgian passports shall contain the identity of the holder and shall include a picture and signature. Since March/April 2001, passports with machine readable zones were distributed and since 2004, a Belgian so-called biometric passport with machine readable zone and with chip could be obtained. The chip contained in the first phase identity data, signature and picture, which is information that can *de visu* be read on page two of the passport. Fingerprints were not included yet.

*Immigration legislation*

The collection and the use of specific biometric data have been regulated in Belgium in the context of immigration legislation.

In a so-called 'Program Law', which is passed by parliament at the end of the year and which contains an amalgam of various legal provisions, most often in the context of budget and fiscal matters, some provisions about the collection of biometric data from foreigners where included in 2004.[131] In the parliamentary discussion, it was critized that such provisions were part of this 'Program Law' and were not subject of a separate bill which was properly debated in parliament.

It the legislation relating to access, stay, establishment and removal of foreigners[132], it is now specified that fingerprints and 'photographic material' can be collected from foreigners requesting a *visum* or a stay on the territory by Belgian or who are expulsed (Art. 30*bis)*. The data are collected upon the initiative of the diplomatic or consular representatives, the minister, an officer of the judicial police or an officer of the administrative police (Art. 30*bis* §3*)*. The biometric data shall only be used for (1) the *identification* of the foreigners or the *verification* of the identity (stress added), (2) the checking whether the foreigner is a danger for the public order or the national security, or (3) the compliance with regulations or directives of the Council of Ministers of the EU (Art. 30*bis* §4*)*. It is further provided that the collection and the processing shall be done *under the control of the Belgian Privacy Commission*. It is also stipulated that the same biometric data can be obtained upon request of the Minister from the police, the judicial police and the officials and agents of public services who would have such biometric data (Art. 30*bis* §6*)*. A Royal Decree has stipulated that the *term for keeping* the biometric data which are taken from foreigners under this legislation

[131] Article 450 of the Program Law of 27 December 2004, *Belgian State Gazette*, 31 December 2004 (2nd ed.), 87097. This Article was inserted in the Act of 15 December 1980.
[132] The Act of 15 December 1980 with regard to the access to the territory, the stay, the establishment and the removal of foreigners, as modified.

shall be kept for a term of *ten years* and is subject to further implementation by the competent Minister.[133] The legal provisions relating to the collection of biometric data however have no effect for the foreigners who were already on Belgian territory when the legislation entered into force. The same legislation also already provided for the collection of fingerprints from *asylum* seekers (Art. 51.3*)*. These prints may only be used for establishing the identity of the foreigner or for determining the State which is responsible for the asylum request (Art. 51.3 §2*)*.

In the parliamentary discussions, reference was made to an already existing system for the collection of biometric data of asylum seekers, the so-called 'Printrak system. Since 1993 until 2004, 271962 sets of fingerprints were taken and registered in this system. The legal provisions described above, however, intend to expand the collection to other categories of foreigners and immigrants. The Minister for Internal Affairs clarified that notwithstanding the Eurodac system of the European Commission, in which the biometric data are kept for ten years, national countries can decide to establish their own national databases, such as Printrak of the Service foreigners' affairs, in which fingerprints are kept, possibly for a longer period.[134]

*The International Seafarer's identity document*

A new (biometric) identity card for seafarers has been discussed, developed and agreed in a Convention no 185 of 2003 of the International Labour Organization. The treaty entered into force on 9 February 2005 after the ratification by France and Nigeria. The treaty provides for new biometric identity cards for seafarers. The new identity card which shall include biometric information is intended to increase the security of the identity documents while improving the facilities and conditions for the seafarers to go on land in a country of which they are not a national.[135] As long as a country has not ratified the treaty, seafarers need their own national passport and visa if needed, to go on shore.

Belgium *has adopted* the Convention, but has *not ratified* it yet.[136] Various other countries, however, such as the Netherlands do not intend to ratify the Convention because of the high costs for producing, implementing and securing the Seafarer's Identity Document (SID) while the advantages of ratifying the Convention are in practice not proven.[137]

---

[133] Article 1 and 2 of the Royal Decree of 21 April 2007, *Belgian State Gazette*, 31 May 2007 (2nd ed.), p. 29533.
[134] *Parl. Doc*, Chamber 2004-05, n° 1437/022, 19-20.
[135] See also the positive opinion n°1.533 of the National Labour Organization of 9 November 2005, available at http://www.cnt-nar.be/ADVIES/advies-1533.pdf
[136] For the list of the ratifications of the Convention no 185, see the ILO site at http://webfusion.ilo.org/public/db/standards/normes/appl/index.cfm?lang=EN; See also *Parl. Doc*, Chamber 2005-06, n° 2308/01, 22 p., available on http://www.dekamer.be/FLWB/pdf/51/2308/51K2308001.pdf;
[137] The Netherlands have stated that they do not intend to ratify the Convention because of the cost and since other countries have not yet or are hesitating to ratify. See Second Parliamentary Chamber ('*Tweede Kamer*'), 2007-2008, 29 427, no 48, available at http://ikregeer.nl/document/KST117845 and http://static.ikregeer.nl/pdf/KST117845.pdf

*Law enforcement*

The collection, the storage and the use of DNA data for law enforcement purposes has been regulated by law in Belgium in 1999.[138]

The Act of 22 March 1999[139] provides for the setting up of two DNA databases with the Belgian National Institute for Criminalistics and Criminology ('NICC'): a database named 'Criminalistics' and a database 'Convicted Persons'. In addition, the Act contains two new legal provisions to be inserted in the Code of Criminal Proceedings ('*Wetboek van strafvordering*'/'*Code d'instruction criminelle'*). A new Article 44*ter* regulates the collection (of traces) of human cell material, DNA profiles and the use and storage thereof in the context of a criminal investigation ('*opsporingsonderzoek*'). A new Article 90*undecies* provides for a DNA analysis ordered by the investigation judge ('*onderzoeksrechter*'/'*juge d'instruction'*).

The DNA database 'Criminalistics' contains the DNA profiles and additional data of traces of human cell material found. The database also contains results of the comparative DNA analysis, i.e. a positive link with other profiles and/or a code given by the magistrate which links the profile to a person.[140]

The DNA database 'Convicted Persons' which was (formally) established in 1999 with the NICC contains the DNA profiles of each person who has been convicted to imprisonment or a more severe punishment or who has been locked away for one of the crimes listed. Additional data is stored as well.

Since Belgium is a signatory state of the Prüm Treaty[141] of 2005 and various important provisions of the Treaty were adopted in EU legislation[142] for Schengen States in June 2007, DNA and fingerprint information becomes within the EU internationally available for law enforcement authorities.[143]

As of now, fingerprints from suspects are sometimes still taken with ink on a paper[144], where after the fingerprint(s) are sent by fax to the national database for comparison. However, the use of digitalised fingerprint collections, which can be sent electronically, are more and more introduced.

The collection of fingerprint of asylum seekers is in principle not intended for use for law enforcement purposes. However, this does not mean that law enforcements may not request fingerprints collected from asylum seekers in order to compare those with prints taken in the course of an investigation. This could be asked to establish the identity of a person who is under investigation. In that case, an investigation judge could request such comparison.

---

[138] The collection and the use of DNA data, however, were already practiced before, without any legal basis.
[139] Act of 22 March 1999 relating to the identification procedure via DNA-analysis in law enforcement, *B.S.* 20 May 1999, err. *B.S.* 24 June 1999 ('Act DNA-analysis').
[140] See Art. 4 §1 Act DNA-analysis.
[141] Other signatory states are Germany, Spain, France, Luxembourg, the Netherlands and Austria. The Prüm Treaty is the basis for exchanging DNA and fingerprint, as well as vehicle data, across the EU. The Prüm Treaty is therefore sometimes also referred to as Schengen III.
[142] See the Council Decision 2008/616/JHA of 23 June 2008 on the stepping up of cross-border co-operation, particularly in combating terrorism and cross-border crime, *O.J.* L, 210, 6.08.2008, pp. 12 – 17, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF
[143] The NCCI received in 2008 less than 50 requests for the comparison of DNA from countries outside Belgium. See *Questions & Answers* Chamber
[144] See *Questions & Answers* Chamber 2008-09, 16 February 2009, p. 1129 (Question of 2 February 2009 n° 229 Van Biesen).

### 3.3.3 Legal provisions relating to other biometric applications (access control, public-private, convenience and surveillance applications)

For biometric applications other than in the passports and the use of biometric information for asylum seekers and immigrants, there are presently no specific legal provisions which would regulate the collection and use of biometric data for purposes other than the use for law enforcement (see *above*).

In this context, it is interesting to note that for access control, there is a (rather recent) collective labor agreement ('CAO')[145] of 30 January 2007 for theft prevention and exit control of employees upon leaving the company or the employment place.[146] This CAO no 89 lays down the principles of the exit control and aims to enhance transparency and to protect the privacy of the employees, but does not refer to any biometric measurement for the control of the identity of the employees.

### 3.3.4 Biometric systems and the privacy rights of employees

The CBPL issued an opinion on the use of badges and on employee tracking by use of GPS systems. The CBPL hereby stressed that the continuing surveillance of employees was not in proportion with the purposes envisaged by a systems of geographic tracking and not necessary. The CBPL considered the use biometric identifiers in the context of badge systems used to monitor the hours of an employee's presence also disproportional, because of the intrusive nature of this type of surveillance.[147]

## *3.4 The National Data Protection Authority on biometrics*

*Volume of files related to biometrics*

The CBPL stated in its annual report for 2007 that it treated five files related to the use of identification technologies, in particular biometrics, in the field of e-government and almost an equal number of files (four) related to biometrics/DNA in the sector of police, justice and security. Biometrics in general was also subject of one file. These files represent less than 1% of the total number of files that the CBPL had to resolve in 2007.[148]

*Opinion of April 2008 concerning the processing of biometric data*

As mentioned above, the CBPL has issued at its own initiative an opinion on the use of biometric data for the authentication of persons in April 2008.

The opinion is restricted to the field of the use of biometric data by public and private parties for purposes other than police and security purposes (law enforcement) and border control.

---

[145] A collective labour agreement is an agreement which is the result of discussions amongst representative organisations of employees and of employers. They may become generally binding upon confirmation in a Royal Decree.

[146] Collective Labour Agreement N° 89 concerning theft prevention and exit control of employees upon leaving the company or the employment place.

[147] See also Article 29 Data Protection Working Party, *Ninth Annual Report*, June 2006, p. 22.

[148] Commission for the Protection of Privacy, *Annual report 2007*, p. 54-55.

The focus of the opinion is the use of biometric data for authentication purposes. The use of the term 'authentication', however, is confusing, because both the identification functionality of a biometric system and the verification functionality can be used to authenticate a person. These two functionalities of a biometric system are however completely different and pose different risks for the privacy. The Working group 37 of ISO/JTC 1 which spends many efforts in the establishment of a harmonized vocabulary, recommended earlier to no longer use the term authentication in the context of biometric systems and to refer to either identification or verification.[149]

After an introduction in which the CBPL stressed the importance of biometric information as a tool to link the identity of a person to a physical person and an explanation of the functioning of a biometric system, the CBPL stated clearly that it considers biometric data in principle as being *personal data*. Nevertheless, the CBPL stated in a footnote that in rare cases, biometric data may not be personal data because a link with persons can not be established with reasonable means. The CBPL hereby stressed that while data may at a given point in time may not be personal data, they may become personal data because of new circumstances or new technologies which facilitate identification.[150] The CBPL also stated that biometric data can give information relating to health or racial origin.[151] However, they will only be considered as 'sensitive' data by the CBPL if they are *used* to obtain information relation to health or racial origin. The CBPL further commented that the processing of templates implies in its opinion that one does not process sensitive data.[152]

The core of the opinion of the CBPL relates to the requirement that the processing shall not only be *legitimate* (*'rechtmatig' of 'toelaatbaar'*), but also *proportional*. The CBPL hereby explained in about nine pages what it considers to be proportional. This lengthy description of the factors which have to be taken into account to judge the proportionality is quite interesting.

The legitimate processing of personal data requires that the processing is based on one of the conditions of Article 5 of the Law of 1992 (which implements article 7 of the Directive). One of these conditions is that the data subject has consented with the processing. Interesting is that the CBPL notes that a 'free, specific and informed' consent requires that there is an *alternative system* to be used by the data subject. Furthermore, the CBPL also notes that consent will not make an excessive biometric processing, which is a processing that is not 'absolutely necessary', legitimate.[153]

The CBPL explained that for measuring the proportionality, one shall take the interests of the controller into account and balance these interests against the right for respect to private life of the data subjects. The interests of the controller are according to the CBPL the automation of the process, the increased certainty, sometimes the decreased cost and the user friendliness, but above all the *increased security* offered by biometrics as an authentication tool. The right and interest of the data subject with regard to respect for private life is explained by the CBPL by pointing to (1) the fact that the biometric data *are normally unchangeable*, hereby

---

[149] E. Kindt, 'Biometric applications and the data protection legislation', *Datenschutz und Datensicherheit* 2007, vol. 3, p. 166 *et seq*. The groups stated that authentication is depreciated and should be replaced by verification.
[150] CBPL Opinion on biometrics , *o.c.* at footnote 113, p. 8.
[151] *Ibid.*, p. 9. The CBPL stated that various kind of biometric data could contain information relating to health and referred in a footnote to the use of hand geometry.
[152] *Ibid.*, p. 9. The CBPL referred for its position to Council of Europe, *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, February 2005.
[153] *Ibid.*, p. 10.

increasing the risk for lifelong profiling, (2) the deployment of biometric data and *human dignity* aspects, (3) the biometric data as *an identification tool*, (4) the increased risk of *identity theft* in case biometrics are increasingly used as an authentication tool, (5) the fact that some biometrics leave traces (such as fingerprint) which increase *the risk for re-use of the data* and (6) the choice of a society by allowing unrestricted use of biometrics, for example in school libraries, while biometrics pose *risks.*[154]

The CBPL recapitulated that the proportionality of the use of biometric systems shall be interpreted in a *strict way*. Proportionality means that only biometric systems shall be used which respect the privacy as much as possible, for applications which require special measures, further *avoiding excessive use of personal data* (e.g., consumers shall not be identified for purchasing goods) or excessive use of additional identifying data accompanying the biometric data.

Biometric systems which respect the privacy as much as possible are put by the CBPL in two categories:

A. the biometric systems which are by the CBPL considered *in se* proportional and, if the system does not comply herewith,

B. the biometric systems which have to be first compared with other systems on the market.

These two categories are hereunder further explained. The biometric systems which are by the CBPL considered *in se* proportional (category A)

- only use personal data *if necessary or proportional*; and

- do *not* use biometric characteristics which leave *traces*, and

which follow the recommendations of the CBPL to

a. *not* store reference data in *databases* and use the verification functionality,

b. not store images but *templates* (because of the risk of cross linking),

c. *not use* biometric characteristics which can be collected *without the data subjects's knowledge*, and

d. which deploy appropriate *security* measures.[155]

The CBPL interestingly commented that the fact that the central storage may be more user friendly (because the data subject does not need to carry a token), does not outweigh the risks of central storage.[156]

If a biometric system does not comply with the above mentioned criteria, for example because the system uses biometric characteristics which leave traces (category B), the system has to be compared with other non-biometric systems which are available on the market and should only be used if they are *the only* way to reach the objective. The CBPL stated that this is for example required for systems used by schools. Only if the control at high level is justified by a specific circumstance, the use of a biometric system could be considered proportional. The same applies according to the CBPL for the use of a biometric system as time and attendance control. The controller should first make *an evaluation of the type and importance of fraud*

---

[154] *Ibid.*, p. 13. The CBPL hereby referred to the Working document on biometrics of 2003 of the Article 29 Data Protection Working Party, p. 3.
[155] *Ibid.*, p. 15-17.
[156] *Ibid.*, p. 16.

*and the rights of the data subjects*. Furthermore, the CBPL stated that the risk of fraud diminishes considerably in case the number of employees is small. A pure *economic advantage alone* is *not sufficient for the proportionality*. Finally, for these systems of category B in so far the conclusion would be that a biometric system is the only way to reach the goal, all recommendations of the CBPL which apply for the systems of category A (which are per se deemed proportional (see *above*)), (recommendations such as no central database, no samples, etc) apply.[157]

The proportionality further requires according to the CBPL that the use of the system is *restricted to the areas or services which justify biometric control* and that *no more personal data need to be mentioned with the biometric information* than required.[158]

The CBPL further concluded with recommendations with regard to *the information to be provided to the data subject* (such as about the type of system, the *possibility of errors* and the *procedure in that case*, and about the right to prove the contrary), the term of storage (including that storage shall be limited to the time employees have access rights to a specific place and that sensors shall not keep the data longer than for the comparison phase) and security measures (which shall be very high and designed for each and every step in the processing).

The CBPL stated that the opinion may be reviewed later in function of further developments of technology and the experiences of the commission.

## 3.5 Conclusion

With the Opinion on biometrics of the CBPL in 2008, the proportionality of the deployment of biometric systems gained attention in Belgium. While the use of biometric identifiers was already briefly reviewed in some opinions of the CBPL in relation with proposed (mainly immigration) legislation, the Belgian DPA has now extensively clarified its opinion on the proportional use of biometric identifiers.

There has been no legislation initiatives however in order to regulate the (general) use of biometrics in the public or private sector.

[157] *Ibid*, p. 18, §74.
[158] *Ibid.*, p. 19.

# 4 France

## 4.1 Introduction

Biometric systems have been introduced in France as well. The use of biometric systems has become quite widespread, in particular for Type II access control purposes in companies, administrations and schools. Various systems are also used for Type I government controlled ID applications, in particular for foreigners (visa) and immigrants, although biometric systems are intended to be deployed in Type I government controlled ID applications for the French citizens as well (e.g., the *INES* project and biometric passports).

In 2004, the French data protection legislation was modified. The French law now requires that the automated processing of biometric data for identity control, whether by public or private entities, is subject to the *prior authorisation* of the French Data Protection Authority, the *Commission Nationale de l'Informatique et des Libertés (*'CNIL*')*. In case of such biometric processing for the government, such biometric data processing needs to be authorised by a decree ('décret').

The CNIL stated in a communication that it reviewed its first biometric application for civil purposes in 1997, and that since then, the requests for authorization of biometric systems have rapidly grown. In 2005, the CNIL had reviewed and approved 34 biometric systems (while five systems were refused). In 2006, this number of reviewed systems has been *multiplied with ten*: the CNIL registered 299 declarations of conformity, approved 52 biometric systems and refused nine systems.[159] In 2007, 515 biometric processing applications were submitted for review by the DPA (an increase of 43 % as compared with 2006), 449 of which were *declarations of conformity*, and 66 systems which requested prior checking. Of the latter, 21 systems were *refused authorisation*, and 45 were authorized. 120 requests for checking were *still pending*.[160]

Because of the ever increasing number of requests, the CNIL has adopted in 2006 three simplified procedures for authorization which will be explained below.

It is further important to note that the CNIL favours the use of biometrics which *do not leave traces* (such as hand geometry) and the storage of biometrics (e.g. fingerprint) on *objects under the control of the data subject*. Finally, importance is also given to the ethical aspects of the use of biometrics.

## 4.2 The spreading of biometric applications

### 4.2.1 Fields in which biometric applications are implemented

As stated above, biometric methods are in France mainly used for access control purposes, in particular in the employment context. Such biometric access control systems represented in 2006 299 out of the 351 systems for which an approval was given.

---

[159] CNIL, *27e Rapport d'Activité 2006*, p. 13, available at http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-27erapport-2006.pdf

[160] CNIL, *28e Rapport d'Activité 2007*, p. 18, available at http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-28erapport-2007.pdf ; See also CNIL, *Biométrie : la CNIL encadre et limite l'usage de l'empreinte digitale*, 28 December 2007, available at http://www.cnil.fr/index.php?id=2363&0=

However, a new trend is that biometrics are increasingly used by controllers other than employers, such as casino's, who ask approval for the (voluntary) use of membership cards with fingerprint of customers for access control (the access control is imposed by law since 1 November 2006 in France).

### 4.2.2 National studies and debate about biometrics

*Attention by the National Parliament*

The use of biometric methods has received attention from the French parliament. In 2002, the 'Assemblée Nationale' commissioned with the parliamentary Office for the Evaluation of the Scientific and Technological Choices a study about the scientific methods of identification of persons based on biometric data and related technologies. The Office deposited its study on June 16, 2003 ('Report Cabal').[161] The Report Cabal consists of three parts, in which the use of biometrics is discussed by experts, not only from a technical point of view, but also including a discussion of the need to come soon to an adapted legal framework, and with recommendations.

In November 2005, the French Senate and the CNIL also organized a two day conference entitled 'Information technology: slavery or liberty?', during which identification by biometric technologies was discussed as well.[162]

*Studies*

In 2008, the DPA commissioned for the first time three studies in the field of biometrics in order to evaluate 'the state of the art'.[163]

*Ethical aspects*

The ethical aspects of the use of biometric data were also the topic of study and an opinion of the National Advisory Commission for Ethics for Life and Health Sciences.[164]

*National Electronic Secured Identity project ('INES')*

The Minister of the Interior, Jean-Pierre Raffarin, approved on 11 April 2005 the project '*Identité nationale électronique sécurisée* ('*INES'*) to review the issuance of the national identity card in France.[165] A problem is that new non falsified identity cards are increasingly issued on the basis of falsified documents establishing identity. The idea was to reinforce the reliability of the identity card by establishing a root identity, a so-called '*titre fondateur'*[166] which consists of a bloc of secured information and which should allow to secure the issuance of the identity cards. The data for such root identity would include not only picture and

---

[161] Office for the Evaluation of the Scientific and Technological Choices, *Study about the scientific methods of identification of persons based on biometric data and the used technologies*, Assemblée National N° 938/Sénat, N° 355, ('Report Cabal').

[162] '*Information technology : slavery or liberty'*, Conference organized by the CNIL and the Univesity Panthéon-Assas-Paris II, Senate, available at http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat1.html

[163] CNIL, Press conference. Presentation of 28th annual report 2007, p. 15, available at www. cnil.fr.

[164] Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé, *Opinion N° 98. Biométrie, données identifiantes et droits de l'homme*, 31 May 2007.

[165] E. Dumout, *"INES", nom de baptême de la carte d'identité électronique*, 25 August 2001, ZDNet.fr , available at http://www.zdnet.fr/actualites/telecoms/0,39040748,39168171,00.htm#storytalkback

[166] See also references to such 'titre fondateur' in the Report Cabal, cited at footnote 161, p. 48.

signature, but also fingerprint. Two digital fingerprints would be included in the chip on the card, and six digital fingerprints would be stored in a data base. INES would foresee in the creation of two large central databases, one for the digital images of the French citizens and the other one with the fingerprints. In addition to secured identity title deliverance, the objective was to simplify the process of issuance by the administration and to establish an electronic identity card that could be used for e-government. This plan was also considered in line with international developments in the United States and Europe, which require biometric passports. One of the other uses of the databases would also *be their use by the police* for comparison of 'anonymous' biometric data with those of the INES databases in order to identify the owners.

The first electronic identity cards were scheduled to be issued in 2006. The plan, however, caused a lot of debate.[167] The CNIL clarified its position on the proposed biometric eID as well.[168] The INES project involves according to opponents major societal issues, such as the biometric identification of the French population. Therefore, the INES project is not on schedule anymore.

*Schools*

The installation of biometric systems for access control purposes in schools or for access to school restaurants has caused tumult as well. In November 2005, two biometric systems in a high school of Valleé de Chevreuse were destroyed during a playful action. In June 2006, students destroyed two biometric access control systems of a school restaurant in a high school of Gif-Sur-Yvette. Various schools that installed a biometric access system are listed as nominees for the Big Brother Awards in France. The school Joliot-Curie de Carqueiranne that was the first school that attempted (without success) to install a biometric access control system and filed a declaration with the CNIL in 2002 obtained for France the 'Big Brother award' of Privacy International in 2005 because 'it caused dozens of other schools in 2003, 2004 and 2005 to follow its example'.[169]

## 4.3 Legislation regulating biometric applications

### 4.3.1 General and specific legal privacy framework for biometrics

*General*

The French general data protection law N° 78-17 of 6th January 1978, as modified, (hereinafter the 'Act N° 78-17') mentions explicitly biometric data.[170] The Act N° 78-17 requires since a modification of the Act in 2004 that all the automated processing of biometric data for identity control *must receive the prior authorisation* of the CNIL (Article 25, I, 8°).

---

[167] See e.g., Le Forum des droits sur l'internet, *Carte nationale d'identité électronique. Deuxième étape du débat public itinérant*, 31 March 2005, available at http://www.foruminternet.org/telechargement/forum/cpte-rendu-lyon-20050331.pdf

[168] See CNIL, *Position de la CNIL sur la carte nationale d'identité et la biométrie*, 31 May 2005, available at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Position-cnil-CNI-05-2005.pdf

[169] See "Big Brother Awards France", available at http://bigbrotherawards.eu.org/spip.php?page=liste-bba&annee=2005

[170] For the text of the Act N° 78-17', see the website of the CNIL, at http://www.cnil.fr/index.php?id=300.

The processing of biometric data necessary for the 'authentication or the identity control' for the government needs to be authorised by a decree ('*décret en Conseil d'Etat*') in execution of the law after the CNIL has rendered its opinion which shall be public and motivated (Article 27, I, 2°).

The CNIL may also issue an unique authorisation ('*decision unique*') for the data processing which include biometric data and which have a same purpose, contain the same categories of personal data and have the same (categories of) receivers as set forth in the unique authorisation which the CNIL proclaims (Article 25, II). If a controller esteems that the data processing of the biometric data meets these criteria, he shall send a 'letter of conformity' to the CNIL stating that the data processing complies with the description in the unique authorisation.

Since this modification, the CNIL has issued three so-called 'unique authorisations' with regard to the processing of specific biometric data for specific purposes. Two of the three unique authorisations relate to the use of biometrics in the employment context. [171] They will be discussed in section 4.3.4. The other unique authorisation N° 103 relates to the use of hand geometry of pupils and personnel for access to a school restaurant and will be discussed in section 4.3.3.

The Act, however, does not contain any other references to the processing of biometric data than the requirement for prior authorization.

*Case law relating to biometric data*

There has been some (limited) case law in France on the use of biometrics in the employment context (see *below* section 4.3.4). In a decision of March 2007 of the highest administrative court, the Conseil d'Etat, to whom various claims were brought against the setting up of a database of illegal immigrants, named ELOI, for expulsion, stated that since the database would include a digitised photograph, the database should have been created by a law ('loi') or decree ('*décret'*) instead of the ministerial order ('arrêté') of 30 July 2006.[172] The ministerial order was hereby annulled because an incompetent authority enacted the legal basis. According to some commentators, the Court hereby indirectly acknowledged that a digitised photograph is a biometric identifier, even though in the case at hand the images were not processed by face recognition software.

---

[171] In one such authorisation, the use of fingerprints for access control is accepted if the biometric is stored on a token (smart card or USB token) held under the control of the employee. According to another authorisation, the use of hand geometry for access and time and attendance control of employees is possible. See CNIL, *Délibération n°2006-0102 du 27 avril 2006 portant authorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, 27 April 2006 ('*Délibération n°2006-0102'*)and CNIL, *Délibération n°2006-0101 du 27 avril 2006 portant authorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle de l'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail*, 27 April 2006 ('*Délibération n°2006-0101'*). See also below, section 4.3.4.

[172] See Conseil d'Etat, App. N° 297888, 297896,298085, 13 March 2007, available at http://www.conseil-etat.fr/ce/jurispd/index_ac_ld0712.shtml

*Specific regulation on the use of genetic information*

Article 16-10 of the French Civil Code states that *genetic characteristics* shall not be studied except for *medical reasons* or *scientific research*. The written consent shall in that case be required and can be revoked at any time.

Moreover, Article 16-11 states that the *identification* of a person *by his genetic data* shall not be made unless for investigation purposes during a *judicial procedure*, for medical purposes or scientific research. In *civil* matters, such identification can only be made upon order of a judge in matters of *kinship* or for the obtaining or suppression of *subsidies*, all provided consent was obtained. Unless with consent, no identification can be made after death. Penal sanctions are imposed. Moreover, only the persons who are licensed may conduct such identification. [173]

Finally, the French Civil Code states that *nobody* shall be *discriminated* based on his or her genetic characteristics (Article 16-13).

Article 25, I, 2° of the Act N° 78-17 further requires the prior authorisation of the CNIL in principle for the processing of genetic data (except if necessary for preventive medicine, diagnostics or health care administration).

### 4.3.2 Legal provisions for government controlled ID biometric applications (passports, other civil ID biometric applications and law enforcement)

*Legislation for the biometric passport*

By decree (‘*décret*’)[174] of 30 April 2008, the new French biometric passport was introduced. The passport will contain an electronic chip, which contains not only the picture of the holder, like the present passports, but also two fingerprints, in accordance with the Regulation 2252/2004. The same decree provides for the creation of a central database, containing the pictures of the applicants for a passport, and the fingerprint of eight fingers.[175]

---

[173] See Article 16-11 and 16-12 of the French Civil Code, as modified by Act N°2004-800 of 6 August 2004, available at http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006419305&dateTexte=&categorieLien=cid

[174] A ‘décret’ is an executory act and is not the same as a ‘loi’, which is passed by Parliament.

[175] See Article 6-1 of the decree (‘*décret*’) N° 2005-1726 of 30 December 2005 relating to passports (as modified) providing upon application for a passport for the taking of eight fingerprints, Article 18 allowing an automated processing called ‘TES’ for the issuance, renewal and revocation of passports and the prevention and detection of false passports and Article 19 which provides for the storage of the digital image of the face and the fingerprints. Article 21 provides for access to the information stored on the chip of the passport for identity control and control of the authenticity of the passport by the police and Article 21-1 provides for access to the central database, excluding the facial images and the fingerprints, for police and intelligence services for specific cases in the sphere of the fight against terrorism after due authorisation by the head of the police or the intelligence service. Article 23 provides for interconnection with the information systems of Schengen and Interpol, but only relating to numbers of stolen or lost passports. See also the opinion of the CNIL about the proposed modifications, *Délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d’Etat modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques* available at http://www.cnil.fr/?id=2427.

*Modifications to the legislation relating to the French national identity card*

By decree (‘*décret’*) N° 99-973 of 25 November 1999, some provisions of the decree (‘*décret’*) N° 55-1397 of 22 October 1955 which introduced the French national identity card, have been modified. Article 5 of the decree N° 55-1397 now states that when a request is made for a national identity card, *digital fingerprints* of the applicant are taken which are ‘kept in the file of the service administrator’. The law states that the fingerprints can only be used for (1) detection of the attempts to obtain or use an identity card in a fraudulent way; and (2) the secure identification of a person in a judicial procedure.[176]

The CNIL issued in 1980 and 1986 advices at the occasion of the modification of the law on the national identity card for automated data processing and noted at these occasions that, for the request for *fingerprint* at the time someone applies for an identity card, (i) *no manual, mechanical or automated central database with fingerprint on the national level would be made* and that (ii) no digitalised prints would be kept, but on paper support in files kept by the department. In its opinion of 1980, it stated that the (digitalised) signature and the digitalised pictures and the storage in a national database, shall only be used for the term *strictly necessary for the manufacturing* of the card. Moreover, the CNIL repeated its request to take all necessary measures to effectuate the *destruction* of the files in case of *important crisis*.

More recently, the CNIL repeated in 2005 in an opinion on the national identity card and the use of biometrics, its position with regard to the use of biometrics, as developed in 2000. In particular, the CNIL stressed the risk of function creep, i.e. the use of the biometric data for other purposes as initially intended. More precisely, it referred in that annual report of 2000 to the fact that fingerprint was not only in the past mainly used by the police, but that a database with fingerprints is likely to be used *in the future as well by the police* and to become ‘a new instrument of the police’, notwithstanding the original purposes of the processing.

In the meantime, the access rights to the national identity card databases have been enlarged.[177]

### 4.3.3 Legal provisions relating to other biometric applications (access control applications, public-private model, convenience, surveillance)

*Unique authorizations for Type II access control applications*

As stated above, the CNIL issued three unique authorizations. Two of the three unique authorisations relate to the use of biometrics in the employment context and will be discussed in section 4.3.4.

The *unique authorisation N° 103* of the CNIL relates to the use of hand geometry of pupils and personnel for *access control to a school restaurant*.[178] The unique authorization of the

---

[176] Decree (‘décret’) N° 55-1397 of 22 October 1955 introducing the national identity card (as modified), available at at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006060725&dateTexte=20090508 ; For the text of the Decree N° 99-973, see http://admi.net/jo/19991130/INTD9900188D.html

[177] See the decree *(‘décret en Conseil d'Etat’)* N° 2007-391 of 21 March 2007 (*JO* of 23/03/2007) modifying the decree n° 55-1397 of 22 October 1955.

[178] CNIL, *Délibération n°2006-0103 du 27 avril 2006 portant authorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire*, 27 April 2006.

CNIL requires from the system to be compliant *inter alia* that (i) *no pictures* of the hand are kept and that only a template is processed, (ii) *only the geometry* of the hand is used (and not, e.g., lines, or print of fingers,…), (iii) limited and restricted specific information are processed, (iv) the data are restricted to specific receivers and that (v) the data subjects (and their parents) have the right to object in which case they shall receive another way (*alternative means*) to have access to the school restaurant.

Before, for example in an opinion of 2000, published in the annual report of that year, the CNIL had refused a biometric fingerprint system with central database for facilitating access to and the administration of the accounts of a school restaurant. The CNIL hereby referred to the facts that (i) fingerprint leave traces and these prints and traces can be used to identify persons and that as a result (ii) fingerprint databases can be used for purposes other than those initially envisaged. In 2000, the CNIL rendered in fact several opinions with regard to the use of fingerprint centrally stored for a variety purposes.[179] At the occasion of these requests for opinion, the CNIL did not hesitate to point out in its annual report of 2000 that fingerprint was not only in the past mainly used by the police, but that a database with fingerprints is likely to be used *in the future as well by the police* and to become 'a new instrument of the police', notwithstanding the original purposes of the processing.[180] The CNIL concluded that the use of such biometric system in the school was therefore '*excessive*' in relation to the purposes of the processing and rendered a negative advice.[181]

### 4.3.4 Biometric systems and the privacy rights of employees

Biometric technologies deployed at the workplace are mainly used with the purpose of controlling physical access and of monitoring the working time of the employees. The use of biometric systems is furthermore expected to increase in the following years in this context. It is interesting in this context to mention Microsoft's patent regarding the implementation of a biometric device which would monitor employees' for changes in their heart rate or facial expression and report them to their manager.[182] One of the main problems is the impossibility to delete the traces left and the biometric characteristics themselves. Whereas a password may be changed, a biometric identifier can not. Their use renders the technology highly intrusive in terms of privacy and thus calls for stronger safeguards.

---

[179] The first opinion of the CNIL with regard to the use of fingerprint for access control, however, dates from 1997. The CNIL hereby rendered a positive opinion on a fingerprint access control system by the National Bank, *Banque de France*, for access to highly secured zones. CNIL, *Consultation n° 97-044*, 10 June 1997, referred to in CNIL, *21e rapport d'activité 2000*, p.104 ('CNIL, *21e rapport d'activité 2000*').

[180] *Ibid.,* p.108 *:'Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale*'.

[181] CNIL, *Consultation n°00-015 of 21 March 2000 with opinion on an automated data processing by the school Jean Rostand of Nice for access administration to the school restaurant by fingerprint verification*, published in CNIL, *21e rapport d'activité 2000*, p. 110.

[182] Press release, Microsoft big-brother patent? 18th January 2008, available online at: http://www.microsoft-watch.com/content/corporate/microsofts_big_brother_patent.html

*Employees' privacy vs. employer's right to control the working activity*

The use of biometrics at the workplace requires the weighting of the right to privacy against the right of the employer to control the work activity. In 2001, the French Supreme Court acknowledged the protection of the employees' privacy at the workplace. The Court ruled in the so-called "Nikon" judgment that the right of the employer to control the use of the company's personal computers should not put at stake the employee's right to privacy.[183] Legal constraints for the use of biometrics will thus arise from both labour and data protection law.

The Labour Code stipulates that the measures with an impact on the personal rights and individual and collective freedoms of employees introduced and implemented by the employer should be justified by the nature of the task that should be accomplished, and be proportionate to the purpose (Art. L.120-2). Control of the measure's proportionality will be dealt with by the Courts. On the basis of this article, the Tribunal of High Instance of Paris judged in 2005 that a company should *justify* the need to use biometric systems for purpose of monitoring employees' working time. If the company fails to do so, the processing is deemed to be disproportionate and to violate individual freedoms, more particularly the integrity of the body.[184] According to this Tribunal, the integrity of the body does not however justify restrictions on the use of biometrics for purposes of security. The Tribunal further followed the doctrine elaborated by the CNIL.

This reasoning has been contested however by some scholars who considered that body integrity should be acknowledged as an intangible principle to be placed above any other consideration. Whereas derogations to this principle could be justified for purposes of public safety and individual security when processed by judicial or administrative authorities, the processing of biometrics by private parties should be avoided in any case. Derogations to the employees' dignity could not be based on (legitimate) interests of the employer.[185]

Moreover, a general obligation of transparency is set up by the Labour Code. Prior information should be provided to the Work Council[186] and to the workers and candidates (articles L432-2 and L121-8).

*The protection against privacy-invasive biometrics devices: the doctrine of the CNIL*

Personal data processing at the workplace should also be compliant with data protection legislation. In that sense, the Supreme Court judged that the processing relative to the monitoring of working hours that have not been declared to the CNIL could not be used by the employer to ground a dismissal.[187]

As mentioned above, any processing involving biometrics data should since the last reform of the French data protection law in 2004 be authorised by the CNIL. Before the reform, the

---

[183] Cass. Soc., 2 Oct. 2001, n°99-42 942, Nikon c/Frédéric Onof: Juris-data n°2001-011137; Dr. Social 2001, p. 915, note J.-E.Ray.

[184] TGI Paris, 1ère ch. Soc., Comité d'entreprise d'Effia Services, Fédération des Syndicats SUD Rail c/ Société Effia Services, 19 April 2005, available at Juriscom.net, <http://www.juriscom.net/jpt/visu.php?ID=700>.

[185] D. Touchent, *La mise en oeuvre d'un système de badgeage par empreintes digitales dans l'entreprise*, La Semaine Juridique Entreprise et Affaire n°37, 15 September 2005, 1337.

[186] The violation of this obligation constitutes a hindrance [*délit d'entrave*] (Article L438-1 of the Labour Code). The texts applying to civil service established a similar obligation of information and consultation.

[187] Cass. Soc. 6 April 2004, n°01-45227, Sté Allied signal industriel Fibers SA c/X.

CNIL had a mere power of recommendation, which were not always followed in practice. Over the last years, the CNIL has been defining the margin of manoeuvre of controllers depending on the kind of storage, the type of biometrics identifiers and the purpose of the processing. It is thus a multitude of criteria that will be examined by the CNIL to assess the proportionality of the processing. Some of these components will be further discussed below. It is important to retain, however, that fingerprints are designated as the paradigm of biometrics data that leaves traces. Individuals may not be aware that their traces are being captured and this thus increases the risks of function creep and more particularly of ID fraud. To that effect, the CNIL will be more willing to authorise application base on hand geometry or iris scan rather than ones based on fingerprints. [188]

*The "unique authorisations" of 2006 of the CNIL in the context of employment*

On the basis of the criteria developed by the CNIL, the CNIL has issued various 'unique authorisations'[189], i.e. simplification notification procedures, for three different biometric processing based on hand geometry and fingerprint, two of them for the use of biometrics in the context of employment. These processing are by the CNIL deemed to present lower risks for the data subject's right to privacy and are hereunder briefly discussed.

*Biometric applications for access control of employees based on fingerprints stored on individual carriers*

First, applications with the purpose of *access control* based on *fingerprints* stored on *individual carriers* over which the data subject keeps a complete control are deemed compliant with the Data Protection Act.[190] Individual carrier means any carrier under the exclusive control of the individual, e.g. a card with a chip or magnetic. The purposes of the working time monitoring are expressly excluded from the scope of this authorisation.

Furthermore, the application should comply with a series of additional technical features such as:

- Only the '*template*' of the fingerprint can be stored on the device. Images of the fingerprint can not be stored;
- The information stored can not be read without knowing of the individual;
- After the enrolment and registration process, the fingerprint data should be erased from the computer used to this purpose. This process should not last more than a few seconds;
- The access control should be realised though a *comparison* between the finger and the fingerprint template. No copy of the 'template' can be made;

---

[188] CNIL, Press release, *La biométrie sur les lieux de travail*, 19 July 2006, available online at: http://www.cnil.fr/index.php?id=1555&news[uid]=130&cHash=f74e43e56a

[189] Certain files or processing of sensitive data or data with a high risk of intrusion in privacy right, with a same purpose, are authorised by the CNIL through framework decisions called unique authorizations ('*unique autorisation'*). Controllers are then only required to submit a declaration of conformity.

[190] CNIL, *Authorization unique n° AU-008, Délibération n°2006-0102,* 27 April 2006, O.J. of 16 June 2006, text n° 100.

- Other non biometrics data necessary to the identification of the individual and the verification of the validity of the badge can be recorded on the server dedicated to access control.

There is also a limitation on the personal data that can be processed to: (a) the identification data (name, surname, card number and fingerprint template), (b) professional data (internal number, department and grade), and (c) movements (used door, areas and time when the access is authorized, data and hours of entries and exits). When the application controls the access to a parking, it is moreover possible to process (d) the license plate number and the number of parking place. When it is necessary to process visitors' data, in addition, data relating to the company and the name of the employee guiding the visitor may be processed.

The Authorization stipulates that the staff managing human resources and security may access the data related to identity, professional life (not for security staff), movements and parking for the needs of the accomplishment of their tasks. However, they have in principle no access to the fingerprint template unless temporarily and for purposes of registration or deletion from the individual carrier.

Finally, strict delays of storage for various categories of data are established. The biometric template can only be processed during the time that the employee is authorized to access the restricted area. Data relating to the movement of the employees and the visitor related information can not be kept for more than 3 months. The other data can be stored a maximum of five years after the employee has left the company.

In addition, various other obligations, such as relating to security and confidentiality, information of the employees and the data subject's rights to access and correct personal data apply.

In case a biometric data processing complies with *all* the stipulations of the Authorization, the data controller does not have to submit the processing to the prior authorization of the CNIL.

*Biometrics applications based on hand geometry*

Applications for the management of working hours and presence time, and for access control of employees to restricted areas and access control of visitors, based on hand geometry, and for catering at the workplace (access control, management, payment system) have also obtained the benefit from an unique authorisation.[191]

The biometric application should comply with the following technical constraints:

- No picture of the hand can be stored. Only the *template* can be stored in a *database* where it can be linked to an identification number;
- The elements analysed for the identification purpose exclusively rely on the hand geometry;
- When the purpose consists in controlling working hours, the biometric system can be linked to an application of time schedule management;

[191] CNIL, *Authorization unique n° AU-007, Délibération n°2006-0101,* 27 April 2006, O.J. n° 138 of 16 June 2006, text n°99.

- When the purpose consists in controlling the access to the catering service the biometric system can be linked to a catering management software and a payment system.

The unique authorization limits the personal data that can be processed to the data of identity, professional life, time of presence, movements and parking. In the case of catering services, other data may be processed, but only a general description of the food may be made.

Biometrics identifiers should be deleted when the employee leaves the company. For the other data, other terms apply.

A strict definition of the *authorized use* of personal data collected through the use of these systems by other staff members of the company shall also be realized depending on their tasks.

In case a biometric data processing complies with *all* the stipulations of the Authorization, the data controller does not have to submit the processing to the prior authorization of the CNIL.

## 4.4 Legal measures in response to specific threats by biometric systems

As described above, France has adapted its data protection legislation by imposing that all biometric data processing *shall be submitted to the prior authorization* by the CNIL. Moreover, a decree is required if authentication or identity control is to be done by or for the government. These modifications of the law are supposedly taken to handle the specific threats posed by biometric systems.

The same law also provides that the CNIL can issue *simplified notification procedures.* The CNIL has at the same time used this possibility for the notification of biometric applications, by issuing various so-called 'unique authorizations' as mentioned above.

## 4.5 The National Data Protection Authority on biometrics

*Early involvement of the CNIL and an increasing number of cases*

The French DPA, the CNIL, is one of the first established DPAs in Europe. The CNIL celebrated recently its thirtieth anniversary.

In the last twenty years, the CNIL has reviewed many biometric systems and the use of biometric characteristics for various purposes. One of the first occasions at which the CNIL expressed its opinion in this matter relates to the National Database of Digital Fingerprints ('*Fichier National des Empreintes Digitales' ('FNAED')*) of the Ministry of the Interior, which was used for law enforcement purposes.

Over the years, and as mentioned in the introduction, the CNIL was requested to render its opinion in a steep increasing number of cases. The modification of the data protection act in 2004 does not seem to have solved all outstanding issues. In 2007 only, the DPA received 602 requests for the review and the authorization of biometric systems (as compared to 186 requests in 2005 and 2006 all together).

In its annual report for 2000, the CNIL devoted one full chapter to access control by biometric systems.[192] At that time and based upon figures of the industry, the market of biometric systems consisted for 30% of systems which used digital fingerprints, shortly followed by systems using hand geometry (27%).[193] Because of the predominance of the systems which use these two biometric characteristics, the observations of the CNIL focused on these systems. In the same year, the CNIL also issued various opinions.

*Preference by the CNIL for biometrics which leave no traces*

In its report for 2000, the CNIL expressed its doubts with regard to the use of some specific biometric characteristics, in particular digital fingerprints, and qualified some biometric characteristics as being more 'dangerous' than other biometric characteristics. First, biometric characteristics *which leave traces* in places where individuals go, pose in the view of the CNIL more risks. In this regard, fingerprint and DNA (e.g., as contained in hair, skin flakes, …), but also face because of the increased use camera surveillance in combination with face recognition, are hereby *identified by the CNIL as problematic*. It is for the CNIL hereby essential to know whether these traces left in various places can, after analysis, be compared with the biometric reference data kept in the databases by controllers. The *storage of biometric data in databases is hereby perceived as problematic* and the storage on a protectable object such as a smart card or PC therefore is preferable.[194] The traces become also less reliable, because they can be found by anyone from anyone everywhere.[195] Second, fingerprint is comparable with the national registry number, in France called NIR ('*numéro d'inscription au répertoire'*); both contain a real risk that the *purposes and finality of data bases become loose*. The CNIL hereby referred in particular to the risk that the databases with the biometric data become accessible and *will be used by police*.[196]

For the same reason, the CNIL has in 2007 approved five biometric systems, based on the use of veins in fingers, for access control. Because such veins are 'hidden', it is according to the CNIL not possible to collect such information without the knowledge of the person involved, and such biometric information could therefore be stored in a database.

The CNIL also authorized in 2007 for the first time the use of another at that time rather uncommon biometric systems for access control, i.e. the use of a voice recognition system for employees of the company Michelin who wanted to renew their password.

---

[192] CNIL, 21e rapport d'activité 2000, chapter 4, 101 – 120 (328 p.), available at http://lesrapports.ladocumentationfrancaise.fr/BRP/014000460/0000.pdf
[193] *Ibid.*, 104.
[194] *Ibid.*, p. 108.
[195] CNIL, 21e rapport d'activité 2000 : '*Sans doute, l'empreinte digitale présente-t-elle, à la différence d'autres caractéristiques, une spécificité : elle est le seul élément biométrique qui soit omniprésent (…) A cet égard, l'empreinte digitale est presque aussi redoutable que les traces ADN'*, p.102.
[196] *Ibid.*, p. 108.

*The CNIL on the type of storage of the biometrics identifiers*

The CNIL makes a distinction between biometrics applications where the biometric data is stored on a device under the control of the data subject or is under the control of a third party. In the first case, the individual stays in control of the biometric data. If the device were to be stolen or lost, it would not be possible to identify the data subject without his prior knowledge. On the contrary, when the data is stored by a third party, unlawful intrusion into the system will generally lead to access to biometrics data and to the linked identity. Risks of function creep and ID theft are thus higher and security measures should be reinforced.

As a way of example, the CNIL is more willing to authorise devices where the fingerprint is exclusively stored on an individual carrier, e.g. a chip card, an USB key, than systems relying on a centralised database. [197]

This interpretation has led the CNIL to prefer biometrics applications based on the storage of information on individual carrier. Only a strong need for security may justify the second option under very specific conditions (see also *below*).[198]

*The CNIL and its position on the purpose of the processing*

The CNIL will check the compliance with the proportionality principle with regard to the purpose itself, i.e. weighing the legitimate interests of the employer when using a biometric system against the employee's right to privacy, and with regard to the means used to achieve this objective. Solutions will differ depending on the type of system used (if the individual remains in control of the biometrics data stored or not) and the type of biometric identifier used.

In that sense, the use of biometrics applications based on fingerprints and which require the storage by a third party is in principle banned in this context, except when an important significant security interest is at stake. As a way of example, the CNIL authorised in 1997 the French national Bank to implement a control access system based on fingerprint for the access to highly secured areas.[199] By the same token, Roissy Airport has been authorised to use such system to access restricted safety areas of the airport.[200] On the contrary, authorisations have been denied to systems of this kind for purposes access control and working hours monitoring due to the fact they were not based on any significant security motive.[201]

---

[197] CNIL, *Biométrie : l'autorisation de la CNIL est obligatoire!* Press release, 5 January 2007, http://www.cnil.fr/index.php?id=2166&news[uid]=421&cHash=2bd711454d.
[198] CNIL, *Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 28 December 2007.
[199] See above at footnote 179.
[200] CNIL, Decision n°04-017 of 8 April 2004.
[201] CNIL, Press release, *Biométrie : quatre refus d'autorisation d'utilisation des empreintes digitales*, 30 January 2006, available online at http://www.cnil.fr/index.php?id=1938&news[uid]=304&cHash=4fe9a32a5e

*Negative opinion on a central database for biometric passport*

On 11 December 2007, the CNIL issued a negative advice on the proposed legislation for biometric passports.[202] The CNIL stated that such central biometric database for French citizens can only be justified for a strong requirement of security or public order. The CNIL deems the purpose of the delivery or renewal of passports not a sufficient reason to keep the biometric data stored in a central database.[203] The advice of the CNIL however is not binding and was not followed.

*Criteria for the use of fingerprint stored in a database*

On the 28th of December 2007, the CNIL has clarified in a communication the criteria that it applies for an authorization for biometric systems using fingerprint with storage other than on card, i.e. in the reader-comparator or on a central server. In 2007, the CNIL received 53 of such requests for authorization involving fingerprint, and rejected 21 of such requests.

The CNIL stated in its communication that the published criteria should help the companies and the administrations to ask the 'right questions with regard to technology and human rights' before deciding to install biometric fingerprint systems and before filing a request for authorization with the CNIL.[204] In the document, the CNIL reminds the readers about the risks of fingerprint data. The CNIL reiterates that fingerprints easily leave traces, such as on glasses or on a door knob. These traces can be used by third parties without the knowledge of the individual to *identify* that person or to *commit fraud* with biometric systems.[205] The CNIL states that, in addition, if fingerprints are stored in a central place, such as in the fingerprint terminal of a biometric system for the reading and comparison of the data or in a central database, the individual loses control over his biometric data and the risks of abuse of the fingerprint data are increasing considerably. Further, the identification functionality capability of the biometric data[206] implies that the privacy rights of an individual are more intruded. Therefore, the CNIL is of the opinion that 'only *an important necessity for security reasons*' may justify the storage of fingerprint data in a fingerprint terminal or central data base[207] and that this technology shall only be used as a matter of 'exception'.

The four criteria are for the CNIL the following:

1) Finality criterion: The use of digital fingerprint systems with storage in a database shall '*be limited to the access control of a limited number of persons to a well defined area*

---

[202] See above at footnote 175 ; See also CNIL, *Passport biométriques : la CNIL reservé sur la création de la première base de données biométriques relatives aux citoyens français'*, 5 June 2008, available at http://www.cnil.fr/index.php?id=2428 ;the French DPA issued in 2005 also an opinion on the electronic passport, which included at that time only the digitalised picture but no fingerprint (see CNIL, Opinion N° 2005-279 of 22 November 2005 available at http://www.cnil.fr/index.php?id=1916&news[uid]=300&cHash=3e013e7d09 )

[203] CNIL, Opinion N° 2007-368 of 11 December 2007, p. 3.

[204] CNIL, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 28 December 2007, 12 p., available at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf ('*Communication central storage fingerprint'*).

[205] *Ibid.*, 4; see also *D.6.1. Forensic Implications of Identity Management Systems*, M. Meints and M. Gasson (eds.), Fidis 9 January 2006, p. 28 *et seq.*, available at www.fidis.net.

[206] See also E. Kindt and L. Müller, *o.c.*, p. 13.

[207] *Communication central storage fingerprint*, p. 5.

*representing or containing a major stake which surpasses the strict interest of the organisation and which relates to the protection of the (1) physical integrity of persons, (2) the protection of goods and installations or of (3) information'*[208] (underlining added).

The CNIL gives some examples for each of the categories defined above: (1) *physical integrity of persons:* the use as access control to places with risks of explosion or with dangerous goods, or with risks of theft of such goods (e.g., access to specific zones of nuclear installations or cultivation of vaccines, but also access to use of elevating vehicles); (2) *protection of goods and installations:* The use as access control to specific area's which could incur irreversible and important damages going beyond the strict interest of the organisation (e.g., a company engaged in national defence), and (3) *information.* The use of access control to information which need to be protected in particular because of the risks of divulgation, other use or destruction (e.g., to rooms of a company classified and producing goods restricted for exportation, but also to the rooms of an intellectual property advisor).

2) Proportionality criterion: The use of digital fingerprint systems with storage in a database shall '*be well suited or the best suited for the finality that has been determined before'*.

This criterion requires that one shall check (a) whether non-biometric access control systems could provide a sufficient or equivalent level of security and (b) the reasons for use in a database (instead of storage on card). Whether *access* has to be secured *at all times* and without delay could play a role, as well as to whether the number of persons in the database is limited.

3) Reliability and the security of the biometric system; and

4) Information and transparency for the data subject: The use of digital fingerprint systems with storage in a database shall be made transparent for the individuals concerned. The CNIL hereby refers to the general information obligation as set forth in the data protection legislation.

The CNIL hereby also states that if these individuals are employees, the representative organisations of these employees need to be consulted in accordance with the requirements of labour law.

None of the criteria above will solely determine the legality of the system. The CNIL will finally always take the state of the art of the technology into consideration.

*VIS and SIS II*

The CNIL is also concerned about the establishment of VIS, the information system about visas. In a communication in August 2006, the CNIL shares various points made by the Article 29 working party, such as the fact that data collected for public administration purposes (so-called 'first pillar' data collection) is used for the prevention and the combat against crime (so-called 'third pillar').[209]

*Other*

---

[208] *Ibid.,* 7.

[209] See CNIL, *Système d'information sur les visas VIS : dernières négociations avant la mise en oeuvre de la plus grosse base d'empreintes digitales au monde*, available at http://www.cnil.fr/index.php?id=1773

The CNIL will also shortly issue guidelines on the use of facial recognition and video surveillance (to be further checked).

Finally, The CNIL started awareness campaigns in order to inform people, inter alia pupils in schools, about the importance of data protection.

## 4.6 Conclusion

France is one of the first countries to adapt its data protection legislation to the risks of biometric systems. The law expressly states since 2004 that biometric systems employed in the private sector need to be *prior checked and authorized* by the CNIL, unless the controller files a declaration under a simplified procedure that the system conforms to one of the 'unique authorizations' issued by the CNIL. Such 'unique authorizations', of which three were issued for biometric applications 2006 were deemed useful, also in the interest of the CNIL, because of the high demand for review of biometric systems.

The French CNIL has furthermore developed since quite some time its views and position on the use of biometric systems in France. Long before 2004, the CNIL clearly indicated its preference for biometric systems which deploy characteristics which do not leave traces (such as hand geometry, and more recently vein analysis of fingers). In case fingerprint is used, such should according to the CNIL only be stored on a card under control of the data subject. The central storage of biometric data is only proportional in case the criteria forwarded by the CNIL in its communication of December 2007 are met.

The opinions and the unique authorizations of the French CNIL provide many elements for the review of the proportionality of biometric systems, including the central storage of biometric characteristics which do leave traces, such as fingerprint. These criteria certainly provide guidance in determining the proportionality of a system, while other criteria remain more disputable. The finality criterion for central storage of fingerprint, for example, does not clarify much as to whether the verification or identification function is permitted or about the error rates of the system. Another criterion on the same subject matter is whether there is a need for access in urgent cases without delay, which seems to contradict the need for a biometric (restricted) access control. The unique authorizations, for example, also do not impose alternative means for the data subjects in case they would not consent or if the system fails. In any case, a request for authorization is subject to a *factual analysis* of each case, where an outcome is sometimes hardly predictable.[210] Further clarifications and harmonization with the guidelines of other CNIL would therefore be welcomed. The unique authorizations give more certainty, but in that case, strict observance of all criteria are necessary, but may not always be fit in a particular case.

[210] For example, the use of fingerprint in a centralized system for access control to and for the use of lifting devices was accepted by the CNIL while access to rooms where uniforms are manufactured was not deemed proportional by the CNIL.

# 5 Germany

## 5.1 Introduction

One of the first steps towards the use of biometrics by public authorities in Germany goes back to January 2002 when the German government adopted an act against terrorism (*'Gesetz zur Bekämpfung des internationalen Terrorismus') ('TBG'*).[211] The TBG was passed to enable the use of biometric characteristics in passports and identity cards for German citizens as well as in identity cards for foreign citizens.[212]

When the European Union agreed on the inclusion of biometrics in the electronic passport by Council Regulation No 2252/2004, Germany was among the first countries in Europe to issue a travel document containing a digital facial image as a biometric characteristic of its holder (*Elektronische Reisepass, ePass*) in November 2005. In June 2007, the German government decided on the inclusion of finger scans. As a result, the second generation electronic passports, including the fingerprint identifiers as well, have been issued since November 2007.[213] Even though the above Council Regulation does not apply to identity cards, Germany will include biometric data on its yet to be introduced electronic Identity Card (*Elektronischer Personalausweis*) as well.

The use of biometrics in the German private sector, however, has gone more undocumented. At the same time, compared to other countries, there have been some stakeholder efforts to make reliable information accessible. Producers have worked together to make information about biometric products available to the public. One of the results is a geographical map that is available on line and that allows consumers to access information and to find expert advice.[214] It is obvious that there are a large number of German firms selling biometric applications successfully.[215] Germany is the largest market for biometric products, according to BITKOM (the German Association for Information Technology, Telecommunications and New Media).[216] The German market showed sales of 100 million Euros (US$126 million) in

---

[211] *Terrorismusbekämpfungsgesetz* [Act against terrorism] of 9 January 2002 (BGBl. I S. 361, 3142), modified by Article 2 of the Act of 5 January 2007 (BGBl. I S. 2), available at http://www.buzer.de/gesetz/4197/

[212] T. Petermann, S., Scherz, and A. Sauter, 'Biometrie und Ausweisdokumente' [Biometrics and Identification Documents], *TAB Arbeitsbericht*, issue 93, 2003, p. 11. See for example article 7 (1) (b) and article 8 (1) in the aforementioned act, available at <http://217.160.60.235/BGBL/bgbl1f/bgbl102003s0361.pdf>, last consulted 18 March 2009. See also TAB working report 76, *Biometric Identification Systems*, available at http://www.tab.fzk.de/en/projekt/zusammenfassung/ab76.htm

[213] There is an abundance of literature on the introduction of biometrics into the German passport. For some authoritative sources see: A. Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizitat im elektronische Rechtsverkehr und Personlichkeitsschutz, Nomos, Baden-Baden, 2003; G. Hornung, 'Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues', *European Public Law*, vol. 11, issue 4, 2005; H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock, *White Paper zum Datenschutz in der Biometrie*, 2008, available at http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf. See also the implementation by the German home office, available at http://www.interoptest-berlin.de/pdf/Elbel_-_Experiences_in_introducing_the_new_German_ePassport.pdf

[214] See http://www.enisa.europa.eu/doc/pdf/studies/GermanLandscape_of_Stakeholders.pdf and www.bitkom.org/files/documents/Flyer_Landkarte_Biometrie_-_V6.0_de.pdf; Compare with P. De Hert and A. Sprokkereef, *The Use of Privacy Enhancing Aspects of Biometrics: Biometrics as a PET (privacy enhancing technology) in the Dutch Private and Semi-public Domain*, 2009, University of Tilburg ('TILT'), pp 1-50 and the efforts of their project team to gather information in the Dutch situation.

[215] There are more than eighty large biometrics companies in Germany.

[216] http://www.bitkom.org/en/about_bitkom/42611.aspx

2005, expected to grow 25 percent annually through 2010.[217] According to market analysts at Frost & Sullivan 'the market for biometrics products is going to almost triple by 2012 from its 2008 value'[218], despite the economic situation. As can also be deducted from the information provided by the German Commissioner for Federal Data Protection and Freedom of Information[219] on notifications of handling of biometric data, a considerable number of German citizens have agreed to the use of their biometrics to obtain services.

Some examples of applications involving a large number of people include paying with your finger for example, which is used by customers at the 120 stores of a German supermarket chain.[220] At Hannover Zoo, a face recognition system is installed that allows a "smile and go" for the over 70.000 regular visitors with a season pass.[221] Smaller applications can be found in a range of settings, such as, for example, for access control purposes in nursery schools.[222]

In what follows, an attempt will be made to provide an overview of relevant legal aspects and issues relating to the use of biometrics in Germany.

## *5.2 The spreading of biometric applications*

### 5.2.1 Fields in which biometric applications are implemented

*The ePass*

As in the rest of the European Union, the traditional passports[223] in Germany are gradually being exchanged for the new digital passport, also called the ePass, in accordance with Council Regulation No 2252/2004. The Federal Parliament approved the introduction of electronic passports on 8 July 2005. Four months later the first ePass was issued with the RFID chip containing only the facial image of the holder as the biometric feature. In June 2007, the Passport Act, which will be dealt with in more detail below, was again revised and approved by the parliament in order to lay down the legal foundation for the second generation electronic passports including additional finger scans (usually two index fingers) as biometric identifiers. These second generation electronic passports were issued in Germany from 1 November 2007 on.[224] Holders of these new passports thus carry a document with a chip containing their biometric data. These finger scans *are not stored centrally* but only

---

[217] http://www.cio.com/article/26000/German_Railway_Tests_Biometric_Technology

[218] http://news.prnewswire.com/ViewContent.aspx?ACCT=109&STORY=/www/story/03-19-2009/0004991263&EDATE=

[219] http://www.bfd.bund.de/EN/Home/homepage__node.html

[220] http://www.cnn.com/2008/TECH/12/12/digitalbiz.biometrics/index.html

[221] The Zoo first introduced a finger scan system but this proved too time consuming because the most frequent groups of visitors to a zoo (children and older people) had practical difficulties having their fingers scanned. See http://www.zoo-hannover.de/zoo-hannover/en/zoo_v3/unternehmen_zoo/presse/pressedetails/presseDetails_1791.html

[222] See http://www.net-tribune.de/article/r071207-01.php Even the traditional passport could be read electronically with scanning and optical character recognition (OCR)!

[223] With traditional passports we refer to passports that in principle would not be read electronically (although such passport could be read electronically with scanning and optical character recognition (OCR)) and the passports that included already the Machine Readable Zone (MRZ).

[224] See also J-H. Hoepman *et al*.. 'Crossing borders: security and privacy issues of the European E passport', *Advances in Information and Computer Security*. LNCS 4266, 2006, Berlin, Springer, pp. 152–167.

stored on the RFID chip. This means that in case there is a suspicion that biometrics on RFID chips have been tampered with, the data cannot be compared to the originals as submitted at the moment of enrolment. The relevance of this will be discussed below. Another interesting observation is that according to German officials, the data are hardly ever read out by German authorities, as the equipment to do so is currently not present or not used.[225]

*The eID Card (Electronic Identity Card -Elektronischer Personalausweis)*

The German government has considered the advantages and disadvantages of the introduction of an electronic identity card for some time, launching a first feasibility study in 2003.[226] A second study was carried out by the Office of Technology Assessment (‘*Büro für Technikfolgenabschätzung’*), which had already submitted a first general report on biometric systems.[227] The Federal government adopted an electronic card strategy in a cabinet decision of 9 March 2005 aiming at the coordination of various projects (mainly ePass, electronic health card and the eID Card) carried out by different federal ministries.[228] As it stands, the electronic health card is not yet set to include biometric data.

The legal basis for the current paper-based identity cards (‘*Personalausweis’*) can be found in the Identity Card Act (‘*Personalausweis Gesetz’, ‘PAuswG*’). This act is in the process of being revised, in order to provide for the introduction of the proposed eID Card. On 23 July 2008, the German cabinet decided on the wording of the law proposal for the new eID Card. It was agreed that, in addition to the traditional functions (photo ID, identification document, travel document), the new card would offer *the possibility* to store biometric data (facial image/ finger scans) on the microchip. By including biometrics, the *use of the new eID Card as a travel document*/passport replacement could be guaranteed whilst the new features would also improve the card’s resistance against fraud.

A draft law was presented by the federal government to the Parliament (‘*Bundestag’*) on 7 October 2008.[229] The inclusion of the facial image will be mandatory while the inclusion of the *finger scans will be at the discretion* of the card holder.[230] The card can store two finger scans, but only when the holder specifically agrees. The inclusion of finger biometrics is therefore *optional*.[231] The proposed law also contains a provision that biometric data *will not be stored centrally*.[232] When the index fingers are lacking or because of physical problems the quality of the scans is not sufficient, then a thumb, middle finger or ring finger is scanned. When as a result of a permanent medical condition no good quality scan can be obtained, the scan will not be stored on the chip. Further details on the proposed eID Card can be consulted

[225] Bundes Kriminal Amt Interview in November 2008. This statement has not been checked statistically as no such data are available.
[226] G. Hornung, *l.c.*, p. 503.
[227] Büro für Technikfolgenabschätzung, ‘Biometrische Identifikationssysteme’ [Biometic Identification Systems], *Sachstandsbericht Bundestags.*
[228] IDABC, *eID Interoperability for PEGS: National Profile Germany*, available at http://ec.europa.eu/idabc/servlets/Doc?id=31524>, p. 17.
[229] http://dip21.bundestag.de/dip21/btd/16/104/1610489.pdf
[230] IDABC, *eGoverment Factsheet Germany*, available at < http://www.epractice.eu/factsheets>, last consulted 11 December 2008, p. 23 (‘IDABC, *eGoverment Factsheet Germany’).*
[231] See the proposed addition to the Personalausweis Gesetz: § 1 Abs. 4 bis 5 PAuswG.
[232] § 1 Abs. 5 second sentence PAuswG. Section 1, para 5 (9) reads that the left and right index finger will be scanned and that the scans will be stored on the chip.

in the draft law as presented by the federal government to the national parliament (*Bundestag*) on 7 October 2008.[233] The revision will come before Parliament in 2009,[234] while the first eID Card is expected to be issued on 1st November 2010.[235]

*eGovernment services*

The eID Card will be the universal token for authentication and identification on the Internet for eGovernment and eBusiness services. The introduction of the eID Card can be considered as an important prerequisite for the eGovernment 2.0 programme, Germany's eGovernment strategy.

For the purposes above, features for electronic authentication and for digital signatures will be implemented. The chip of the eID Card will also contain certificates to prove these data. Data from the chip can only be read if the holder agrees by entering a PIN beforehand (multi factor authentication). As the card shall be used for authentication in the private sector as well, and because in different contexts different parts of the total data are necessary, there will be a function to allow *the holder to control which data can be read* in a specific situation. For example, when an age check is required, only the data from the age field can be read. The new identity card thus offers possibilities of an electronic identity proof for eGovernment and eBusiness applications. The new eID Card will also contain a *pseudonym function*. The central idea is that the individual card number is used to generate a pseudonym that cannot be reconverted mathematically into the original card number. This pseudonym could then be used to register at, for example, eBay, or any other web service that requires personal identification. Section 4 of the proposed modifications is devoted to the use of the eID Card as an electronic signature. The use is limited by the following conditions: (1) the objective for using the electronic signature is not illegal, (2) the data transmitted are not used for commercial gain, (3) the service provider has justified the necessity of using the data for the goal of the transaction, (4) data protection law is adhered to, (5) and there are no indications that data abuse might take place. (par.2 (1) – (5)).

On 29 January 2009, the German government approved its eGovernment implementation plan.[236] It presents the government's view of an innovative and modern public administration with eGovernment. It provides a detailed overview of the progress achieved in 2008. For public authorities to provide on-line services to citizens based on biometric technologies, administrative law (*'Verwaltungsgesetzgebung'*) such as the social codes (*'Sozialgesetzbücher'*) which regulate the processing of social and medical data has to be applied. Of the thirty-two eGovernment projects, some are concerned with the identification with the Electronic Office ID Card. In section 3.3.2. the plan is detailed on how to test the ID card and how to attract a maximum of interested parties to make the use of the ID card for

---

[233] See *Entwurf eines Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften*, Bundestagsdrucksache 16/10489, available at http://dip21.bundestag.de/dip21/btd/16/104/1610489.pdf

[234] http://www.typotype.de/news-und-faqs/news/latest/bundesrat-gibt-gr-nes-licht-f-r-den-elektronischen-personal ausweis.html

[235] IDABC, *eGoverment Factsheet Germany*, p. 23.

[236] Bundesministerium des Inneren, *Umsetzungsplan 2009, E-government 2.0. Das Program des Bundes*, Berlin, 2009 (,*Umsetzungsplan'*), available at http://www.cio.bund.de/cae/servlet/contentblob/325318/publicationFile/16655/egov2_umsetzungsplan_2009_download.pdf (*'Umsetzungsplan')*

electronic services as attractive as possible. The implementation plan confirms that the date for introducing the new card is 1st November 2010.[237]

*Other domains*

Apart from the large scale public authorities initiatives mentioned above, various private initiatives use biometrics such as casinos and most notably many companies use biometric access control and time registration.[238] The latter will be touched upon in more detail below.

In the semi-public domain, biometric applications are used in various places. For example, Deutsche Bahn has tested a facial recognition system at Mainz train station. Special cameras scanned the train station in search of 200 people who have volunteered to have their pictures stored in a database whose features can be detected by special biometric facial recognition software.[239] All these initiatives have been reported to the German data protection authority, but very little is known about the extent to which they comply with the Directive 95/46/EC and German legislation in practice. There is some case law regarding the use of biometrics at work (see below), but we have not come across other case law specifically dealing with the use of biometrics.

### 5.2.2 National studies and debate about biometrics

We have already mentioned that a national report on biometric identification systems was commissioned in 2003.[240] This was followed by a clear guide on how to use biometrics in private organizations and companies issued by the Teletrust organization in 2005.[241] In 2008, the Teletrust organization also published a white paper on data protection and the use of biometrics.[242] The recommendations of the report concentrate *on the use of privacy enhancing features* of biometrics:

> 'A solution that does justice to data protection should contain the following characteristics:
>
> The complete biometric part of the application, containing a sensor, characteristic extraction (template), and data reference storage, is *under the direct control of the user*.

---

[237] *Umsetzungsplan*, p. 61.

[238] See also Unisys, *Biometrics in Europe: trend report*, available at http://www.europeanbiometrics.info/images/resources/121_975_file.pdf , last consulted 11 December 2008, p. 32.

[239] See also the reference to the research project at footnote 66 and http://www.cio.com/article/26000/German_Railway_ Tests_Biometric_Technology

[240] Büro für Technikfolgenabschätzung, 'Biometrische Identifikationssysteme', *Sachstandsbericht Bundestags*, 2003.

[241] Teletrust, *Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme* [Guideline for the employment of a biometric system], 21 September 2005, available at < http://www.teletrust.org/uploads/media/ag6_ak-recht_orientg-betriebsvbg-biometrie_1.2.pdf>, last consulted 25 March 2005. TeleTrusT is a non-profit organization dedicated to the promotion of trustworthiness of Information and Communication Technology. It was founded in 1989 and comprises members from industry, science and politics.

[242] H. Biermann, M. Bromba, C. Busch, G. Hornung, M. Meints, G. Quiring-Kock (eds.) *White Paper zum Datenschutz in der Biometrie*, 2008 (*'White Paper zum Datenschutz in der Biometrie'*), available at http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf . Both the guide and the white paper were edited by a working group with support from the German Data Protection Authorities from the Federal and the State level.

> To realise this goal, the biometric part of the system is *stored on a token* which does not leave the control of the user. The biometric section of this card is *completely separate* from the data handling activity of the system. The latter has been protected with strong encryption and will produce no, or only the minimum of data, as necessary in the particular situation. The validity of the certification used will be confirmed by a third trusted party (for example a Trust Centre) for every transaction. This way, illegally obtained tokens can be "de-activated". With the use of a token will the advantage of being able to authenticate without having to carry or remember things. On top of these requirements it can be noted here that there are several other privacy enhancing application that work in individual situations and provide possibilities for secure data handling.' (stress added) [243]

In 2005, BITKOM[244] conducted a study to develop a strategy for the German biometrics industry, and set up a national working group concerned with biometric issues, called *German Biometric Strategy Platform*. The study included the assessment of requirements, objectives, tasks and member structure of the German Biometric Strategy Platform.[245] The report states that the two most important international factors influencing the German biometric industry are international *standardization* and *security policy efforts*.[246] According to the report, the German federal government is the most important driver for biometric technologies in Germany. It takes a position as promoter and customer – on the one hand it seeks to support the industry with a national, seller-independent economic policy, and on the other hand it is expected to be the first major German customer for biometric applications. Moreover, federal and Länder authorities are involved in the biometric standardization process.[247] The six most important federal institutions involved in biometrics identified in the report are:

- the Federal Ministry of the Interior ('*Bundesministerium des Innern', 'BMI'*) mainly concerned with ID document safety and smart cards,
- the Federal Border Police ('*Bundesgrenzschutz', ,BGS'*) the Automated Biometric Border Control ('*Automatisierte und biometriegestützten Grenzkontrolle'*) at Frankfurt airport,
- the Federal Office for Information Security ('*Bundesamt für Sicherheit in der Informationstechnik', 'BSI'*). The BSI is involved in testing biometric applications, standardization and representative work in international bodies,
- the Federal Criminal Police Office ('*Bundeskriminalamt*', *'BKA'*) coordinating the AFI-systems (Automated Fingerprint Recognition System) for criminal prosecution purposes,
- the Federal Ministry for Economics and Labour ('*Bundesministerium für Wirtschaft und Arbeit', 'BMWA'*) involved in stimulating the economical development of the biometrics industry, and

---

[243] *White Paper zum Datenschutz in der Biometrie*, p. 25 (free translation by the authors).

[244] BITKOM represents more than 1,300 companies with combined sales of more than 120 billion Euro, with 900 direct members and around 700.000 employees, including practically all German global players as well as 600 key midsize companies in the information technology, telecommunications, and new media industry. The association's services comprise political consulting, public relations, knowledge management and other customized services.

[245] BITKOM, *The German Biometric Strategy Platform: Biometric State of the Art, Industry Strategy Development and Platform Conception*, Berlin, 2005, available at http://www.europeanbiometrics.info /images/resources/95_363_file.pdf ('BITKOM, *The German Biometric Strategy Platform')*

[246] BITKOM, *The German Biometric Strategy Platform*, p. 24.

[247] *Ibid.*, p. 35.

- the Federal Ministry of Education and Research (‘*Bundesministerium für Bildung und Forschung’, ‘BMBF’*) which provides research support.[248]

The report was very ambitious, and many of the facts and figures it brought together very useful, but it seems that the strategy has not worked. The *German Biometric Strategy Platform* has not become a major player in the field.

Many studies on the introduction of biometrics in Europe lament the lack of debate.[249] In Germany, Hornung also observes an absence of a widespread public debate before the European Regulation 2252/2004 was adopted. Deliberations have occurred in several hearings[250], but this has not resulted in a decision from the *Bundestag* on the issue. The *Bundestag* had nevertheless in an earlier act reserved itself the right to decide on the issue.[251] At the same time, there has been some organized assessment and there have been public discussions. So on a scale indicating level of public discourse or debate in Europe, Germany would do relatively well.

Compared to other countries, the public perception of biometrics in Germany is also strongly influenced by ethical questions.[252] This translates itself also into a more principled stance on the use of biometrics. The clearest example of this is a general agreement on the fact that a central database containing biometric data would be unconstitutional and be a violation of basic rights.[253] The possibility of a *nationwide database has already been ruled out by the German legislation* relating to the ID card.[254] The compatibility of the idea of a central data base with the German Constitution will be discussed further below.

## *5.3 Legislation regulating the use of biometric data*

### 5.3.1 General and specific privacy legal framework for biometrics

Three so-called ‘first pillar’ instruments govern the EU data protection framework: the general Directive 95/46/EC which has been implemented in Germany through the Federal Data Protection Law (‘*Bundesdatenschutzgesetz’, ‘BDSG’)* [255], the specific Directive 97/66/EC[256] concerning the processing of personal data and the protection of privacy in the telecommunications sector (replaced by the privacy and electronic communications Directive

---

[248] *Ibid.*, p 35.
[249] See J. Ashbourn, *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies*, European Commission, DG JRC, Sevilla, 2005.
[250] See the Bundestagsdrucksache No. 15/3145, 9; 15/3642, 12 ff.; 15/3663, 3; 15/3765, 4 f.; 15/4211, 7 ff.; 15/4477, 8 f., 17 ff).
[251] Sec. 4 (4) Passport Act (Passgesetz). See Hornung, *Die digitale Identität* [The Digital Identity], 173 ff.; Hornung, *Biometrische Systeme* [Biometric Systems], 355 ff.
[252] BITKOM, *The German Biometric Strategy Platform*, p. 24.
[253] See also Z. Geradts, ‘Forensic implications of identity systems’, *Datenschutz und Datensicherheit*, 2006, 30, pp. 556–558.
[254] §1 (5) of the German Gesetz uber Personalausweise of 21st April 1986 (Bundesgesetzblatt I, 548), as amended (‘Personalausweisgesetz’), available at http://bundesrecht.juris.de/persauswg/BJNR008070950.html .
[255] This act came into force in 1977 and was revised in 2001 to integrate the Data Protection Directive 95/46/EC into the German framework. For a translation of the Act see: http://www.iuscomp.org/gla/statutes/BDSG.htm
[256] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector; *O. J.* L 024, 30 January 1998, pp. 1-8

2002/58/EC)[257] transposed in the Telecommunications Act (‘*Telekommunikationsgesetz’*, ‘*TKG’*) and the Regulation No 45/2001 of the European Parliament and of the Council of 18 December 2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data.[258]

As stated above, the Directive 95/46/EC constitutes the main and general legal framework for the processing of personal data. For a general discussion of the provisions of the Directive in relation to biometrics see the general section above.

In Fidis deliverable D3.10, it was already highlighted that national regulators have a considerable margin of appreciation when evaluating biometrical issues. This can be explained by the fact that most national data protection laws implementing the Directive 95/46/EC contain no specific provisions or criteria on the processing of biometric data.[259] This observation certainly applies to the German legal framework that contains no specific laws or regulations on the use of biometrics. The most important general requirement is the protection of human dignity according to Article 1 of the German Constitution (‘*Grundgesetz’* ‘*GG’*). This article stipulates that ‘Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority’.[260] Furthermore, in Germany, as elsewhere in Europe, the application of biometrics is predominantly governed by general data protection laws.

In Germany, the Federal Data Protection Law, controls the storage, processing and use of personal data collected by public federal and state authorities and by private parties, the latter in case they process and use data for commercial or professional aims. The Federal Data Protection Law is the most important law for the processing of biometric data and contains rights and obligations with respect to data protection. The Federal Data Protection Law stipulates the following principles: proportionality, purpose specification, and data reduction and data economy. This means that it has to be guaranteed that only data are collected or used, which are necessary and which are permitted by the law.[261] Although there is no German case law dealing specifically with the handling of biometric data, there is some publicly available data protection advice on the application of the various laws to biometrics and the choices that can be made for privacy enhancing variations of the technology.[262]

---

[257] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O. J.* L 201, 31 July 2002. Article 3 §1 states: ‘This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community’.

[258] *O. J.* L 8, 12 January 2001.

[259] Kindt, E. and Müller, L. (eds.), *o.c.*,

[260] http://www.iuscomp.org/gla/statutes/GG.htm

[261] For more details, see section 2 of this deliverable or E. Kindt, l.c, , *Datenschutz and Datensicherheit (DuD)*, 2007, 31, pp. 166-170.

[262] See the publications by Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, available at https://www.datenschutzzentrum.de/projekte/biometrie/kap6krit.htm; https://www.datenschutzzentrum.de/projekte/biometrie/index.htm; see also Datenschutz Berlin, available at http://www.datenschutz-berlin.de/content/themen-a-z/biometrie/biometrische-authentisierung; and the website of: http://www.datenschutz.de/. In addition, and apart from FIDIS publications, see other academic literature, for example, L. Donnerhacke, ‘Anonyme Biometrie’, *Datenschutz und Datensicherheit* 1999, Vol. 23 , Nr. 3, S. 151-154; M. Köhntopp, ’Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren’, Horster (ed.), *Sicherheitsinfrastrukturen*, Vieweg, Braunschweig 1999, sections 177-188; A. Pfitzmann et al., ’Trustworthy User Devices’, Müller and Rannenberg (eds), *Multilateral Security in Communications*, Addison-Wesley, München 1999, sections 137-156.

Finally, the German Constitution (*'Grundgesetz')* includes the right to informational self-determination (*'Recht auf informationnelle Selbstbestimmung'*). At first it was argued by most commentators, that a central database (or its de-central equivalents) would be incompatible with this right.

However, the strict legal interpretation of this principle seems to come under some pressure.[263]

One significant and recent case on the issue of central storage of personal data of the European Court of Justice relates to a preliminary question of a German court. The background, the Court's reasoning and the implications of the case have been discussed above in section 2.3. The German Act relating to a Central Register of Foreigners Act **('***Gesetz über das Ausländerzentralregister***')**[264] has established a centralised register which contains certain personal data relating to foreign nationals who are resident in Germany for a period of more than three months. From 2005, The Federal Office for Migration and Refugees (*'Bundesamt für Migration und Flüchtlinge'*) is responsible for maintaining that register.[265] There are around 7 million permanent inhabitants in Germany that do not have the German nationality. The register is used for statistical purposes by security and police services and judicial authorities in exercising their powers in relation to the prosecution and investigation of criminal activities which threaten public security. In its ruling, the Court of Justice stated in an answer to the preliminary questions that the centralisation of the data does not satisfy the requirement of necessity laid down in the Directive 95/46/EC.

### 5.3.2 Legal provisions for government controlled ID biometric applications (passports, other civil ID biometric applications and law enforcement)

The design and the use of the identity card and passport are regulated in respectively the Identity Card Act (*'Personalausweis Gesetz', 'PAuswG'*). and the Passport Act (*'Passgesetz')*, which have already been discussed to some extent above.[266]

With regard to biometrics, Article 7 of the Act against terrorism (*'TBG'*) (see *above*) adds a new paragraph 23a to the Passport Act that allows the use biometrics in the German passport.[267]

The authorities responsible for the identity cards (the citizen's registration offices at the *municipality level*) keep records on identity cards.[268] Among others, these local registries issue the identity cards and verify their authenticity. Every identity card has a unique serial

---

[263] G. Hornung, 'The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards', *SCRIPTed* vol. 4, issue 3, 2007.
[264] *Gesetz über das Ausländerzentralregister* (**'**AZR-Gesetz') of 2 September 1994 (BGBl. I S. 2265), recently modified by Article 2 of the Act of 26 February 2008 (BGBl. I S. 215). See http://www.gesetze-im-internet.de/bundesrecht/azrg/gesamt.pdf
[265] See http://www.bamf.de/cln_092/nn_441806/sid_4914EA581C5A6781FB012BA5814E3264/SharedDocs/Pressemitteilungen/DE/DasBAMF/2005/050629-pressemitteilung-07-05-bamf.html?__nnn=true
[266] For the full text of the Act In German, see http://www.gesetze-im-internet.de/pa_g_1986/index.html
[267] See also Article 11 TBG which changes the foreigner law (Ausländergesetz, AuslG) and provides for the integration of biometrics in visas and residence permits of foreigners.
[268] § 2a of the Identity Card Act.

number. It is explicitly forbidden to use this number for accessing personal data in files or for linking data in different files.[269]

The by the Passport Act regulated passport register is controlled by the passport authorities (again, the *citizen's registration offices at the municipality level*). They issue passports and verify their authenticity, as well as the identity of the person who owns the passport or for whom it has been issued. Besides authorisations for respective police, customs and registration authorities, the Passport Act explicitly stipulates that the use of biometric data is strictly *limited to verification and authentication* of the passport and the identity of the holder (purpose specification).[270] Careful reading indicates that the fingerprint data are not stored on a database, but only on the passport itself.[271] In the future, only other Nations granted permission by the Federal Republic of Germany (in the form of a special cryptographic certificate to be used in electronic Passport reading devices) will be able to access the microchip's data of the ePass.

As already mentioned above, *a nation-wide database*, hence not only a biometric database, is *explicitly forbidden by the legislator in the German Passport Act (§ 4 (3)).*

Biometric facial data can be preserved in a local database.[272] As regard to fingerprints, the 2007 revision of the Passport Act stipulates that finger scans are to be stored exclusively on the passport's microchip, and that they should in no case be stored locally or in a central database. Subsequent the scanning and use of the finger scan data the authorities are obliged to delete the data.

### 5.3.3 Biometric systems and the privacy rights of employees

German companies increasingly base their security systems on biometrics, for example to organize workplace and network access control.[273] Notwithstanding this development, Germany does not have a specific employee data protection law. The two laws that govern the use of biometrics are therefore the above mentioned Federal Data Protection Law together with the Codetermination Act ('*Betriebsverfassungsgesetz', 'BetrVG'*). [274]

The Federal Data Protection Law stipulates a general prohibition on the use and processing of personal data.[275] This is accompanied by an exception clause making it permissible only in case of a legal basis or an explicit consent of the parties concerned. Moreover, the German Federal Office of Health ('*Das Bundesamt für Gesundheit', 'BAG'*), and the German labour court ('*Bundesarbeitsgericht'*),[276] issued a decision in 2004 making the introduction and use

[269] § 3 of the Identity Card Act.
[270] § 16a of the Passport Act.
[271] See § 4 (3) in connection with § 16a of the Identity Card Act; see also http://dip21.bundestag.de /dip21/btd/16/104/16104 89.pdf The digital face picture, however, will be stored by the citizens register in the same way as a second paper based photo was stored in the past.
[272] Most of these local databases, the citizens registers, however, would be centrally accessible via an XML-interface. So technically there is no big difference to a central database in case of an authorised access e.g. by police forces e.g. in cases of ongoing investigations is needed
[273] E. Schedel, 'Mitbestimmung bei biometrischen Kontrollen' [Codetermination with respect to biometric control], *C't magazin für computertechnik*, vol. 21, issue 4, 2004, p. 39.
[274] For the full German text see: http://bundesrecht.juris.de/bundesrecht/betrvg/gesamt.pdf
[275] § 4 section 1 of the FDPL.
[276] Decision of 27 January 2004, 1 ABR 7/03.

of biometric systems within the working environment subject to the codetermination rights of employee representatives such as the works council and trade unions.[277]

Biometric technology used at work falls within the scope of informational self-determination. As already discussed above, the right on informational self-determination is embodied in the German Constitution (*Grundesgesetz*) in articles 1 and 2. It includes the right to decide and know where one's personal data is captured, stored and used.[278] The submission to the codetermination regime derives from the Codetermination Act itself, namely that biometric technologies are intrinsically linked with issues concerning work rules and behaviour of employees ((§ 87 I 1 Codetermination Act).

Consequently, an agreement – usually the employment agreement - will provide a legal basis for the collection, processing and use of personal data in case a biometric application is installed by the employer. In this agreement, it must be specified precisely, among others, what the purpose of the biometric application is. In addition, it should indicate whether verification or identification takes place, whether raw data or templates are used, whether data is stored, and, if so, whether this will be in a decentralized or a central database. There are also clear rules about preference for use of chips on card from a data protection point of view.[279]

The employees – usually represented by the works council (which may be supported by trade unions) – and the employer will have to take into consideration their respective interests during the negotiations before they sign the agreement. In specific cases, the security interests of the employer will have to be weighed against the affected privacy rights of the employees in an appropriate way. In particular, the question has to be addressed whether the use of the biometric application is necessary in view of the purpose it is expected to serve. Purpose binding should take place in the context of a proportionality test. This means that biometric applications which potentially interfere with the right to informational self-determination require a justified interest of the employer in each case. Of course, the more privacy enhancing alternatives of for example Type II access control systems should be carefully explored in the interest of the employee.[280]

## 5.4 The Supervising Authorities

The federal oversight is executed by the Federal Data Protection and Freedom of Information Commissioner who controls that all federal agencies comply with the data protection legislation.[281] Chapter 3 of the FDPL provides the legal basis for the Commissioner and outlines his functions. The key role is to ensure that the Data Protection Act is implemented correctly. Section 24 states that the Commissioner has to monitor compliance with the Act and grants him powers of access to information as well as the opportunity to inspect all

---

[277] G. Hornung, 'Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential' [Biometrics at the work place – secure inspection procedures versus expanding control potential], *Arbeit und Recht*, vol. 29, issue 6, 2005, p. 205.

[278] T. Probst, T., 'Biometrie aus datenschutzrechtlicher Sicht' [Biometrics from the data protection legal perspective], in Nolde, V. and Leger, L. (eds.), *Biometrische Verfahren* [Biometric procedures], pp. 115-128, Fachverlag Deutscher Wirtschaftsdients, Cologne, 2002.

[279] http://www.bfdi.bund.de/cln_007/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Chipausweise.html#inhalt

[280] *Ibid.*

[281] http://www.deutschland.de/link.php?lang=2&link_id=24

documents and the right of access to all official premises at any time. Section 25 stipulates that the Commissioner can lodge complaints with higher authorities (e.g. the competent supreme federal authority) in the case of breaches. In Section 26 it is laid down, inter alia, that the Commissioner can be requested by federal government to give opinions and make recommendations on matters pertaining to the law. The FDPL also sets out the penalties for breaches in Sections 43 and 44.1. They are fines and imprisonment.

However, as the Federal Republic of Germany is a federation of 16 States (*Bundesländer)*[282] the competences of the State are divided between the federal and the State governments. The federal system of government, with its clear division of powers between the governments of the States and the federal government also affects the supervision of data protection. Therefore, there is number of different authorities that are responsible for making sure that data protection laws and regulations are complied with. Thus German Federal States have their own DPAs, which are responsible for controlling the observance of data protection legislation by public bodies located in their jurisdictions.[283] There is no uniform system for the supervision over the private sector in the individual states. In some States, the supervisory functions are performed by the Ministry of Home Affairs or by the authorities that report to the Ministry. In other States, e.g. North Rhine-Westphalia, supervision is exercised by the DPA.[284] A private company is supervised by the authority that has jurisdiction over the district where it has its headquarters.

## 5.5 Conclusion

This country study has provided a short overview of all relevant aspects and issues surrounding the use of biometrics in Germany. Clearly, a pivotal event in this regard was the introduction of the ePass in Germany. The introduction of the passport, so soon after the EU Regulation 2252/2004, was the result of independent German government deliberations about the introduction of biometrics since 2002. Initially, the ePass contained only a facial image as a biometric identifier, but as of June 2007 the German government approved the inclusion of finger scans. As a result, the second generation electronic passports, with EAC and including the fingerprint identifiers have been issued since November 2007. The fingerprint identifiers, however, are by law stored exclusively on the passport's microchip, and not stored locally in the citizens' registers or in a central database.

The German government is also proposing to include biometric data on its new eID card, albeit on voluntarily[285] grounds. The eID Card, planned to be issued from the end of November 2010 onwards, will encompass a mandatory electronic facial image, whilst the inclusion of fingerprints will be at the discretion of the citizens. The aim is to implement the eID Card as a universal token for authentication and identification on the Internet for eGovernment and eBusiness services.

---

[282] These States ('Bundesländer') are not just provinces but states with their own original sovereign rights and legislative responsibilities.

[283] For a list see https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Datenschutzbeauftragte/Datenschutzbeauftragte.php

[284] For a list see https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Aufsichtsbehoerden/Aufsichtsbehoerden.php

[285] Voluntary in the sense that is not required by EU law.

As for the regulatory framework, there are no specific regulations or laws concerning biometrics in German law. The Federal Data Protection Law, which covers the storage, processing and use of personal data collected by public federal and state authorities and by private parties, serves as a framework for the handling of biometric data. A nation-wide database, with data relating to the passports, hence not only a biometric database, is explicitly forbidden by law (§ 4 (3) Passport Act). Biometric facial data can be preserved in a local database, while finger scans are stored exclusively on the passport's microchip thus excluding any local or central storage.

Given the fact that there are more than eighty major biometrics companies in Germany and the market for selling biometric products per capita is considered the largest in the world, it is surprising that there are no significant court cases yet.[286] On the other hand, the use of biometrics in the workplace and the weighing of privacy rights of employees has been a legal issue already. From the current public information[287] available, it is difficult to determine whether biometric technologies are used in a privacy enhancing manner in day to day routines across Germany. Therefore, in the forthcoming years we might well see individuals come forward asking for legal clarification on data protection or other aspects of biometric applications.

[286] Apart from the cases concerning the privacy rights of employees mentioned above.
[287] For sources for good practice see: FAQ referred to at many DPA websites: https://www.datenschutzzentrum.de/faq/biometri.htm and also note 62.

# 6 The Netherlands

## 6.1 Introduction

During the Dutch presidency, a consensus was built on the content of the *The Hague Programme* and the programme was adopted by the European Council in November 2004. In June 2005, the Commission presented a detailed five year programme.[288] *The Hague* set a new policy agenda and specific objectives for the next five years for developing the Area of Freedom, Security and Justice (AFSJ). The programme made the road for the introduction of biometrics, and the move towards *availability* and *interoperability* of data systems in the European Union.

The Dutch government itself had in fact already started up a policy process aiming at the introduction of biometrics in identity documents. This was five years ago. In this country report, we will first sketch the current use of biometrics in the Dutch public and private domain. We will then describe the legal framework for the use of biometrics and how this has evolved.

## 6.2 The spreading of biometric applications

We see a gradual rolling out of biometric applications in the Dutch public sector. The main government policies in this regard are the introduction of face and finger scans into the Dutch passport, identity management using biometrics within the criminal justice system (Progis)[289], and the use of biometrics for the registration and identification of foreigners (in visa, residence permits and political asylum and immigration procedures). Of these examples, only the use of biometrics in the criminal justice system is not in direct parallel with developments in the EU. All the other government applications that are being introduced have been initiated, or at least re-enforced by decisions made at EU level about machine readable documents.[290] Therefore, although the introduction is gradual, in a few years time the majority of people living in the Netherlands will have become enrolled in a government biometric application.

Over the past decade, biometric applications have spread across the Dutch semi-public and private sector. At the same time, they are not *omni* present. One of the conclusions of our recent report on the use of biometric applications in the private domain was that detailed information is very difficult to obtain.[291] We found that it proved impossible to draw up a reliable inventory of all biometric applications in the Netherlands. The Dutch Data Protection Authority (*College Bescherming Persoonsgegevens, 'CBP'*) keeps a register of all projects

---

[288] See http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf and http://ec.europa.eu/justice_ home /news/information_dossiers/the_hague_priorities/

[289] CIS (*Coordinatiegroep Informatievoorziening Strafrechtsketen*), *Protocol for establishment of identity (in law enforcement)* (*Protocol Identiteitsvaststelling (strafrechtketen*)) ('Progis'), 3 September 2008, Directie Generaal Rechtspleging en Rechtshandhaving, the Hague, 2008.

[290] P. de Hert, W. Scheurs and E. Brouwer, "Machine-readable identity Documents with Biometric Data in the EU - part III - Overview of the Legal Framework", *Keesing Journal of Documents and Identity*, 2007, No. 22, pp. 23-26.

[291] P. de Hert and A. Sprokkereef, *The Use of Privacy Enhancing Aspects of Biometrics: Biometrics as PET in the Dutch Private and Semi-Public Domain*, TILT, January 2009, p. 23 available at http://arno.uvt.nl/show.cgi?fid=93109 (last consulted 1st april 2009) ('*The Use of Privacy Enhancing Aspects of Biometrics*').

notified under the data protection legislation[292], but in the current set up, the biometric projects are difficult to count and to qualify. Detailed information is often unavailable and the circumstances under which data handling takes place are in practice unclear without further investigation.

There are private initiatives such as the Netherlands Biometrics Forum (*Nederlands Biometrie Forum*) starting a web project on the voluntary registration of biometric projects in 2007.[293] All in all, it remains unclear whether information about the spread of biometric applications in the Netherlands will become better accessible in the near future.

### 6.2.1 Fields in which biometric applications are implemented

Our estimation is that the number of private and semi-public projects using biometrics at this moment in time will not exceed a few thousand. We examined the use of privacy enhancing aspects of biometrics in less than a hundred projects, as randomly found on the Internet.[294]

Despite a lack of statistical information, it goes undisputed that the number of applications that use biometrics has increased considerably. Improved measurement methods and reliability rates, decreased physical sizes of sensors and accompanying price reductions have all played a part in this process. Biometric applications have also been integrated with other products such as cars and computers. Another observation in our report *The Use of Privacy Enhancing Aspects of Biometrics* was that companies selling biometrics have employed marketing strategies designed to create a demand.[295] It is interesting that in the German country study of this deliverable (see section 5), a supply led tendency can equally be detected. This is illustrated by a press report of a German biometrics manufacturer giving a biometric access system to a nursery school as a Christmas present.[296] In March 2008, the first Dutch schools started using biometrics as a key for personnel and parents.[297] These schools sought to acquire a biometric entry system nor did pay for it: they were offered a trial for free.[298] It is too early to conclude whether the use of biometrics in semi-public institutions such as schools in the Netherlands will mushroom over the next few years. If it will, then at least it will do so at a slower pace than in the UK.[299]

---

[292] See Article 27 of the Dutch Data Protection Act. The so-called notification duty (*meldingsplicht*) applies to all automatic data processing, with the exception of processing falling within the decision with exemptions (*Vrijstellingbesluit)*.
[293] See an announcement at http://www2.biometrieforum.nl/bio/annoucement.php?aid= 24&cid=17
[294] *The Use of Privacy Enhancing Aspects of Biometrics*, pp. 48-50.
[295] *The Use of Privacy Enhancing Aspects of Biometrics*, p. 24.
[296] See http://www.net-tribune.de/article/r071207-01.php (last accessed 28th March 09)
[297] See http://www.identysoft.nl/pers.php (last accessed 28th March 09)
[298] See *The Use of Privacy Enhancing Aspects of Biometrics*, pp. 24-26.
[299] Compare with the UK country report in the present deliverable. As far as we are aware, Dutch schools do not fingerprint pupils yet. There are schools with access control systems for parents and personnel. Library- and access control systems for pupils are already available in the Netherlands but we have not found a school that employs them. In the UK, a large number of schools were quick to take up biometric library card systems sometimes in combination with the use of the cards for school meal provision. A school meal system does not exist in the Netherlands but the reasons for a different pace may well be found in the various marketing strategies employed.

### 6.2.2 National studies and debate about biometrics

At the end of the 1990s, biometrics became a subject of discussion and the first Dutch legal academic articles were published.[300] In 1999, the Dutch Data Protection Authority published an extensive report on the privacy aspects of biometrics with the title *At Face Value*.[301] It was the result of a study performed jointly by the DPA and the Dutch Organization for Applied Research- Physics and Electronics Laboratory ('TNO-FEL'). The report concluded that designers, developers, suppliers and users of products using biometrics for identification, authentication or exposure of emotions *needed to consider ways to protect the privacy of users*. Amongst others, the report recommended the following measures to minimise or eliminate privacy risks:

> '1. Analysis of the *need for biometrical identification or authentication*. Is the application of biometrics proportional with the goal to be achieved?
>
> 2. Decentralisation of the template storage and verification process; as a rule both the storage of templates and the verification process *should be decentralised*. In some specific cases and environments, the processing of personal data can be seen as a pure personal activity.
>
> 3. Encryption of databases: the protection of personal data can be realised by using different encryption keys and algorithms to encrypt the personal data (including biometrical data) in different databases. The original biometrics should preferably be destroyed after the derivation of the *digital template*.' (stress added)[302]

The *At Face Value* report also briefly mentioned *certification* of privacy-compliance of products as a possible solution for future problems. According to the report, certification would guarantee an adequate handling of the personal data of future users.[303] The research results also included a checklist with practical directions, for those who want to build a privacy-enhanced product that processes biometrical data. It stated that personal data should be protected with proper PETs[304] and referred to crucial decisions in the design phase. In particular, it referred to decisions concerning the question whether to protect data by decentralisation of the template storage and/or verification, or encryption.[305]

---

[300] R. van Kralingen, C. Prins and J. Grijpink, *Het Lichaam als Sleutel. Juridische Beschouwingen over Biometrie* [The body as a key. Legal observations on biometrics], Samson, Alphen ad Rijn, 1997*;* C. Prins, 'Making our Body Identify for Us: Legal Implications of Biometric Technologies', *Biometric Technology Law - Computer Law and Security Report* , 1998, Vol. 14. no. 3; J. Grijpink, 'Biometrics and Privacy', *Computer Law and Security Report*, 2001, Vol. 17 no. 3, pp.154-160.

[301] R. Hes, T. F. M.Hooghiemstra and J.J. Borking, *At Face Value. On Biometrical Identification and Privacy*, Registratiekamer, Achtergrond Studies en Verkenningen 15, September 1999, 70 p., available at http://www.cbpweb.nl/documenten/av_15_At_face_value.stm ('*At Face value report*'); compare with A. Albrecht, 'BIOVISION. D 7.4, *Privacy Best Practices in Deployment of Biometric Systems* (Final Report)' 2003 and V. Andronikou, D. Demetis and T. Varvarigou, 'Biometric Implementations and the Implications for Security and Privacy', *Journal of the Future of Identity in the Information Society*, 2007 Vol. 1 N° 1, available at http://www.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf (last accessed 1st april 2009)

[302] *At Face Value report*, p. 63.

[303] *Ibid.*, p. 63.

[304] The *At Face Value* report identifies PETs as different technological elements that can help to improve privacy compliance of systems. See p. 49.

[305] See pp. 58-59 of the *At Face Value* report.

The report is still regarded as authoritative. Until now, it has not been updated. In fact most of the conclusions and recommendations, especially those on the use of biometrics as a privacy enhancing technology, are still valid. What is lacking now, are more detailed guidelines and descriptions of best practice as developed over the past ten years.

The Dutch Organization TNO-FEL mentioned above has also conducted technical studies to assess the claims made about biometrics products or processes. TNO was the first to investigate the use of fingerprint-based biometric technology on *children*. Their conclusion was that in the current state of the art (two dimensional) *fingerprint technology is impractical for children under the age of six*.[306] TNO found that facial recognition can be used for young children, although with adaptations to standard hardware.

TNO carried out research on a relatively small sample of 161 children aged from birth to twelve, with at least five children for each year of age. Fingerprints and facial images were successfully taken from all the children aged seven and over, with success defined by a NIST quality check for fingerprints[307] and a biometric verification check for the facial image. But no infants from birth to two years old could be enrolled for fingerprints, along with just 8% of three-year-olds. The fingerprint success rate rose with age, to 50% of four-year-olds, 67% of five-year-olds and 89% of six-year-olds.[308] Facial images were much more successful, taken with 77% success for the group from birth to two years, and at least 89% from all age bands above three years.

In 2008, a Telematica Institute report on government identity management examined and assessed current trends in the field, and the role of new technologies in particular. The report is brief on biometrics and concludes that the use of biometrics as PET often does not sit easily together with customer friendly identification and user comfort.[309] The unintended side effects of using biometric applications are highlighted. The side effects identified are inconvenience for citizens, certain categories of people that have physical difficulties with biometric systems (children, older people, and people without hands), possibilities for biometric identity theft, absence of 100% reliability and the impact on the use of fingerprint data in criminal prosecution.[310]

In early January 2009, a report named Our Digital Shadow (*Onze Digitale Schaduw*) was commissioned by the Dutch Data Protection Authority.[311] The main aim of the research was to assess in how many data bases a Dutch citizen would normally be registered. The outcome of the research was that a citizen who is inactive in social life and on the internet will feature

---

[306] Ministerie van Buitenlandse zaken, *Evaluatierapport Biometrieproef 2b or not 2b*, Den Haag, 2005, pp. 26-28 (section on children (3.3)), available at www.minbzk.nl/aspx/download.aspx?file=/contents/pages/43760/evaluatierapport1.pdf. See also http://www.infosecurity-magazine.com/news/051021_biometrics_children.htm

[307] This is a standard set by the US National Institute for Standards and Technology (NIST) (see http://www.nist.gov/public_affairs/factsheet/biometrics.htm)

[308] The results were improved by wiping and then drying children's fingers, to get the best level of humidity.

[309] Brussee, R., Heerink, R. Leenes, S. Nouwt, M. Pekarek, A. Sprokkereef and W. Teeuw, *Persoonsinformatie of Identiteit? Identiteitsvaststelling en Elektronische Dossiers in het Licht van Maatschappelijke en Technologische Ontwikkelingen*, 2008, Telematica Instituut, Report TI/RS/2008/034:1-98 (*'Persoonsinformatie of Identiteit?'*). See also Ministry of Home Affairs, *Privacy Enhancing Technologies. Witboek Voor Beslissers*, 2004, R. Koorn *et al.*, The Hague.

[310] *Persoonsinformatie of Identiteit?*, p. 18. See also E. de Leeuw, 'Biometrie en Nationaal Identiteitsmanagement', *Privacy and Informatie*, 2007, Vol. 2 N°. 10, pp. 50-56.

[311] Schermer and Wagemans (Considerati), *Onze Digitale Schaduw*, Amsterdam, January 2009, available at http://www.cbpweb.nl/downloads_rapporten/rap_2009_onze_digitale_schaduw.pdf?refer=true&theme=blue

in about 250 data bases, whilst an active citizen can end up in thousands of data bases. In view of these numbers, and of the increasing trend of government departments and companies to share information, some questions can be posed about the practical workability of Article 33 and 34 (duty to inform) of the Data Protection Act. In a reaction, the Dutch Data Protection Authority urged public and private institutions to strengthen the information provision on their data handling practices.[312]

In February 2009, the study Migration Machine (*De Migratie Machine*) was published.[313] This is the first academic study that attempts to assess the impact of the use of biometrics and the body on the Dutch society as a whole, and the vulnerable group of migrants in particular.[314] The work brings experts together who are writing on the daily and increasingly automated practice of immigration and border control in Europe and the Netherlands. The book, so far only available in Dutch, poses meaningful and longer term questions about the role of biometric and other body related technologies, the political discourse surrounding the introduction of biometrics and the impact of the belief in the unfailing measurability of the human body. A chapter on the legal context laments *the lack of power of the Dutch Data Protection Authority to give binding advice*. It also identifies a discrepancy between data protection powers and the *staffing levels* of the data protection authorities in the EU in general.[315] According to the authors, the migration machine is still in development and in *need of evaluation*. In fact, to paraphrase, they identify a machine geared towards 'delivering high tech' and 'screening broad' with an increasing danger of running out of control.[316] By choosing a title that suggests efficiency but also hints at an unfair balance between the anonymous state and a vulnerable, individual migrant, the authors hope to stimulate debate and increase democratic accountability. In the concluding chapter, Dijstelbloem and Meijer conclude that shaping technological boundaries is of democratic, humanitarian and legal concern and deserves more attention than it does to date.[317]

Security and public policy implications of the large scale use of biometric data have not been addressed in Dutch national reports yet. The national differences in approach become clear from the different solutions preferred by EU Member States when deciding on centralized and/or de-centralized storage of biometric data contained in the new EU passports.[318]

Analysis of current Dutch laws or proposals (especially the amendment to the Passport Act and the Act relating to Foreigners of 2000 - see *below*) show that *centralisation* is the trend in the Netherlands. Dutch policymakers favouring the creation of central databases see the storing of biometric characteristics on the passport chip only as irresponsible.[319] Failure to

---

[312] http://www.cbpweb.nl/documenten/rap_2009_onze_digitale_schaduw.shtml?refer=true&theme=blue

[313] H. Dijstelbloem, and A. Meijer, *De migratie-machine : de rol van technologie in het migratiebeleid* (The migration machine : the role of technology in migration policy) Amsterdam, Van Gennep, 2009 ('*De Migratie Machine')*.

[314] On the role of biometrics, see the chapter by D. Broeders 'mobiliteit en surveillance: a migratiemachine in de maak', pp 35-60 and the chapter of Van der Ploeg and Sprenkels, 'migratie en het machine-leesbare lichaam: identitificatie en biometrie', pp. 61- 98, both in *De Migratie Machine*.

[315] This is the chapter by Brouwer, 'Juridische grenzen aan de inzet van biometrische technologie', *De Migratie Machine* , pp. 191-228.

[316] See the final chapter of *De Migratie Machine* pp. 229-254.

[317] Dijstelbloem and Meijer , 'public attention for an unprecedented machine', *De Migratie Machine*, p. 253.

[318] See for example the German country study in this deliverable.

[319] For an overview, see J. Grijpink, 'Identiteitsfraude en Overheid', *Justitiele Verkenningen*, Vol 32, n° 7, 2006, pp 7-57.

store the biometrics in a database that is accessible for the future will make prevention, investigation or prosecution of identity fraud possible in case of illegal tampering with the chip. The prevailing view is that *the impossibility to compare the scan on the chip with the scan originally taken will hamper identity fraud detection and will encourage fraud.*

## 6.3 Legislation regulating the use of biometric data

### 6.3.1 General and specific privacy legal framework for biometrics

In the Netherlands, as in many other countries, the existing data protection legislative framework governs the use of biometrics and no separate legislation has been proposed or adopted. As the data protection perspective on technology is characterised by an 'enabling logic', law has not acted as a barrier to the diffusion of biometric technologies. Thus, data protection legislation makes existing processing practices transparent, and does not prohibit them as a rule.[320] In other words, Dutch data protection regulations create a legal framework based upon the assumption that the processing of personal data is allowed and legal in principle.[321] Therefore, ownership of individuals regarding their data is not recognised, but individual controlling rights are granted instead.

The legal framework for data protection in general in the Netherlands consists of Article 10 of the Dutch Constitution, Directive 95/46/EC, the Dutch Data Protection Act (*'Wet Bescherming Persoonsgegevens'*)[322], and a number of other specialized laws and regulations such as the Medical Treatment Agreement Act (*'Wet op de Geneeskundige behandelingsovereenkomst'*)[323], the Database Act (*'Databankenwet'*), the Municipal Database Personal Files Act (*'de Wet Gemeentelijke Basisadministratie'*)[324], the Police Files Act (*'Wet Politieregisters'*)[325], Foreigners Act (*'Vreemdelingenwet 2000)'*[326] and the Telecommunications Act (*'Telecommunicatie Wet')*.[327]

[320] There are exceptions. Some sections of the data protection regime provide for a prohibition of processing (e.g. sensitive data, secretly collected personal data) in which case such processing operations actually fall under a privacy or opacity ruling.

[321] An outright processing ban effectively applies only to special categories of sensitive personal data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. On the limitations of the data protection approach see also A. Sprokkereef, 'Data Protection and the Use of Biometric Data in the EU', S. Fischer Huebner, P. Duquenoy, A. Zaccato, L. Martucci (eds.), *The Future of Identity in the Information Society*, IFIP (International Federation for Information Processing), 2008, Volume 262, Boston Springer, pp 277-284.

[322] The Dutch Personal Data Protection Act of 2001, last amended in 2002, available at http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml

[323] http://wetten.overheid.nl/BWBR0007021/geldigheidsdatum_31-03-2009

[324] http://wetten.overheid.nl/BWBR0006723/geldigheidsdatum_31-03-2009

[325] http://wetten.overheid.nl/BWBR0010477/geldigheidsdatum_31-03-2009

[326] http://wetten.overheid.nl/BWBR0011823/geldigheidsdatum_31-03-2009 ; This Act is also available in English at http://www.legislationline.org/documents/id/4680

[327] http://wetten.overheid.nl/BWBR0009950/geldigheidsdatum_31-03-2009.

The Data Protection Act is applicable to the collection and processing of personal data and also applies to the processing of biometric data.[328] The Act does not contain specific provisions that mention biometric data as such. Nevertheless, there has been hardly any discussion about whether, or under which conditions, biometric data should be considered personal data. In 2007, a report called *First Phase Evaluation of the Data Protection Act*, presented an analysis of the obstacles in the implementation and application of the Data Protection Act.[329] One of its conclusions was that 'the vagueness of the concept of personal data implies obscurity on the scope of the act and this leads to divergent interpretations'.[330] It can therefore not be excluded that *encrypted biometric data will in certain instances not be regarded as personal data under Dutch law*. There is, however, no case law at all in this field yet. It is remarkable that the 211 pages report does not mention biometrics once. As the report is based on a literature and case law study only[331], this just reflects the fact that no conflicts or obstacles in the area of biometric data handling have arisen so far.

The second part of the evaluation report (the second phase evaluation) will be based on empirical research and might throw more light on the application of Dutch Data Protection Act to biometric data handling. Based on our own study[332] and the general conclusions of the *First Phase Evaluation of the Data Protection Act* report, we are making an informed guess in stating that the use of biometrics takes place in a relatively uninformed manner. One of the conclusions of the report is that 'self regulation within the scope of the Data Protection Act leaves much to be desired'.[333] The final conclusion of the report is that many rights and obligations of controllers and persons involved that arise from the Data Protection Act are not effectively exercised through a lack of familiarity with these rights.[334] Thus, one of the core objectives of the Data Protection Act, *to increase the transparency of data processing* though the granting of rights and obligations and the introduction of a regulatory authority, has not been fully achieved yet.

### 6.3.2 Legal provisions for government controlled ID biometric applications (passports, other civil ID biometric applications and law enforcement)

*Passport and a Central Database*

Since 26 August 2006, all Dutch passports are issued as a biometric passport with an embedded RFID chip for storing the face scan. Two finger scans will be added from the end of June 2009 onwards. An amendment[335] to the Passport Act enabling the storage of finger scans *in a central data base* on top of two finger scans on the chip in the passport itself, is

---

[328] For one of the first Dutch attempts to provide an oversight of all laws that govern particular aspects of biometrics: S. Artz and van Blarkom, 'Beveiliging van persoonsgegevens: de WPB. Privacy en Biometrie: een technisch vraagstuk?', *Jaarboek Fraudebestrijding*, 2002.

[329] G.J Zwenne, A.W. Duthker, M. Groothuis, H. Kielman, W. Koelewijn en L. Mommers, *Eerste Fase Evaluatie Wet Bescherming Persoonsgegevens: Literatuuronderzoek en Knelpunt Analyse*, eLaw@Leiden/WODS, 2007 ('*Eerste Fase Evaluatie'*).

[330] *Eerste Fase Evaluatie*, p. 210.

[331] See *Eerste Fase Evaluatie*, p 5.

[332] *The Use of Privacy Enhancing Aspects of Biometrics* 2009.

[333] *Eerste Fase Evaluatie*, p. 211. According to the authors, especially further interpretation of substantive standards through self-regulation has only been realized to a restricted extent.

[334] *Eerste Fase Evaluatie*, p. 211.

[335] First Chamber, 31.324 (R1844).

currently going through the parliamentary process. On 20 January 2009, the Dutch Second Chamber passed the amendment with a majority formed by the PvdA, VVD, ChristenUnie, SGP, CDA, PVV and the member Verdonk. The amendment is still pending before the Senate (First Chamber). The Senate commission for Home Affairs (BZK/AZ) has published its report on 24th March 2009[336] and is waiting for a ministerial reply.

The amendment to the Passport Act provides that the *public prosecutor can request access to the data in the central database* '*Gemeentelijke Basisadministratie'*, under the strict rules applying to access to data in the context of a criminal investigation. [337] For a ruling about the necessity of central storage, we refer to the *Huber* case[338] of the European Court of Justice discussed *above* in section 2.3.

*Basisvoorziening Vreemdelingen (Foreigners' Database)*

Finger scans of foreigners (including other EU citizens)[339] are stored in the Foreigners' Database for the purpose of identification. The finger scans are stored to prevent identity fraud and to make the implementation of the Foreigners Act 2000 more efficiently. The finger scans are *not stored for law enforcement purposes*.

After the Huber case, the Commission Meijers, the Dutch Standing Committee of Experts on International Immigration, Refugee and Criminal law,[340] has suggested[341] that the European Court of Justice may find a swipe search of the Foreigners' Database on the basis of Article 55c Code of Criminal Procedure [342] unlawful. In a reply to the Dutch Senate, the Minister of Justice has indicated that he does not think this is the case. He refers to the fact that in the proposal for the amendment to the Passport Act, Article 4a (1) stipulates that a face scan and four finger scans of every Dutch citizen are stored when he or she applies for a passport. As a result of Article 4b (4) of that amendment, the public prosecutor can request access to these data. According to the Minister, the conditions in the law which apply to a Dutch passport

---

[336] http://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vi3muuvdnnsz/f=y.pdf

[337] Artikel 4b, al. 4 of the amendment states it in Dutch as follows : 'De verstrekking van biometrische kenmerken van de houder uit de reisdocumentenadministratie in de gevallen, bedoeld in het tweede lid, onder a en c, geschiedt uitsluitend aan de officier van justitie. De verstrekking vindt slechts plaats: a. ten behoeve van de vaststelling van de identiteit van een verdachte of veroordeelde voor zover in het kader van de toepassing van het strafrecht van hem biometrische kenmerken zijn genomen en er twijfel bestaat over zijn identiteit; b. in het belang van het onderzoek in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten', available at http://parlis.nl/pdf/kamerstukken/KST121168.pdf

[338] OJ C 44 21.2.2009, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:044:0005:0005:EN:PDF

[339] See Article 1(e) of the Foreigners Act 2000, available at http://www.legislationline.org/ documents/id/4680

[340] The Standing Committee of Experts on International Immigration, Refugee and Criminal law, is an independent committee established by five non-governmental organisations: the Dutch Bar Association, the Refugee Council, the Dutch section of the International Commission of Jurists, the Dutch Centre for Immigrants/FORUM and the National Bureau against Racism (LBR). It monitors developments in the area of Justice and Home Affairs and presents its opinion to the Dutch Parliament, the European Parliament, parliaments in other Member States, the European Commission and to other public authorities and non-governmental organisations.

[341] The Commission Meijer has published an open letter about the Bill on identification of suspects (*'Wetsvoorstel Identiteitsvaststelling verdachten') on* the 22nd January 2009, which is available at http://www.commissie-meijers.nl/assets/commissiemeijers/Commentaren/2009/CM0901%20Brief%20Commissie%20Meijers%20Wetsvoorstel%20Identiteitsvaststelling%20verdachten.pdf

[342] Article 55c of the Code of Criminal Procedure provides for a procedure which allows the prosecutor to access data held by other authorities under certain circumstances.

holder who is suspected are similar to the ones in applying to a suspect who 'is probably an alien' and 'a search request is made by the prosecutor in order to have access to data of foreigners in the database.'[343]

An interesting legal point is here whether the Minister in fact implies that swipe searches can be held in both databases to compare the finger scans of a suspect against all scans held.

*Progis Protocol Identification in the Criminal Justice Chain (Progis Protocol identiteitsvaststelling in de Strafrechtketen)*

The goal of the draft law on Identification in the Criminal Justice Chain[344] is to strengthen a trustworthy identification of suspects and convicts in the criminal justice chain. The proposed Act on the Identification of Suspects, Convicts and Witnesses ('*Wet identiteitsvaststelling verdachten, veroordeelden en getuigen'*) recognizes four ways of identifying a person: a declaration, the presentation of a valid identification document, providing a face scan and finger scans. The proposed law indicates which type of identification is required/allowed at which moment in time. The law would also introduce new elements such as that the suspect needs to identify him or her self before a judge.

The proposed law was passed by the second chamber of the Dutch Parliament in December 2008 and is currently pending before the Senate Chamber. The Justice committee of that Chamber has received a Ministerial reply ('*Memorie van Antwoord'*) on 17th of March 2009.[345] The Progis protocol has in the meantime been tested within the criminal justice system and several changes have been made. The protocol relies heavily on the efficiency and effectiveness of biometric identification and verification.

---

[343] *Memorie van Antwoord 31436*, 17 March 2009, p. 11, available at http://www.dnasporen.nl/docs/wetregelgeving/KST128925.pdf .The Minister stated it as follows : 'These conditions are materially similar to the conditions under which the fingerprints of foreigners for the purpose of determining the identity of a suspected foreigner (see Article 55c, second and third paragraph, Code of Criminal Procedure) and the detection and prosecution of criminal offenses (see my letter of November 12, 2007) are consulted. Therefore, I believe, contrary to the Commission Meijers, that there is no reason to doubt whether the Court would deem it acceptable that the fingerprints that have been taken from a suspect on the basis of Article 55c, second and third paragraph, Code of Criminal Procedure are compared with the fingerprints that have been processed in the context of the "Basisvoorziening Vreemdelingen", if the suspect is probably a foreigner' (free translation).

[344] http://www.eerstekamer.nl/behandeling/20081202/gewijzigd_voorstel_van_wet_2/f=y.pdf

[345] See Eerste Kamer Stand van Zaken: http://www.eerstekamer.nl/wetsvoorstel/31436_wet_identiteits vaststelling

## 6.4 The National Data Protection Authority on biometrics

In contrast to France, it is in the Netherlands not mandatory to request an opinion on or an authorization for the processing of biometric data. A notification of the use of a biometric application with the DPA is all that is required to get a new biometric application started. Normally, the DPA does not take further steps after it receives the notification of the processing of biometric data.[346] In principle, the notification to the DPA does not imply an approval. To the contrary, the notification allows the authority to react if this is needed. In practice, and due to *staff constraints*, this seldom happens, however. As it is not required that the processor or controller waits for a 'green light', the controller can start the processing straight after notification.

Thus, in practice the role of the DPA has been to receive notifications, to make an administrative check on them and to place all notifications on a register accessible through its website.[347] A few organisations have asked the DPA to issue a preliminary opinion. Whilst the 1999 report *At Face Value* mentioned above was pro-active, the Dutch DPA activities have been of a more re-active nature since then.[348]

Concerning the semi public or private use of biometric applications, the main supervisory activity of the DPA has been the publication of three preliminary (non-binding) opinions, which are hereunder discussed.

*Opinion relating to an access control system with the use of a biometric disco pass*[349]

In 2001, a producer requested the DPA an opinion on an access control system named '*VIS 2000*'.[350] This biometric system was designed for use by sport centres, social clubs or similar establishments. Apart from organising access control, the system served marketing and management purposes and allowed keeping a 'black list' of customers who had violated the rules. The *VIS 2000* stored the templates of the fingerprint and the face. The templates of the face were stored in a central database, combined with the membership card number and a code for the 'violation of club rules'. The card number was linked to the personal details of the members. The biometric data were also stored on a smart card, and used for membership verification when entering the club. When a person entered with the card, the system performed a check against the black list of banned persons, one of the main purposes of *VIS 2000*. The biometrics were hence used for the purposes of verification (1:1 check, comparing whether the holders of the membership cards were the owners of the card) and of identification (1:N check, comparing whether the holders were registered on the black list). In case of incidents, violators could be identified by their biometric characteristics. This involved reverse engineering of the stored templates of the face to images, comparing the

---

[346] See also *The Use of Privacy Enhancing Aspects of Biometrics.*
[347] See www.cbp.nl.
[348] For a comparison between for example Belgium and the Netherlands see also E. Kindt and J. Dumortier, 'Biometrie als Herkenning- of Identificatiemiddel', *Computerrecht* 2008, p. 132 *et seq.* and P. De Hert and A. Sprokkereef, 'Biometrie en Recht in Nederland', *Computerrecht*, 2008, pp. 301-302.
[349] CBP (before 'Registratiekamer'), *Biometrisch toegangscontrole systeem VIS 2000,* 19 March 2001 *('discopas opinion')*, available at www.cpbweb.nl (last accessed 28th March 2009).
[350] About this opinion, see also E. Kindt, '3.2.2. Situation in some selected countries. The Netherlands', in FIDIS deliverable *D3.10 Biometrics in Identity Management,* E. Kindt and L. Müller (eds), p. 45 et seq., available at www.fidis.net

images with the images of the violators taken by surveillance camera's, and connecting the templates with the name, address and domicile data if a membership card had been issued. The purposes of *VIS 2000* were to increase the security of visitors and employees at the clubs, to maintain order and to refuse access to unwanted visitors.

The DPA stated in its opinion that the use of biometric data for access control purposes is far reaching. It should be evaluated whether the use of biometric data is in proportion with this purpose. To this end, the DPA checked the collection and use of the biometric data against several obligations of the Data Protection Act. The DPA did not report on investigating whether there were other, less intrusive means to maintain order and refuse black list individuals entry to the club without storing biometrics in a central database.[351] In this opinion, the DPA explicitly recognizes the possibility of the algorithm used to reconstruct the face of the original scanned facial image from the template. This reverse engineering of the templates was one of the main functionalities of *VIS 2000* in identifying violators. This technical feature, however, has important consequences. First, it should be noted that the face scan might well contain information about race, which shall in principle not be processed. The Dutch Data Protection Act contains an explicit exception to this prohibition of processing of this information, in particular, when such processing is used for the identification of the person and to the extent that this is necessary for this purpose. On the one hand, the DPA concluded it was inevitable that use is made of templates of the face (containing information about race) for the identification of troublemakers.[352] On the other hand, the DPA stated that the use of personal data for marketing purposes should not include biometric data and that the processing for this purpose should be separated from the other purposes. The DPA concluded its opinion with several recommendations, including conditions for storage and security (encryption of templates and membership card numbers) and for the operation of the biometric system. The DPA also requested that any systems already installed would comply with these requirements.

This opinion of the Dutch DPA is different from the evaluation, comments and conclusion of the Belgian DPA with regard to a similar system. The Belgian DPA reported in its annual report of 2005 that it rendered a negative opinion on a similar system. It considered the use of biometric characteristics for access control for a dancing club not proportionate with such purpose.[353] More particular, the Belgian DPA found the use of biometrics for identification purposes disproportionate and entailing risks for the privacy of the visitors.

*Opinion relating to the amendment to the Passport Act in order to introduce biometrics in 2001*[354]

Several EU member states planned or started to issue biometric passports in furtherance of the Council Regulation (EC) No 2252/2004. The regulations and the legal aspects of the use of biometrics in ID documents and passports have been analyzed in detail in FIDIS deliverable

[351] For example, the simple confiscation of the membership card of the person concerned in combination with checking new applications against a central list of suspended individuals.
[352] As stated above, the DPA *did not make a proportionality test about the use of biometric data*, and the opinion therefore indicates that a necessity test to use information about race should be regarded as sufficient for the purpose.
[353] See E. Kindt, *l.c.*, *Datenschutz and Datensicherheit (DuD)*, 2007, N° 31, pp. 166-170.
[354] CBP, *Wijziging Paspoortwet* z2001-1368 (invoering biometrie), 16 October 2001.

3.6. 'Study on ID Documents' of 2006.[355] On 19th September 2001, the Dutch Home Office Minister requested the DPA's advice on some new paragraphs proposed to Article 3 of the passport law. On examination of the provisions, the DPA concluded that the new passport law would allow biometric data to be stored in the travel document administration of the appropriate authorities. The DPA pointed out that there were not enough arguments to support the necessity of the measure. On the basis of the current arguments, the DPA rejected the need for such a measure. It also stated that even if these grounds were to be put forward, the Passport Act would still need to be based on the purpose limitation principle, whilst in the current wording the purpose was open ended.

In a second advice of 30 March 2007, this argument was repeated, and the DPA *argued against (de-)central storage, warning for the effect of 'function creep'*.[356] It should be noted that databases are not necessary for passport control procedures as the data are to be matched against the reference data on the chip in the passport. It is clear that central databases may prevent citizens from obtaining several identity documents in different names. At the same time, the question is whether anti identity fraud objectives cannot be achieved with other means. A central, or decentralized, database is inherently privacy invasive and security sensitive.[357]

A strong proponent of storage of original biometric data is Grijpink who argues that decentralized storage of four (in stead of two in the passport only) finger scans in the local data base of a Dutch municipality is a very powerful way to prevent large scale identity fraud with biometrics in passports.[358] In the absence of a database, the biometrics of an individual who claims to be the victim of identity fraud cannot be checked against original finger scans stored, and the perpetrator can easily go undetected. According to Grijpink, in the case of *small scale, private or semi public applications, this argument does not hold*, because the impact of identity fraud is not so profound and proportionality becomes a more important issue. In smaller scale applications, it is also possible to detect or prevent fraud through other means.

*Opinion of 2004 on the use of face recognition and the use of biometrics for access control to public events, combined with use for police investigations*[359]

The most concrete DPA opinion on the legal requirements to be fulfilled when introducing a biometric system is this opinion on the protection of personal data and the use of face recognition technology.

The system involved the use of a smart card that served as an entry ticket at large scale events. The smart card contained an identifying number, a limited period of validity and a face scan (digital template) of the holder. At the entry gates, a digital picture was taken of the person

[355] For a very good analysis, see Hornung, 2007.
[356] CBP, Wijziging Paspoortwet advies z2007-00010 (invoering biometrie), 30 maart 2007, 5 (cbpweb.nl)
[357] See for example JH, Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk and R. Wichers Scheur, 'Crossing Borders: Security and privacy issues of the European e-Passport', 1st Int. Workshop on Security, *LNCS* 4266, page 11, Kyoto, Japan, October 23-24, 2006.
[358] J. Grijpink, 'Biometrie, Veiligheid en Privacy', *Privacy en Informatie* 2008, Vol 11, pp. 10-14; J. Grijpink, 'Two Barriers to Realizing the Benefits of Biometrics', *Computer Law and Security Report* 2005, Vol. 21(3), 249-256; J. Grijpink, 'Biometrics and Privacy' , *Computer Law and Security Report* 2001,Vol. 17(No. 3), pp. 154-160.
[359] CBP, *Vragen over de inzet gezichtsherkenning* z2003-1529, 3 February 2004.

offering the card and the resulting template compared to the template on the smart card. This entailed a verification as to whether the person offering the card is in fact the legal holder. The decision to let someone pass the gate was an *automated decision* as the number of the smart card would be checked against the card numbers of banned persons on a *black list*. The templates made at the entry gates and the numbers of the cards would be stored on a *temporary event database*. These data served to identify persons that had caused disturbances at the event, through templates obtained through pictures taken by surveillance cameras. These would be checked against the templates stored in the event data base. A hit would result in getting access to the information stored on the card and in the administration of the event organiser.

The DPA stated in a commentary at its website www.cbp.nl that, generally speaking, it is *not an opponent of the use of biometrics for event access control.* In fact, the DPA stated that sometimes the use of biometrics can prevent the unnecessary handling of personal data. In the present case, however, there is a strong link between access control and identification. However, as the templates are in this case stored in an event data base, the use of the smart card is not restricted to access control. Therefore *the objectives* of the access control system needed careful examination and specification, especially when visitors have no other option than using the system.

Whether more personal data are processed than necessary in detecting the violators of the event's rules, is determined by the following. An adequate process for the issuance and management of smart cards leads to better access control and therefore to a reduced need for setting up a ticket holder data base. Stricter access control would normally lead to a reduction in the number of those intending on misbehaving, and therefore less identification is needed. To determine whether the building of an event data base is necessary, it would be *necessary to have an insight into the impact of biometric controls*. It can also be expected that potential violators of the rules will try to avoid recognition by the system by putting on all kind of *disguises* after having passed access control.[360]

When the detection of a violator *depends only to a limited extent on the templates* stored on the event data base, then the use of the system threatens to become *disproportional*. If the use of the system does not really produce more benefit than the already existing instruments to detect violators, then the concept contains unnecessary processing of data. The DPA confirms that unnecessary processing of data is illegal.[361]

In the conclusion, the third DPA opinion introduces the basic condition that it needs to be proven that the use of face recognition technology increases safety in a proportional manner. The key sentence in the opinion is therefore the following:

> "When the introduction of the system, in view of all the instruments already available, does not provide additional value, the concept entails unnecessary processing of data".[362]

[360] All these observations are mentioned the DPA opinion itself
[361] See the full opinion on a detailed test of the concept of data processing: CBP , 27 May 2004, z2003-1529.
[362] See also section 6.1.2. of the fore mentioned opinion of the DPA.

## 6.5 Conclusion

Our fieldwork reported elsewhere[363] and other studies[364] have shown that in the Netherlands *external supervision on the use of biometrics is lacking especially.* Due to *staff shortage and/or lack of powers*, the Dutch DPA has not been able to develop an active policy on the promotion of good practice in the use of biometrics. At the same time, the DPA can possibly not be expected to provide informed steering of the approach to biometrics all by itself.[365] So far, the introduction of biometrics has not been given significant attention. *Guidelines* on good practice in the implementation of biometrics such as those issued on the use of biometrics in schools in the UK would be one way of providing a lead and improving the information position of data subjects. For the DPA to issue detailed guidelines no new legal powers would be necessary.

*Certification* of biometric applications would require a separate regulation on biometric applications. This approach was hinted at in the 1999 *Face Value* report but was never given serious attention. When such a legal basis for certification would be established, then other rules on the use of biometrics could be considered for codification. These provisions could include *inter alia* explicit *legal prohibition to process raw images*, an obligation to encrypt biometric data used for processing and an obligation to use *multiple authentications*.[366] The question is of course whether in practice these goals cannot be achieved with other means such as the information provision, the broadening of administrative powers[367], the extensive use of opinions and effective enforcement through increased consultation. Categorisation of different biometric applications in combination with more incentives for self regulation, would be a mid way house. This could be done through organising informal negotiations among stakeholders resulting in non-binding government advice (or categorisation of products) on the criteria with which biometric applications should comply with in particular situations. The advice would also have to include the conditions placed on overall system safety and information provision.

Given the complexity of the assessment of the technical possibilities of biometrics, *detailed legislation* on the use of biometrics might make compliance more likely. However, no other European country has issued detailed and separate regulation for biometrics yet. As this study has shown, there is at least still room for *a more effective enforcement* of existing legislation through the instruments mentioned above in the Netherlands. Therefore, enforcement is the more obvious choice for the regulation of biometrics.

---

[363] See *The Use of Privacy Enhancing Aspects of Biometrics*.
[364] For example: *First Phase Evaluation of the Data Protection Act* and also Brouwer in *De Migratie Machine.*
[365] On the role of the DPA and the development towards a second generation of supervisory authorities see P. Hert, *Citizens' Data and Technology: An Optimistic Perspective,* 2009. The Hague, Dutch Data Protection Authority, pp. 38-40.
[366] See *The Use of Privacy Enhancing Aspects of Biometrics,* p 302.
[367] *Citizens' Data and Technology: An Optimistic Perspective,* p 39.

# 7 Switzerland

## 7.1 The spreading of biometric applications

Switzerland delivers since September 2006 a passport for a limited period of 5 years containing the digital image of the face of the person in a so-called pilot-project. The introduction of the biometric passport, however, remains pendant as the introduction waits for a decision of the people of Switzerland that will vote on the subject, foreseen for 17 May 2009.

Biometrics are not yet implemented in the Swiss ID and neither in the social security card.

Furthermore, and according to reports of the Federal Data Protection Agency, biometrics have been implemented in other applications for access control. The two different access control implementations are as described below.

First of all, a biometric application was used for securing the check-in at the airport of Zürich-Klotten.[368] During a test phase (from December 2004 to mid-April 2005), the firm Swissport International AG used biometrics for easing the boarding. The test was limited to one destination and one company. The passengers for that destination received the opportunity to participate to the pilot project. At the check-in desk, the attendant checked the ID of the participant and the biometrics of the participant was then stored on a chip-card that was carried by the passenger. The passengers could then use a biometric system (matching their data with the ones on the card) for boarding. The advantage was that *identity was checked only once* by the Swissport. This didn't interfere with the security checking and border control that were not affected by this measure. The information on the card was deleted right after the boarding and *no central database* was used. The Data Protection Agency (DPA) made some recommendations regarding the information to be provided and the explicit consent of participants, as well as on the immediate deletion of data contained in the cards.

Biometrics was also implemented in the *access control system of a swimming pool* in Schaffhouse.[369] This application was introduced in a first version in the summer 2005 for a test period. Then the comments of the DPA required changes in the implementation and these changes were introduced during the year 2006. The system is used to control the access to the swimming pool. The system is based on a *central database* containing all the templates, and a set of cards, and each user of the pool receives one card. In the enrolment phase, each user shows his/her forefinger whose fingerprint is registered. The fingerprint is transformed into a template that is stored centrally in the database. The user also receives a *card* containing an identifier. For entering the pool, the user inserts his/her card in the system. The system gets the corresponding template and asks the user to present his finger. The fingerprint is scanned and compared to the template. If the data match, the person can enter the swimming pool.

---

[368] Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)/ Préposé Féderal à la Protection des Données et à la transparence (PFPDT)) [Federal Data Protection and Information Commissioner (FDPIC)], *Einsatz von Biometrie beim Check-In und Boarding im Rahmen des Pilotprojektes "Secure Check" der Swissport International AG und Checkport Schweiz AG am Flughafen Zürich-Kloten*, June 2005.

[369] Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)/ Préposé Féderal à la Protection des Données et à la transparence (PFPDT)) [Federal Data Protection and Information Commissioner (FDPIC)], *Erhebung biometrischer Daten beim Erwerb einer Dauerkarte in den Sport- und Freizeitanlagen KSS Schaffhausen, Schlussberricht,* April 2006.

Biometrics are also used by the police. The police use biometrics to find the committers of crimes. In some cases of the federal court, reference is made to biometrics.[370] The police is also allowed to use DNA profiles to identify criminals.[371] Since Switzerland has now become part of the Schengen Area, it will participate in the Schengen Information System which contains biometric information.

As to whether there has been any public debate about the introduction of biometrics in Switzerland, reference is made to the discussion about biometrics because of the introduction of biometrics in passports (see *below*).

## 7.2 Legislation regulating biometric applications

Biometric applications are governed by the Law on Data Protection.[372] The federal law on data protection has been revised in 2008 and includes a definition of the role of the DPA. The Swiss Federal DPA published guidelines for the development of biometric applications.[373] These guidelines will be discussed *below.*

As far as known, there are in general no specific provisions in the national legislation which refer to biometric data/applications, and no legal definition of biometrics.

For the adoption of biometrics for passports and travel documents (implementation of Council Regulation 2252/2004), the parliament (both Chambers) discussed the issue and the legal text was approved by the Chambers.[374]

Notwithstanding this law, a referendum has been set up and the citizens of Switzerland will vote on the subject on 17 May 2009.[375]

During the months of April and May 2009, it is very likely that there will develop a new public debate to convince voters about the choice to make for the biometric passports. All the elements of this debate are not yet known, but the promoters of the referendum who are against the biometric passport used the following arguments in their campaign:[376]

- The passport will be more expensive;
- Risks with the security because of the centralization of data;
- Competence transferred to the Swiss Confederation;

---

[370] See, for example, Swiss Federal Court, 6S.454/2006 /rod, Refus du sursis à l'exécution de la peine et à l'expulsion (art. 41 CP), 28 December 2006.

[371] Swiss Federal Court, 1B_71/2007, Probenahme und Erstellung eines DNA-Profils im Rahmen eines Strafverfahrens, 31 May 2007.

[372] Loi Fédérale sur la Protection des Données [Federal Data Protection Act ], June 1992, as modified ('Federal Data Protection Act').

[373] See Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)/ Préposé Féderal à la Protection des Données et à la transparence (PFPDT)) [Federal Data Protection and Information Commissioner (FDPIC)], *Guide relatif aux systèmes de reconnaissance biométriques*, November 2008 ('*Guide for Biometric Systems 2008'*).

[374] Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et la Communauté européenne concernant la reprise du Règlement (CE) 2252/2004 relatif aux passeports biométriques et aux documents de voyage (Développement de l'Acquis de Schengen) [Federal Act approving and implementing Regulation (CE) 2252/2004] (Développement de l'Acquis de Schengen), Swiss Parliament, 13 June 2008.

[375] Département Fédéral Justice et Police [Federal Department Justice and Police], Communiqué '"Passeport biométrique et liberté de voyager: votation populaire en mai prochain", Bern, Switzerland, October 29, 2008

[376] Überparteiliches Komitee gegen Biometrische Schweizer Pässe und Identitätskarten [Party-independent committee against the Swiss biometric passport and identity card], *FREIHEITSKAMPAGNE.CH*, available at http://www.freiheitskampagne.ch/

- Insecurity about where and when the RFID tag can be read;
- Insecurity about the usage of the data stored inside the passport or in the central database.

The arguments of the advocates of the new passport are not known. Nevertheless, the main argument was until now the obligation to comply with the Council Regulation (CE) 2252/2004.

In a communication[377], the federal government of Switzerland ('*Conseil Fédéral'*) states that the biometric passport must be introduced for the following reasons:

- Obligation to fulfil the ICAO (International Civil Aviation Organisation) recommendations ;
- The fact that every state member of the Schengen area will include two fingers and the picture of the person inside their passports ;
- Obligation for Switzerland to implement the Council Regulation because of the Schengen Association Agreement ;
- The fact that electronic and biometric passport have been or are being introduced in 54 states and that such passports simplify the verification of identity, and make it more secure. As a result, electronic biometric passports reduce the risk of misuse of a passport and travelling under a false identity.

As to the decision about the use of a national biometric database, such database is created by the "arreté fédéral".[378] It can only be introduced if the citizens of Switzerland accept it at the referendum of the 17th of May 2009.

## 7.3 Approach to the specific legal issues of biometric applications

There are, as far as known, no specific rules for the processing of biometrics as unique identifiers in particular. The goal of the "Guide relatif aux systèmes de reconnaissance biométique" ('Guide for Biometric Systems 2008') of the Swiss Federal DPA, however, was to *prevent the use of biometrics as unique identifiers*, by limiting the use of central databases and *promoting decentralized applications*.

In the same Guidelines, the Swiss federal DPA states that some biometric data can contain sensitive information which fall within the relevant provisions relating to sensitive data of the Swiss Federal Data Protection Act. Sensitive data are data related to race or health (art.3 lit.c of LPD), so the following characteristics and biometric technologies which could contain some sensitive information are mentioned: fingerprint, hand or face geometry, iris scan, voice recognition because they contain information related to the race or the health of the person.

---

[377] *Département Fédéral Justice et Police* [Federal Department Justice and Police], Communiqué "Passeport biométrique et liberté de voyager: votation populaire en mai prochain", Bern, Switzerland, October 29, 2008.

[378] Arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et la Communauté européenne concernant la reprise du Règlement (CE) 2252/2004 relatif aux passeports biométriques et aux documents de voyage (Développement de l'Acquis de Schengen) [Federal Act approving and implementing Regulation (CE) 2252/2004] (Développement de l'Acquis de Schengen), Swiss Parliament, 13 June 2008.

The law in Switzerland gives a special status to "sensitive" data as described above. There is no other special type of data. Biometrics in general are not special data.

Although the proportionality principle is mentioned both in the Federal Data Protection Act and in the Guide for Biometric Systems 2008 of the DPA, no precise definition of this criterion is given in both documents.

As to whether consent is accepted as a basis for the processing of biometric data, the Swiss Federal data protection officer insisted in the two cases documented and described above[379] on the notion of consent. The DPA obliged the providers to offer an alternative solution to the customers/users refusing the enrolment at the same costs for the service. The DPA also obliged the provider to give enough information (by augmenting the size of a poster for the check-in or by providing flyers to the clients of the swimming pool). As a result, the consent is only valid if it is given by a well informed customer who has also the opportunity to deny the offer.

As to whether there are additional information and transparency requirements for the benefit of data subjects, the Data Protection Agency recommends informing the user before he enters such a program for the deployment of a biometric application.

A biometric system should also not be based on elements that can be acquired without the users' knowledge. The DPA hereby referred to the Working Document on biometrics of the Article 29 Data Protection Working Party, which recommends the use of elements that can not be seen as traces.

A biometric system that is only used to verify the identity of a person should always be decentralized, that means, that the user has in his/her possession a token containing his/her biometrics.

In its Guide for Biometric Systems 2008, the Swiss Federal DPA recommends to implement *security measures*, without giving details. The biometric data are sensitive, so one should *prevent any unjustified access*. The access control can be both *physical* and *logical*. The identified risks are located inside the storage and the data communication subsystems.

As stated above, an alternative procedure must be provided according to the non-discrimination principle.

[379] See *above*, at footnote 368 and 369.

## 7.4 The National Data Protection Authority on biometrics

*Position of the DPAs in 2005 on the biometric passport*

In 2005, a group composed of federal and all cantonal Data Protection Officers wrote a commentary on the introduction of new passports containing biometrics.[380]

In this document they recommend not to use fingerprint and iris template in the passport. They also recommended *not to store any raw data* (for instance, the picture of the face) on the card, but *rather to store a template*, because the raw data may give access to more information (information relating to race, health, ...). They further recommend storing the information *only inside the passport and not in a central data base*. The use of RFID-chips to store the information is also a security risk for the DPAs.

*Guidelines on biometrics of November 2008*

In November 2008, the Swiss federal DPA published guidelines on the introduction of biometric applications.[381] The Guidelines provide definitions regarding core concepts of biometrics, such as "biometric template", "failure to enrol", "biometric identification" or "verification", "false acceptance rate" or "false rejection rates". The Guidelines further provide recommendations for the implementation of biometrics based identification systems. Finally, the Guidelines also include an evaluation guide.

The decisive criteria deployed by the Swiss federal DPA and explained in the Guidelines mentioned above, are hereunder briefly described.

The DPA requires that the biometric application is legal ('*licite'*), transparent and contains a clearly defined goal. If the goal is explicitly identification (means 1 to N matching) then the data have to be centralized. But since in most of the cases only verification of the identification (means 1 to 1 matching) is required, the DPA suggests to only use decentralized data in this case. The objective is that the user *always controls* the use of his/her personal biometrics *by carrying it physically with him/her* (smart card or any similar device).[382]

The processing of biometric data is further restricted: it must be done accordingly to the purposes. No central data base should be used for doing the verification of the identity of a person, since other less privacy-invasive solutions exist.

The Guidelines of de Swiss federal DPA *restrict* the use of biometrics to biometric information that *need the consent of the person to be captured*.[383] Some biometric characteristics can be captured and used without been noticed by the concerned person. In real life, people leave a lot of more or less usable traces. Moreover, some biometric characteristics can be captured in a way such that a person does not notice it. One should not implement biometric system using technologies based on data that can be leaved as traces or captured without involving the person ('*à l'insu des personnes concernées'*). So one should opt for a system based on the shape of the hand rather than for a system based on fingerprints.

---

[380] Die Schweizerischen Datenschutzbeauftragen/Les commissaires Suisses à la protection des données [The Swiss Data Protection Authorities], *Vernehmlassung. Einführung des biometrischen Passes: Vorentwurf zur Änderung des Gesetzes und der Verordnung über die Ausweise für Schweizer Staatsangehürige*, 26 September 2005, available at http://www.privatim.ch/content/pdf/050926.pdf

[381] See *above*, at footnote 372.

[382] *Ibid.*

[383] *Ibid.*

As to the security measures the Swiss federal DPA recommends to storing the templates of data and *not the raw data*. One has to explicitly express the need for storing raw biometric data.

*Guidelines on biometrics of Privatim of February 2007*

The group of Swiss DPAs, Privatim, had also issued earlier guidelines for the evaluation of data protection guidelines of biometric systems.[384] In these guidelines, the Privatim group stressed compliance with the existing legislation, recommending respect for the proportionality principle, restricted use of a minimum amount of personal data, in a decentralised way, with the use of anonymity or pseudonymity where possible, the use of systems which give results close to 100 %, security evaluation and appropriate legislative measures relating to liability.

*Pilot projects on biometrics in Switzerland*

Two pilot projects have been conducted under the surveillance of the DPAs. One pilot project related to the check-in at the airport of Zürich-Klotten and one was an access control system of a swimming pool in Schaffhouse.[385]

For the pilot at the swimming pool, the DPA obliged the operator of the system to include following features or improvements: *improvement of the information about the system*, provision of a possibility *to use an alternative system* for entering the pool and the anonymisation of the transaction data as soon as possible.

But the main improvement imposed by the DPA was to store biometric data on smart cards. Since the system was only used for the verification of the identity of persons entering the area, there was no need for the central database. According to the report, this improvement should have been implemented for the start of the summer season 2007 (before 15 May 2007).

## 7.5 Conclusion

Switzerland is waiting for the result of the referendum of the 17th of May 2009. This vote will certainly influence the future developments of biometrics in the country.

[384] Privatim, Guidelines for the data protection compliance review of biometric systems, 6 February 2007, 15 p. reference available at http://www.privatim.ch/content/suche.php?zoom_query=biometrie
[385] See above at footnotes 368 and 369.

# 8 United Kingdom

## 8.1 Introduction

Unlike most of the other EU Member States, the UK did not participate in the decision making around the Council Regulation 2252/2004 which introduced the European electronic passport with biometric identifiers. This Regulation was adopted in the context of Schengen, in accordance with Council Decision 2000/365/EC. As such, because the UK does not take part in Schengen, there was no obligation on the UK to introduce biometrics, in particular biometric fingerprint.[386] Nevertheless, in line with international developments, the British government prepared for the introduction of biometrics into UK passports. More importantly, the UK government has made it clear with the proposed National Identity Register (NIR) that it intends to take the use of biometrics in identity management to an unprecedented large-scale.

At the same time, in the private and semi-public domains, the first biometric applications have already found their way into schools, banks, places of work and so on. What follows is an overview of relevant aspects and issues surrounding the use of biometrics in the UK. In our analysis, the NIR will be dealt with in detail. The expectation is that the NIR will play a pivotal and central role in the introduction of biometrics as the major factor in identification and authentication processes in the UK.[387]

## 8.2 The spreading of biometric applications

In general, the use of biometric applications in the UK is rapidly becoming wide spread. Below is a description of the areas where biometric applications are implemented, as well as of the debate about the introduction of biometrics, especially with regard to the introduction in the NIR.

### 8.2.1 Fields in which biometric applications are implemented

In December 2003, the Parliamentary Under-Secretary for the Home Office listed the *government projects* that do or will make use of biometrics. The list was presented in an answer to a parliamentary question. The projects were listed in what seems to be an order of importance: the inclusion of the first and second biometric identifier in the British passport; biometric identifiers in the identity cards programme; the UK visas biometric programme; biometric travel documents; biometric residence permit; IAFS (Immigration and Asylum Fingerprints System); the e-Borders programme; the PITO project to use face recognition to support FIND; LANTERN (a mobile fingerprint system) and the national DNA database. In addition, the Under-Secretary of State listed some smaller projects involving the Home

[386] The UK is, however, an ICAO member and the ICAO document 9303 for Machine Readable Travel Documents binding. This document provides for the inclusion of a digital photograph on a contactless chip, while an addition biometric identifier, such as fingerprint, remains for the members optional (See about ICAO document 9303 and the requirements of biometric identifiers also M. Meints and M. Hansen (eds.), *o.c.*, p. 59 *et seq.*).

[387] The goal of the application of biometrics in the UK is to hold the biometrics of all citizens on a register so that the government can achieve reliable authentication of identity claims, in particular to ensure that the person presenting an identity document is the lawful holder.

Office: IDENT1, Application Registration Cards (ARC), ISRP, VIAFS, IRIS, C-Nomis, pilot of methadone dispensing system using iris recognition at HMP Eastwood Park, and a trial of fingerprint based access control to IT systems in prisons.[388] Participation in most of these government projects is *mandatory*. Of course, the decision to request a passport or identity card can be framed as voluntary. However, given the fact that many government services cannot be obtained without passport or identity card, this is a theoretical argument.

Interestingly, the use of biometrics is also on the rise in the *semi-public domain*. Current estimations are that 1000 schools in the England and Wales use body characteristics of their pupils to increase the efficiency of their processes or the safety on their school premises. When the news about schools using biometric applications for library loans, school access or registration of school lunches was getting some publicity through the media, this resulted in a political response. Questions were asked in the House of Commons,[389] a Member of Parliament started an investigation in his constituency[390] and individual concerned parents filed requests for information in the context of the Freedom of Information Act ('FOI'). Lateron, a parent pressure group was established leading to some coordinated action and a website with advice and information for parents.[391] Some time later, the Information Commissioner for England and Wales[392] and BECTA[393] issued guidelines on the use of biometrics in a school context. In February 2009, the fist draft of Scottish guidelines on the use of biometrics in schools was published.[394] As the use of biometrics on systems involving school children is now growing rapidly, it is interesting to note that at the website of the CESG,[395] it is stated that there are currently no UK government approved biometric applications for this purpose. Schools are thus free, but also relatively alone, in making complicated choices on whether and what kind of applications to introduce.

Although *commercial applications* have become widespread, many projects still take the form of pilots. In some of these projects participation is not voluntary but obligatory. Two pilots have been reported extensively in the media: paying with your finger and renting a car with your finger as a security against theft.

For the first pilot, three Co-op supermarkets in Oxfordshire registered clients who would pay their groceries through a pay by touch (fingerprint) system. Market research by the Coop found that of the 1,000 shoppers questioned in the three stores, half had already signed up to

---

[388] See http://gizmonaut.net/blog/2006/12/03

[389] The question (82580) was submitted by David MacLean on 13 September 2005 and the answer can be found at:http://www.publications.parliament.uk/pa/cm200506/cmhansrd/cm060931/text/60913w2385.htm#06091916000121

[390] See http://archive.thenorthernecho.co.uk/2007/1/9/233273.html

[391] See http://www.leavethemkidsalone.com/

[392] Information Commissioner's Office, *The use of biometrics in schools*, available at < http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf>, last consulted 11 March 2009.

[393] Becta, *Becta guidance on biometric technologies in schools*, available at < http://schools.becta.org.uk/upload-dir/downloads/becta_guidance_on_biometric_technologies_in_schools.pdf>

[394] See http://www.statewatch.org/news/2009/feb/scotland-biometrics-in-schools-consult.pdf

[395] The CESG does provide advice on biometrics product selection and for this purpose publishes on its website a manual: UK Biometrics Working Group, *Biometrics for Identification and Authentication – Advice on Product selection*, available at < http://www.cesg.gov.uk/policy_technologies/biometrics/media/biometricsadvice.pdf>, last consulted 11 March 2009.

the scheme or planned to do so soon and the trial was subsequently extended to three more supermarkets.[396]

The second pilot project by car rental companies and Essex police at Stansted required customers to provide their fingerprints; if they failed to oblige they could not rent a car at the airport. Biometric data that were collected were kept by the rental company, but handed over to police when the car had been stolen or used for another crime. Some customers have reacted negatively and have called the measure disproportionate, felt threatened or exposed or questioned the safety of their data.[397]

Nevertheless, evidence of the use of biometrics in the private sector remains quite anecdotal and as far as we are aware, no reliable empirical data are available.

### 8.2.2 National studies and debate about biometrics

The London School of Economics ('LSE') initiated a project, called The Identity Project, to examine the potential impacts and benefits of the National Identity Scheme in detail. The LSE presented its findings in the highly profiled report 'The Identity Project: an assessment of the UK Identity Cards Bill and its implications'. In this report the LSE concludes that the scheme could offer some basic public interest and commercial sector benefits. However, the main findings and conclusions drawn up in the report indicate that the scheme is too complex, technically unsafe, overly prescriptive and lacks a foundation of public trust and confidence.[398] In particular, with regard to the technology that will be used, that is biometrics, the report states:

> 'The technology envisioned for this scheme is, *to a large extent*, *untested* and *unreliable*. No scheme on this scale has been undertaken anywhere in the world. Smaller and less ambitious systems have encountered substantial technological and operational problems that are likely to be amplified in a large-scale, national system. The use of biometrics gives rise to particular concern because this technology has never been used at such a scale.
>
> The proposed system unnecessarily introduces, at a national level, a new tier of technological and organisational infrastructure that will carry associated risks of failure. A fully integrated national system of this complexity and importance will be technologically precarious and could itself become a target for attacks by terrorists or others.' (stress added) [399]

And with regard to the National Identity Register, the report states:

> 'From a security perspective, the approach to identity verification outlined in the Identity Cards Bill is substantially – perhaps fatally – flawed. In consequence, the National Identity Register may itself pose a far larger risk to the safety and security of UK citizens than any of the problems that it is intended to address.'[400]

---

[396] See http://software.silicon.com/security/0,39024655,39160744,00.htm

[397] The aim of this project was to prevent criminal organisations from stealing rental cars by using stolen passports, driving licenses and credit cards. For customer reactions and the first results of the trial see http://news.bbc.co.uk/1/hi/magazine/6129084.stm

[398] LSE, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, June 2005, available at < http://is2.lse.ac.uk/idcard/identityreport.pdf> ('*The Identity Project*'), p. 5. *The Identity Project*, accompanied with all other relevant reports and documents, can be consulted at http://is2.lse.ac. uk/idcard/

[399] *Ibid.*, p. 10.

[400] *Ibid.*, p. 11.

The same points of criticism were expressed by the Information Commissioner as well, who stated it as follows: "My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with."[401]

In the above report, LSE also observes that since the publishing of the Identity Cards Act in 2006, which is the bill which would lay down the legal foundation for the National Identity Scheme, there was increasing concern within business, academia and civil liberties groups about *the lack of informed public debate* about its implications for the UK.[402] In this respect, a parallel can be drawn with the by Hornung observed absence of a widespread public debate about the Council Regulation 2252/2004 which would bring about the introduction of biometrics within the European Union.[403]

The United Kingdom Passport Service (UKPS) itself carried out an investigation into the performances of several biometric identification methods. The study measured performances of three biometrics (face scan, finger scan and iris scan) in large scale applications in 2005.[404] The key findings published were mainly concerned with technical issues concerning the employment and use of biometrics. The majority of participants from all sample groups successfully enrolled on all three biometrics. The enrolment success rate for disabled participants was much lower than the enrolment success rate for the other participants. Analysis showed that the factors which mostly affect the success rate are environmental, in particular the lighting conditions at different locations. Whilst the majority of participants were 'not very' or 'not at all' concerned about having their biometrics recorded prior to enrolment, there was more concern felt within disabled participants and in particular for the iris biometric. Across all three biometrics and all three groups, the total number of participants 'fairly' or 'very' concerned about having their biometrics recorded after enrolment dropped when compared with pre-enrolment. The majority of participants felt biometrics would help with passport security, preventing identity fraud, preventing illegal immigration and would not be an infringement on their civil liberties.

In 2006, the Information Commissioner commissioned the Surveillance Studies Network to write a report on the surveillance society.[405] The resulting 88 pages report includes some glimpses of life in 2016.[406] Although the use of RFID features in some of the examples, the role of biometrics is not presented as a major aspect of the developing surveillance society. One of the contributions of the report to the national debate is the introduction of the concept of surveillance impact assessment.[407]

---

[401] The Times, Beware rise of Big Brother state, warns data watchdog, available at < http://www.timesonline.co.uk/tol/news/uk/article470264.ece>, last consulted 23 February 2009.
[402] LSE, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, available at < http://is2.lse.ac.uk/idcard/identityreport.pdf>, last consulted 23rd February 2009. p. 15.
[403] G. Hornung, 'Biometric Passports and Identity Cards: Technical, Legal and Policy Issues', *European Public Law*, vol 11, issue 4, 2005; G. Hornung, 'The European Regulation on Biometric Passports: Legislative Procedures, Political Interactions, Legal Framework and Technical Safeguards', *Script-ed*, Vol 4, issue 3, September 2007.
[404] United Kingdom Passport Service, *o.c.* at footnote 66. About the trial, see also fore-mentioned footnote.
[405] The Surveillance Studies Network, *A Report on the Surveillance Society For the Information Commissioner*, London, 2006.
[406] *Ibid.*, pp 64-75.
[407] *Ibid.*, pp 89-98.

In 2007, the Nuffield Council published a report examining current police powers in the UK to take and retain bio information are justified by the need to fight crime. Using the proportionality principle as the basis, the report formulates a number of critical observations and/or recommendations to policy makers: [408]

- the permanent storage of bio information taken from witnesses, victims, children, and people who are not later convicted;
- the use of the National DNA Database for familial searching, ethnic inferencing and research;
- the establishment of a population-wide DNA database;
- the use of bio information in court; and
- the governance and ethical oversight of forensic databases.

One of the main concerns expressed in the report is that the threshold for holding DNA profiles on a forensic database is much lower in the UK than in any other member state of the EU. The government is urged to examine the implications of DNA exchanges for those on the UK NDAD. In this context the UK government should insist on two obligations into the Prüm Treaty.[409] These obligations are an obligation on national agencies to produce annual reports (including statistics) and an obligation on the European Commission to produce an overall evaluation.

In January, 2009 the Rowntree Foundation has published a report on the so-called 'Database State'.[410] The report, written by members of the Foundation For Information Policy Research, poses many questions about the legality of most of the government databases in the UK. This report charts these databases, creating the most comprehensive map so far of what the authors state have labelled the "*Database State*". The authors of the report also indicate that information has sometimes been difficult to obtain and there may be omissions and errors. They point out that this year another study is carried out[411] to get an insight into the data held on citizens by UK government and see their study only as the beginning.[412]

Of the databases examined in this report, some hold biometric data. They are given the following lights[413]:

---

[408] Nuffield Council on Ethics, *The Forensic Use of Bioinformation: Ethical Issues*, September 2007, available at http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/publication_441.html (last accessed 25th March 2009)

[409] *Ibid*., pp xxiii-xxiv.

[410] R. Anderson, I. Brown, T. Dowty, P. Inglesand, W. Heath, A. Sasse, *Database State*, York, Rowntree Foundation, March 2009 ('*Database State*').

[411] N Heath, 'More data breaches to come, warns gov't', Silicon.com, Nov 27 2008, at http://www.silicon. com /publicsector /0,3800010403,39354289,00.htm

[412] *Database State*, p. 11.

[413] In the report, a traffic light system is employed to assess the databases identified. The system thus puts the databases in three categories: **Red** means that a database is almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned. The collection and sharing of sensitive personal data may be disproportionate or done without consent, or without a proper legal basis; or there may be other major privacy or operational problems. **Amber** means that a database has significant problems, and may be unlawful. Depending on the circumstances, it may need to be shrunk, or split, or individuals may have to be given a right to opt out. An incoming government should order an independent assessment of each system to identify and prioritise necessary changes. **Green** means that a database is broadly in line with the law. Its privacy intrusions (if any) have a proper legal basis and are proportionate and necessary in a democratic society. Some of

- INDENT1, the National Fingerprint Database ('NFD'), (criminal), gets a green light (one out of only six green lights)
- CRS, the Border Agency's Central Reference System that holds information on people entering and leaving the country, including visas, is given the amber light
- The Immigration and Asylum Fingerprint System (see below UK biometrics programme) obtains an amber light
- NDAD, the Border Agency's Central Reference System that holds information onpeople entering and leaving the country (see below UK biometrics programme) gets an amber light
- PNC, the Police National Database that contains a wide range of information to support police operations, holds intelligence data and links to many other systems including biometric SIS data from 2010 receives an amber light
- UKvisas Biometrics Programme receives an amber light[414]
- C-Nomis, The National Offender Management Service's system, now part of Omni, used to run prisons: amber light[415]
- (NDNAD) The DNA database which holds DNA profiles taken from crime scenes, suspects and witnesses is shown the red light[416]
- NIR, the National Identity Register, receives a red light
- ID cards (connected to NIR) receives also a red light.[417]

The following database relate to European data sharing:

- SIS, the Schengen Information System, is shown the amber light; and
- Data sharing agreements within the Prüm Framework receive a red light.[418]

Out of the ten recommendations in the report, we will highlight two that are particularly relevant for the use of biometrics in government databases.

Following up on the conclusion that the UK public sector is starting to rely on systems that will have to be changed drastically once a litigant takes a case to Europe, the first recommendation is that government system builders should set out to comply with the ECHR rather than avoid it.[419] According to the authors, the existing mismatch has been made quite

---

these databases have operational problems, not least due to the recent cavalier attitude toward both privacy and operational security, but these could be fixed once transparency, accountability and proper risk management are restored.

[414] *Database State*, p. 24.

[415] *Ibid.*, pp. 26-27.

[416] *Ibid.*, p. 21

[417] *Ibid.*, p. 25.

[418] *Ibid.*, p. 39.

[419] The first recommendation is that *'Government should compel the provision or sharing of sensitive personal data only for clearly defined purposes that are proportionate and necessary in a democratic society. Where consent is sought for further sharing, the consent must be fully informed and freely given."*[419] The third recommendation of the report follows from there: *"The systems rated amber in this report should be subjected to an independent review, for both their privacy impact and their overall benefits to society, while the systems rated red should either be scrapped (ID cards, communications database) or rewritten to support effective opt-outs (NHS Secondary Uses Service).' Ibid.*, pp. 41-42.

clear first by *I v Finland*, which upholds a patient's right to keep her medical records private from clinical staff not involved in her care, and *S & Marper v UK* in which the National DNA Database was found in breach of ECHR (see *above* section 2.2.1).

The tentative conclusion from this section is that some very detailed and critical reports have been written but so far have not resulted in a change of course. That course is that the UK is rapidly introducing large scale biometric applications, and that the possibilities and opportunities for central storage and interlinking of data are explored rather than avoided.

## *8.3 Legislation regulating the use of biometric data*

### 8.3.1 General and specific privacy legal framework for biometrics

The national legal privacy framework for biometrics is the Data Protection Act 1998, which came into force in March 2000 (hereinafter the 'DPA 1998') which is in principle applicable to the collection and processing of biometric data. However, the DPA 1998 does not contain specific provisions which mention biometric data as such.

There are a number of separate instruments at the national and international level that would apply to certain aspects of the use of biometrics. As apart from DNA cases, there are no cases involving biometrics yet. Therefore, an analysis will have to be carried out on the basis of existing case law involving personal data.

As stated above, according to Art 3 (2) and recital 13, the Directive 95/46/EC does not apply to the processing of data in the course of an activity which falls outside the scope of European Community law, such as provided for by Titles V (provisions on common foreign and security policy) and VI (provisions on police and judicial cooperation in criminal matters) of the Treaty on European Union. Activities that are processing operations concerning public security, state security and the activities of the state in areas of criminal law therefore all fall outside the scope of the Directive.

Certainly, all matters relating to passports and national ID cards are not regulated by the Directive 95/46/EC and find their legal basis in UK legislation. For example, as already discussed above, the legal base for biometric data processing has been a major issue in the build-up to the adoption of the Identity Cards Act 2006.[420]

It is clear that beyond the directly applicable national legal framework, the right to privacy and the use of biometrics is complex. This applies especially to the use of biometrics in the context of the fight against terrorism.

### 8.3.2 Legal provisions for government controlled ID biometric applications

*The UK National Identity Scheme*

The UK national identity system, also called the National Identity Scheme (NIS), is the main government initiative with regard to the use of biometrics in the UK. The scheme, based on the Identity Cards Act passed in March 2006, will provide a comprehensive way of recording

[420] See for example the abovementioned *The Identity Project.*

personal identity information, storing it and making it possible to use it if one wants to prove his or her identity. The NIS will apply to all those over 16 years old, including foreign nationals, who legally reside or work in the UK.[421]

The NIS is a long-term programme which will take several years before it becomes fully operational. The UK government envisages that the scheme will protect the public against identity theft and fraud. Other expected benefits include increased safety, through protection of the community against crime, illegal immigration and terrorism, and reassurance that workers in positions of trust, such as those working at airports, are who they say they are.

The scheme is set to compound the deployment of government controlled biometric applications such as biometric visas, enhanced passports and identity cards, including those cards issued to foreign nationals in the form of biometric immigration documents.

Notwithstanding the title of the Identity Cards Act, the basis of the Act is not the ID card but a *database* (The National Identity Register ('NIR')) containing information relating to individuals. The ID card will only be issued after the required "registrable" facts have been entered into the NIR.[422] A registrable fact in relation to an individual includes personal information which is defined as 'his full name', his other names by which he is or has been previously known, data and place of birth, date and place of death and 'external characteristics of his that are capable of being used for identifying him'.[423] The term 'identifying information' is also used in the Identity Cards Act and applies to biometric data especially. The Act refers to a photograph of head and shoulders, fingerprints and 'other biometric information' as well as to a handwritten signature. Iris scans are not mentioned in the Act. The Identity and Passport service has set up a website that also devotes special attention to biometrics. On the website facial recognition is mentioned but also "the features of the iris and other parts of the eye".[424]

This and other explanations in publications of the Identity and Passport Service indicate that options are left open to include other biometrics as a later stage.[425] By using the term 'identifying information' as a label for biometric data, the UK legislator shows that it places its trust primarily on biometrics for the authentication of identity.[426]

The identifying information (including biometric data) is recorded in Schedule 1 that contains eight other categories of information.[427] When a person enrols, biometric information (e.g. facial image, fingerprints) will be recorded, and there are mobile and local centres that are

---

[421] Identity Cards Act 2006 ('Identity Cards Act') section 2 (2)(b). The Identity Cards Act can be consulted at < http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060015_en.pdf>.
[422] Identity Card Act section 6 (6) and (8).
[423] Identity Card Act section 7 (1).
[424] See http://www.ips.gov.uk/identity/scheme-what-produced.asp
[425] New biometric identifiers can be introduced through the procedure as described in Section 3(6) of the Identity Card Act. See also *below*.
[426] The website for example explains: 'Your biometrics will be permanently paired with your biographical information to create completely unique and secure identity data'. See http://www.ips.gov.uk/identity/scheme-what-produced.asp
[427] This information is: the fore mentioned personal information, residential status, personal reference numbers, record history, registration and card history, validation information, security information and records of provision of information. It is important to note that the categories of information in the register can be changed at a later date: under the Act section 3(6) the Secretary 'may by order modify the information for the time being set out in schedule 1'. Under section 3 (7) of the Act, the draft order must be laid 'before Parliament and approved by a resolution to each House'.

equipped to register these kinds of data. The basic identity information will be recorded and maintained on the NIR. The NIR will thus contain only identity-related information.

As it stands, medical records, tax and benefits information and other government records are not stored in the NIR. Of course, an important legal issue is whether registration under the Act is *compulsory*. Registration is only required for certain groups of people, such as all individuals requiring a new passport and individuals subject to compulsory registration as mentioned in section 7(1)a of the Act. An individual subject to section 7 must register and apply for an ID card. The definition of compulsory registration is worded like this: 'required to be entered in the Register in accordance with an obligation imposed by an Act of Parliament passed after the passing of this Act.'[428] So the individuals to whom this applies are as of yet unknown as they may only be required to register as a result of future primary legislation. The number and *kind of groups or individuals that will be compulsory registered* in the future is therefore *left open* and difficult to assess.[429]

As soon as a person is registered, this person becomes also under an obligation to notify changes and errors.[430] In the case of the registration of biometric data, this means that as soon as individuals become aware of an error in (the recording of) their biometric data, notification of this is compulsory on pain of civil penalty.[431] Therefore all British passport holders will eventually be on the NIR on a compulsory basis and will also be under an obligation to report errors/abuse they observe relating to their biometric data.[432]

The NIR is not intended as a single, large, database.[433] The different sets of NIR information – biometric, biographical and administrative – are not all held in a single system, but stored *compartmentalized* to maximise the safeguarding information. The register has links with other government systems to share identity data, and supports identity checking services.[434]

The ID cards themselves combine the cardholder's biometric data with their checked and confirmed biographical information covering basic personal details (e.g. name, address, date of birth). A sub-set of the identity information held on the NIR is also printed on an identity card – a photo card with an electronic chip.[435] The chip holds the identity information as printed visibly on the card such as a digital photograph but also contains two fingerprints. Each card has its own Identity Registration Number (IRN), which is printed on the card and a Personal Identification Number (PIN), which the cardholder can set and use as one would for a credit or debit card.

---

[428] Identity Card Act section 42.
[429] See the explanatory notes to the Identity Card Act: http://www.opsi.gov.uk/acts/acts2006/en/ukpgaen_20060015_en_1.htm, see especially note 58.
[430] Identity Card Act section 10 (1).
[431] Identity Card Act section 10 (1). The maximum penalty is 1000 GBP.
[432] For a more detailed discussion of the complicated issue of compulsory registration, voluntary consequence, compulsory obligation and compulsory consequence flowing from compulsory obligation resulting from the Act see Sullivan, C., 'The United Kingdom Identity Cards Act 2006- Civil or Criminal?', *International Journal of Law and Information Technology*, vol. 15, issue 3, pp 328-330.
[433] Home Office, *National Identity Scheme Delivery Plan 2008*, p. 25, available at < http://www.ips.gov.uk/passport/downloads/national-identity-scheme-delivery-2008.pdf>, last consulted 23 February 2009.
[434] Home Office, *Strategic Action Plan for the National Identity Scheme*, December 2006, p. 7, available at < http://www.ips.gov.uk/passport/downloads/Strategic-Action-Plan.pdf> ('*Strategic Action NIR Plan'*).
[435] Home Office, *Identity Cards Act Secondary Legislation: A Consultation*, available at < http://www.ips.gov.uk/identity/downloads/NIS_Legislation.pdf>, last consulted 23 February 2009, p. 10.

Accredited organisations (that can be both public and private sector organisations such as banks) can check an ID card and/or an NIR record with the *permission* of the holder. In this case, different levels of verification apply, depending on the service a person wants to access.[436] Basically, an individual's identity data or information as presented *will be compared* with his/her entry in the NIR.[437] There are three levels of verification. The lowest level is a check using the photo on the ID card. The next level involves multi factor verification: a check of the physical card including the photo and the use of the personal identification number (PIN) and/or designated questions. The highest level check includes biometrics. Under the NIS correlation is considered to be verification. A check is only made on whether data match, whilst the validity of these matching data is not checked.

As the accuracy of the biometric information itself is not checked, this makes the accuracy and safety of the NIR potentially vulnerable. In terms of biometrics, it places extra importance on accurate enrolment. The assumed reliability of biometric data might otherwise give a false sense of security. Of course, a low false acceptance rate (FAR) and the false rejection rate (FRR)[438] in trials carried out by independent labs is the first requirement for the safe use of biometrics. At the same time, other external factors have an even greater impact on the reliability of the identification and authentication process in large scale applications. To mention a few: racial and age diversity, circumstantial factors such as light or stress non-cooperation factors and fraud and sabotage. The latter can express itself in, for example, manipulation of the equipment, government infrastructure break in, 'spoofing' and sabotaging of the enrolment or authentication process. These factors are often difficult to assess and have never been tested at a large scale and/or over a long period of time. At the same time, some authoritative claims or predictions have been made in the UK in this respect (see national studies *below*).

As regard to the security of the scheme, there are integral functions that will oversee and manage the scheme in order to provide safeguards and to make sure the scheme is properly run and is supported by the proper legislation and regulations.[439] The Home Secretary is ultimately responsible to Parliament for the running of the scheme. The yet to be established independent National Identity Scheme Commissioner will continually review the operation of the scheme and report to the Home Secretary, who has to share the report with Parliament and answer MPs' questions. Finally, the Information Commissioner's key powers to protect personal information will also apply to information held in the NIR.

The most recent information indicates the following timeframe and milestones in the implementation process of the scheme.[440] The first identity cards have been issued on the 25th November of 2008 in the form of biometric immigration documents to *foreign nationals* from

---

[436] For example, a financial institution may ask for proof of identity before completing certain transactions and will wish to check the validity of the ID card when it is presented. Section 12 of the Act provides the legislative authority for the release of information.

[437] Identity Card Act section 7 (3)(a). See also Identity Card Act section 10 (3)(a).

[438] To give an indication: in the context of national identity management in general a FAR of 0,1 % and a FRR of 5,0% are regarded as acceptable result scores for biometric authentication under supervision (see, for example, European Biometrics Forum, *Biometrics in large Scale Systems*, available at < http://www.eubiometricsforum.com /dmdocuments2/3rdEBFRSMaxSnijder.ppt>, last consulted 11 March 2009)

[439] *Strategic Action NIR Plan'*, p. 7.

[440] Home Office, *National Identity Scheme Delivery Plan 2008: A Response To Consultation*, available at <http://www.ips.gov.uk/identity/downloads/ConsultReportv2.pdf>, last consulted 23 February 2009, p. 7.

outside the European Economic Area.[441] Also in the second half of 2009, the Home Office will make a start with the issuing of identity cards to British and foreign nationals working in *sensitive roles or locations*, starting with airport workers.[442] From 2010 on, the Home Office intends to start issuing identity cards to young people, albeit still on a *voluntary basis*. Finally, from 2011/12, the Home Office will start to enrol British citizens at high volumes offering a choice of receiving a separate identity card, a passport or both. Both documents will carry biometric data.

*The ePassport*

In March 2006, the UK made a transition from digital to electronic passports (ePassports) in order to comply with the US Visa Waiver Programme and other international requirements.[443] The main aim was to strengthen border controls. The ePassport contains an electronic chip storing biographical data and a digital facial image of the passport holder. The chip can be read using an appropriate electronic reader located at border control.[444]

To conform to other EU requirements specifying that electronic passports within the EU should include a second biometric identifier in addition to the face scan (digital photograph) by 2009, the UK plans to issue second generation ePassports soon.[445] These passports will store the holder's finger scans on the chip.[446] Although the chip units (chip, its operating system, the antenna and the plastic covering in which it is housed) have been tested in laboratory conditions, their ability to withstand real-life passport usage is unknown.[447]

*Other government controlled applications*

Next to the identity card and the ePassport, the UK is also using biometrics in other government controlled applications. When viewed in the light of the list of the Parliamentary

---

[441] The contract for the early releases was given to Thales in August 2008. In the second half of 2009, the award of contracts for application and enrolment, biometrics storage systems and the production of identity cards and passports will take place.This means a delay in the original schedule. The information was given in reply to a question [224718] by MP Huhne on 25th November 2008. See http://www.parliament.the-stationery-office.com/pa/cm200708/ cmhansrd/cm081125/text/81125w0020.htm

[442] The Identity and Passport Service has commissioned National Identity Scheme Tracking research. The research is carried out "in waves" by IPS, Business Development and Marketing. The results are published on the internet. In the fourth wave (May 2008) of those British citizens questioned, 64% were not aware of the plans to introduce the first cards to airport workers.

[443] House of Commons Committee of Public Accounts, Identity and Passport Service: Introduction of ePassports, available at <http://www.ips.gov.uk/passport/downloads/Introduction_of_ePassports.pdf>, last consulted 23 February 2009, p. 7.

[444] The ePassport was the first official UK document to incorporate an electronic chip in a paper document and it incorporates technically advanced security features to make it harder to forge and prevent unauthorised reading of the chip.

[445] As stated above, the UK is not obliged to comply with the EU regulations as it is not a signatory of the Schengen Agreement. Nevertheless it has decided to participate on a voluntarily basis. This secures participation in the development of the EU regulations in this area and helps maintain the security of the British passport on a par with other major EU nations.

[446] Although planned for 2009, there may be a slight delay in including finger scans in British passport chips. The reasons for this delay have not been made public.

[447] In the UK, there have been reports of doubts on the durability and reliability of the chip units used. British ePassports are intended to last ten years but the RFID chip units used only have a two year warranty. Compare also with footnote 440, p 2.

Under-Secretary for the Home Office in 2003,[448] apart from the introduction of the NIR, the most important biometric applications used by the British Government have not changed since then. The three major ones are hereunder briefly described:[449]

- Through the UK visas Biometrics Programme, biometric visas (fingerprints) are being issued to *foreign nationals* who wish to enter the UK and *require an entry visa*. The programme covers three quarters of the world's population and operates in 135 countries. More than one million fingerprint scans have been completed.
- The UK Border Agency operates the Iris Recognition Immigration System (IRIS) at some UK airports which provides a fast, secure and convenient way for *foreign and returning UK travellers* to enter the UK.
- The fingerprints of *asylum* seekers are recorded when they register for an Application Registration Card (ARC).

*The national DNA database*
In general, DNA (deoxyribonucleic acid) is not considered a biometric. At the same time, DNA also contains information that will uniquely identify a certain person. Because of that reason, and because of major (worldwide) attention for this database, we nevertheless discuss hereunder the in the UK existing DNA database.[450]

The national DNA database (NDNAD) in the UK (comprising in this instance England & Wales and Northern Ireland; Scotland has a separate DNA database with different rules) is the largest in Europe, with liberal rules for taking and retaining DNA samples and profiles compared to other European countries. It is possible in the UK to retain bodily samples and DNA profiles upon arrest for any offence, regardless of whether a charge and conviction follows. With the DNA of 940,000 people on file the UK has the most "profiled" population in the world.[451] Recently, there have been a number of significant developments in the use of DNA profiling techniques in law enforcement. The government has announced an increase in funding to enable the UK DNA database to be more rapidly expanded – at the end of 2008 the number of profiles held was rising at the rate of 6,000 per week.

In view of the fact that EU Member States have already started exchanging DNA profiles, all profiles collected in the UK can potentially be used by authorities in other EU Member States. By its Decision of 23 June 2008,[452] the European Council agreed to integrate the main provisions of the Prüm Convention into the EU's legal framework, to enable wider exchanges (between all EU Member States) of biometric data (DNA and fingerprints). All EU Member States will therefore be required to set up DNA databases. The Framework Decision on the

[448] See http://gizmonaut.net/blog/2006/12/03
[449] Biometrics Assurance Group, *Annual Report 2007*, available at < http://www.ips.gov.uk/passport/downloads/FINAL-BAG-annual-report-2007-v1_0.pdf>, last consulted February 2009, p. 4.
[450] We will not discuss the interface between bio banks and the storage of biometric(s) (templates). This has been done elsewere. See http://www.jus.uio.no/iri/om_iri/seminarer/Bodycontrol.html
[451] In September 2008, the government announced an extra £109 million to expand the database (this comes after the extra £34 million announced in September 1999).
[452] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJ* L 210, 6.8.2008.

protection of personal data in the field of police and judicial cooperation in criminal matters – is the first general data protection instrument in the EU third pillar.[453] In this decision the option of a future European database is not excluded.

In the UK, police are only allowed to keep DNA profiles on the national database from people who are convicted of the offence for which the sample was taken. All other samples must be destroyed. However, a Home Office Inspectorate of Constabulary report, '*Under the Microscope*', estimated that from 752,718 DNA profiles held at the time of their study, those of 50,000 individuals which should have been destroyed have been retained.[454] This figure was based on a non-conviction rate of 20%.[455]

There have been individual court cases about illegally retained DNA samples. In 2008, Michael Weir's conviction for murder was quashed at the Court of Appeal. Weir had been convicted on the strength of DNA evidence based on blood found on a glove.[456] The Court affirmed the rules of the Police and Criminal Evidence Act 1984 which state that '*information derived from the sample of any person entitled to its destruction [...] shall not be used - (a) in evidence against the person entitled; or (b) for the purposes of any investigation of an offence. If the sample was used for purposes of an investigation then all evidence resulting from that information must be excluded.'*[457]

There is also a case pending involving three Police Federation backed police detectives who object to having been assigned desk-jobs as a result of failing to provide a voluntary sample.[458]

The last case to be mentioned here is the European Court of Human Rights judgment of 4th December 2008, in the case of *S. & Marper v. the UK*. [459] The ECHR Grand Chamber (GC) found unanimously that the retention by the police of fingerprints and DNA samples from a man and a boy arrested, but not convicted, violated their right to privacy. The judgment provides a landmark decision setting limits to the growth of national DNA databases in general, and that of the UK in particular. The case had previously been rejected by the House of Lords, which had placed the importance of crime detection above issues of data privacy.

---

[453] See above, section 2.4.

[454] Home Office, *Under the Microscope*, available at < http://inspectorates.homeoffice.gov.uk/hmic/inspections /thematic/utm/microsco.pdf?view=Binary>, last consulted 11 March 2009.

[455] According to Statewatch (<http://www.statewatch.org/news/2008/dec/uk-dna-database-background-article.pdf>), more realistic figures would be non-conviction rates of 33 and 45% - suggesting that 82,UK 500-112,500 DNA profiles should actually have been destroyed.

[456] The police matched the blood to a DNA sample taken from Weir a year previously when he was suspected of drugs offences. At the time, he had not been charged. Nevertheless, his profile was placed in the national register.

[457] Section 64 (3B) of Police and Criminal Evidence Act 1984.

[458] According to Statewatch (<http://www.statewatch.org/news/2008/dec/uk-dna-database-background-article.pdf >) UK the Home Office has confirmed that at least 50,000 people's DNA profiles are held illegally, but are yet to state what is being done about it.

[459] For the implications and the arguments in the case, see *above* and at http://www.bailii.org/eu/cases/ECHR/2008/1581.html. That there were fundamental issues at stake is reflected in the fact that the case was put before the 17 judges of the Grand Chamber. It shall be particularly noted here that the Court gave a very broad definition to the concept of privacy within the meaning of Article 8 – the right to privacy. The Court had no hesitation in viewing fingerprints and DNA samples as falling within the ambit of Article 8. For the original case see: *Regina v. Chief Constable of South Yorkshire Police ex parte LS/ ex parte Marper* [2004] UKHL 39, http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040722/york-1.htm

The applicants had subsequently applied to Strasbourg under Article 8 (the right to privacy) and Article 14 (non-discrimination).

## 8.4 Legal measures in response to specific threats by biometric systems

The ICO has proposed some legal measures to further protect private data, also with a view to possible security lapses that concern biometric data. In his evidence to the House of Commons Justice Committee inquiry into the protection of private data, the ICO made two specific proposals.[460] The first is to give the ICO the power to force data holders to commission *an independent audit* of their procedures. The second is a requirement for bodies to notify the ICO or a similar body, when a major and potentially *dangerous privacy breach* has occurred, as well as notifying the individuals who may be affected.

The UK government plans to increase penalties for trading in personal data, from a fine as currently set to two years imprisonment under new penalties in the Criminal Justice and Immigration bill.

## 8.5 The National Data Protection Authority on biometrics

At the top of the UK Information Commissioner's home page, the mission of the ICO is stated as follows: 'the UK's independent authority set up to promote access to official information and to protect personal information'.[461]

The House of Commons Home Affairs Committee has issued a report on the Surveillance Society[462] which was discussed above. In his response to the report, the ICO supported the proposal that the Home Office should submit *contingency plans for the loss of biometric* information to ICO.[463] The Committee also recommended that the Home Office should address ICO concerns on administrative information collected as part of the National Identity Register (paragraph 248 of the Report). In its reply, the ICO stressed its continuing concern that the amount of information is *to be kept to the minimum* with administrative information deleted as soon as it has served its purpose. The ICO states it is particularly concerned about the 'audit trail' data and wants this minimised, access restricted and early deletion.[464] In its reply, the ICO also supported the Committee's recommendation that the Home Office submits detailed plans for *securing NIR databases and contingency plans* for the loss of biometric information to ICO for comment (paragraph 246 of the report). The ICO confirmed that it

---

[460] House of Commons Justice Committee, *Justice – First Report*, available at < http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf>, last consulted 11 March 2009.

[461] See the site www.informationcommissioner.gov.uk .

[462] Constitution Committee, *Fifth Report session 2007-2008: A surveillance Society?*, available at < http://www.publications.parliament.uk/pa/ld200708/ldselect/ldconst/44/44.pdf>, last consulted 11 March 2009.

[463] House of Commons Home Affairs Committee, *A Surveillance Society? Information Commissioner's Response to the Committee's Fifth Report of Session 2007–08*, available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/1124/1124.pdf , last consulted 11 March 2009, p. 6.

[464] *Ibid.*, para. 6.8.

would welcome the opportunity to provide comments on the data protection implications of the Home Office and IPS plans. [465]

In January 2009, the ICO forced the Home Office to sign a *formal declaration* promising to hold personal data securely in the future.[466] With immediate effect, all portable and mobile devices which are used to store and transmit personal information must be *encrypted*. The case in question occurred in August 2008 when a Home Office contractor, PA Consulting, lost an unencrypted memory stick holding sensitive personal details of thousands of people serving custodial sentences or who had previously been convicted of criminal offences.[467]

## 8.6 Conclusion

In the European context, the UK plays a pivotal role in the roll out of biometrics, at least in the public and in the semi-public domain.

Both in policy and in legal terms, regulation of biometrics takes place at the liberal end of the spectrum. Cases such as *Marper*, and the subsequent challenge of implementing the Court's decision, are a test for this liberal approach. The impact on society of the policies that have been initiated in recent years has only just begun to show.

As a result of the pioneering nature of the use of biometrics in the UK, the outcome of current political processes will without doubt also have an impact on developments in the EU as a whole.

[465] *Ibid*, para 6.7

[466] The ICO has ordered a number of organisations to sign undertakings following breaches of the Data Protection Act. These include the Department of Health, Foreign and Commonwealth Office and Orange Personal Communications Services Ltd.

[467] Mick Gorrill, assistant Information Commissioner, issued the following statement: "This breach illustrates that even though a contractor lost the data, it is the data controller (the Home Office) which is responsible for the security of the information. It is vital that sensitive personal information is handled properly and held securely at all times. The Data Protection Act clearly states that organisations must take appropriate measures to ensure that personal information is kept secure. The Home Office recognises the seriousness of this data loss and has agreed to take immediate remedial action. It has also agreed to conduct future audits to ensure compliance with the Act. Failure to meet the terms of the Undertaking is likely to lead to further enforcement action by the ICO". See http://www.karoo.co.uk/article.asp?id=18987429&cat=headlines. See also Information Commissioner's Office, *ICO takes enforcement action against NHS Trusts for data losses*, available at <http://www.ico.gov.uk/upload/documents/pressreleases/2009/nhs_trusts_undertakings_final.pdf>, last consulted 11 March 2009.

# 9 Conclusions and Recommendations

In general, the existing legal framework *does not provide clear answers* to the issues which are raised by the use of biometric data. Present legal provisions stipulate that personal data which are 'adequate, relevant and not excessive' shall be processed 'fairly and lawfully', 'for specified, explicit and legitimate purposes' and shall not be 'processed in a way incompatible with those purposes' (see Article 6 Directive 95/46/EC). It is not clarified what these notions mean for the applications which process biometric data. As a result, interpretations vary, resulting in sometimes opposing opinions or advices from national data protection authorities on similar data processing applications.

Case law is expected, but is certainly not abundant yet.[468] Such case law may clarify some issues, but is in principle only valid for the specific circumstances of the case, and is therefore not apt to regulate in general the recurring issues of biometric data processing. Therefore, initiatives on the regulatory level are not only desirable but required in order to mitigate the (legal) uncertainty.

The Directive 95/46/EC furthermore *requires* Member States to identify data processing which are likely to present specific risks. DPAs of various Member States have pointed to the risks of biometric data and have issued guidelines, but most Member States have not yet taken specific legislative action in order to protect the rights and the freedoms of the data subjects with regard to the processing of biometric data so far. Only in exceptional cases, prior authorization by the DPA is required before the start of biometric data processing (e.g., France). [469]

For these reasons, and based upon various studies and reports, guidelines and opinions of the Article 29 Data Protection Working Party, the EDPS and the national DPAs, suggestions and recommendations for some headlines of a legal framework are hereunder made. These recommendations aim at basically the use of biometric data in the private sector (as opposed to the public sector) and propose to enact some general limitations in relation with the processing of biometric data. In case the legislator would not opt for such limitations, the processing of biometric data could be subject to well specified conditions for the processing of such data.

## *9.1 Conclusions from the current legal framework, reports and opinions of the DPAs and the EDPS and the country reports*

*The existing legal framework*

The present legal framework which applies to the processing of biometric data, in particular the Directive 95/46/EC and most national data protection legislations, *does not regulate* the

[468] Exceptions includes the important case ECHR, *S. and Marper v. United Kingdom* [GC], no. 30562/04 of 4 December 2008, which clarified some aspects of biometrics, such as with regard to the proportionality of the central storage and retention of DNA and fingerprint. Other exceptions include the French decision of the Conseil d'Etat, App. N° 297888, 297896,298085 of 13 March 2007 which pointed to the requirement of a legal basis for setting up a central database with digitised photographs, and the German decision of the labour court of 24 January 2004 which requires the approval of the workers' council or arbitration board for the installation of a biometric entrance control of workplaces.

[469] Such procedure of prior authorization puts often an important workload on DPAs which have already sometimes too limited means to execute their tasks.

numerous specific issues[470] which result from the processing of biometric data. DPAs in most countries issue guidelines on the processing of biometric data, for example, the requirement that templates instead of raw data shall be used or that alternative control procedures shall be set up, but these guidelines are not binding.

In the discussion about the existing legal framework in section 2 above, it was already demonstrated with various examples that the existing Directive 95/46/EC does not provide clear answers to the issues posed by biometrics (see in particular section 2.3).

The Working Document on Biometrics of 2003 which contains guidelines also does not resolve all issues presently identified and relating to biometrics. These issues include that biometric data can be used (and misused) for identification purposes which affects the fundamental rights of the data subjects.[471] For such identification, there should in principle be a clear legal basis authorizing such identification. The Article 29 Data Protection Working Party should also attach consequences to the fact that the FRR and the FAR are set by the controller/operator according to the purpose of the system, hereby invisibly increasing or decreasing security while the collection of biometric data from the data subjects will still remain required.

The Working Document on Biometrics of 2003 also suggests that national legislators should provide for the requirement of prior checking of biometric applications with the national DPAs.[472] The requirement of prior checking, however, does not provide legal certainty as to the deployment of biometric operations. DPAs take varying elements in their case to case analysis into consideration. It further may lead to conflicting decisions. It is also not practical since DPAs become overwhelmed by requests.[473] We therefore recommend that the conditions for the use of biometric data are set forth by legislation. The Article 29 Data Protection Working Party on the other hand rightfully points to the need of legislation where biometric data is used as an (unique) identifier of general application.

Although the technology is still evolving considerably, the biometric characteristics that are most often used are known, including most risks associated with the use of these characteristics, such as the inclusion of health related and other sensitive information, the use of it as identification tool and, in case of central storage, the use as unique identifier enabling linking information from various sources and the re-purposing of data initially collected for other objectives. Biometric characteristics could hence be abused in many ways, including by using the information collected by the private sector for purposes of law enforcement. For these reasons, a regulation of the use of biometric characteristics is justifiable. Such regulation should provide a binding framework within which biometric data shall be processed.

---

[470] These specific issues were as stated above to a large extent already spotted by the Article 29 Data Protection Working Party in its Working Document on Biometrics of 2003 and in its subsequent opinions on various proposals for large scale biometric data processing in the EU, such as for the epassports, VIS and SIS II. See also various reports, including the report of the Council of Europe, *o.c.*at footnote 18, The privacy and security aspects of biometrics were also described in literature and in various Fidis reports, including in E. Kindt and L. Müller (eds.), *o.c.*, FIDIS, 2007.

[471] 'Identification' is to be clearly distinguished from 'identification verification' as stressed before.

[472] France, for example, has adapted it national data protection legislation in this way in 2004.

[473] The French DPA has therefore issued unique authorisations.

*The country reports*

In almost all countries studied in this report, the general processing of biometric data is *not subject to specific legislation* which completes the general data protection legislation and Article 8 ECHR. France is one of the few countries that have adapted its legislation due to the emergence of biometric applications. The data protection legislation in France has been modified in 2004 and requires that if biometric data is processed for identity verification, it shall be submitted for prior checking to the CNIL. If such processing is done by (or on behalf of) the government, a decree (*'décret')* is required (after advice from the CNIL). French national legislation, however, does not provide more conditions or criteria for the processing of biometric data.

The debate about the introduction of biometric application is taking place at different times in the countries studied. In the Netherlands, some debate took place at the end of the nineties with the report *At face value.* In Germany, a first wave of discussion started end of the 1990s, leading to the first TeleTrusT project on biometrics from 2001 to 2003 and resulting in various publications. The debate arose thereafter again, in particular in the context of the introduction of the epass. In France, the matter retained the attention of the parliament in the period of 2002 - 2005, and in the United Kingdom and Switzerland, the debate seems more recent. Overall, however, the debate was rather limited. In case consumers were questioned about the introduction of biometrics, ease of use was a major factor for these consumers for being positive towards the introduction of biometrics. Whether the information about biometrics that was provided to these consumers included also information about the risks of the use of biometrics is not clear, however.

In some countries, the introduction and the use of biometric systems in the working environment has been made subject to co-determination rights of employee representatives (e.g., Germany). It is also interesting to note that in some countries, there is a suppliers' driven promotion for the use of biometric applications.

In most countries, the national DPAs (e.g., in Belgium, France, the Netherlands and Switzerland) have issued *guidelines, advice or recommendations* for the use of biometrics[474] in addition to opinions on specific biometric systems.

In all countries, the introduction of biometric identifiers in the epass is important and some legislative changes are being or have presented to the national parliaments. Some countries also consider the introduction of biometrics in the eID and plan to use such eID card as a universal token for authentication and identification (see, e.g., Germany; the inclusion of fingerprint however would be optional).

In countries such as France, Germany and Belgium, position is taken *against* the storage of biometric data in (central) *databases* because of the various additional risks such storage entails (e.g., unintended use for law enforcement purposes, other use without knowledge and function creep, ….). There is a clear preference for *local storage* of the biometric data, for example on a card or token. Only in a few countries, the position against central storage is confirmed in some specific legislation, e.g., on the collection and use of biometric identifiers in passports, where for example German legislation forbids the storage of fingerprints in a central database. However, the DPAs do not exclude all storage in central databases, and

[474] These recommendations are sometimes rather technical (for example, Switzerland).

provide some criteria (e.g., France, Belgium, …) which shall be applied in order *to evaluate whether central storage could be acceptable*. Various countries (such as Belgium, France and Switzerland) stress in the DPA guidelines *the risks of the use of biometric characteristics which leave traces* (such as e.g., fingerprint, face, voice…). In the Netherlands, there is preference for storage in a central database for Type I government controlled ID applications. It is disturbing, however, that there is uncertainty to what extent access may be granted to law enforcement in search of suspects. In this way, biometric applications are turned into Type V surveillance applications.

Where required under the legislation (France), the DPAs issue *prior authorizations* for the use of biometrics. In France, where the CNIL issued three 'unique authorizations' so far, these prior authorizations permit to simplify the notification procedure for the controllers (and the DPAs). However, if the biometric data processing operations do not *fully* comply with *all* (detailed) conditions (e.g., because of the nature of the data or term of storage), prior authorization remains required.

For some countries, the authors mention the need for more effective enforcement of the data protection legislation. In many countries, such as in the Netherlands and Belgium, but also in France, the DPAs cope with staff shortage and sometimes lack of powers for an adequate supervision of the use of biometrics.

To conclude, the DPA in the United Kingdom also proposed more legal measures to protect data, including a requirement to notify when a major and potentially dangerous privacy breach has occurred.

## 9.2 Recommendations

*Preliminary remarks*

The suggestions relate to the regulation of biometric applications. Such regulation may take many forms, including by self- or co-regulation (for example by establishing (business or ethical) codes of conduct), but also by taking legislative action on the national or international level. We hereby do not review the various ways in which such regulations can be established, as this is out of the scope of this report. The suggested recommendations do also not only relate to modifications to the Directive 95/46/EC or to the enactment of specific legislation, as legislative action could take many forms.

The recommendations hereunder further mainly focus on the use of biometric applications, primarily in the private sector, whether for commercial or non-commercial purposes, by public and private controllers. Some general recommendations will also address Type I government controlled ID applications. The recommendations do not concentrate upon the use of biometric systems for law enforcement or other purposes which are within the so-called third pillar (e.g., the use of biometric data in SIS II).

*Recommendations*

In addition to the application of Directive 95/46/EC and Article 8 ECHR to the processing of biometric data, the following can be recommended:

➔ The existing legal framework for biometrics is in essence an 'enabling legal environment' regulating the use of biometrics but in fact lacking normative content.[475] For that reason, *more specific rules are needed* which prohibit use where there are disproportionate power balances.[476] Such legislative initiatives have to be sufficiently precise. Regulation which provides for the use of biometrics 'for security purposes only' is superfluous.[477]

Most of the analysis and the country reports mentioned in this deliverable refer to opinions or positions of institutes or authorities (in many cases of DPAs and the EDPS) which have studied biometrics. DPAs and the EDPS have clearly indicated that there are numerous risks of central databases with biometric data. They opt for a *clear rejection, to a greater or to a lesser extent, of the central storage of biometric data in databases*, because of the risks.[478] These risks increase if the databases contain biometric characteristics which leave traces or can be collected without the knowledge of data subjects, such as fingerprint, face, voice, but also DNA.[479] But only few countries, such as Germany, have enacted laws which forbid the establishment of central biometric databases. In that case, such legislation is mostly in relation with a specific biometric application, such as the epassport.

The present data protection legal framework does not (explicitly) forbid central databases. Only the application and the interpretation of general principles may point towards an obligation to avoid central databases. In case of biometric data, a central database with biometric data will in most cases be contrary to the right to privacy as guaranteed by article 8 ECHR because of the various reasons summarized in this and in the previously mentioned FIDIS deliverables.[480] Interference with this right is only acceptable if there is a legal basis, the interference is for a legitimate purpose defined in article 8 ECHR (e.g., national security or public safety) and the interference is necessary in a democratic society. The evaluation of this last mentioned requirement is quite complex. The necessity in a democratic society requires that (i) there is a pressing social need for such central database, (ii) the database is relevant and sufficient and (iii) the interference with the privacy rights of the data subject is necessary (i.e. there are no alternative means which can be used to reach the purposes) and in proportion with the (legitimate) aims pursued (e.g., public safety). These different steps in the evaluation as to whether interference with the fundamental right to privacy is acceptable,

---

[475] DG JRC and IPTS, *Biometrics at the Frontiers : Assessing the Impact on Society*, Sevilla, January 2005, p. 15.

[476] DG JRC and IPTS, *o.c.*, p. 15.

[477] Compare, for example, with the legislation in Slovenia which regulates the use of biometrics but only in a general way.

[478] The European Parliament has also before already pleaded in its legislative resolution of 2 December 2004 on the proposed Regulation 2252/2004 for forbidding the creation of a central database of European Union passports and travel documents containing biometric and other data (see proposed Amendment 5). See European Parliament legislative resolution on the 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), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2004-0073+0+DOC+PDF+V0//EN Furthermore, the risks and fears for central databases and its misuse is also an important factor of (dis)trust of the citizens. See in that regard, Backhouse, J. and Halperin, R., D.4.12 'A qualitative comparative analysis of citizens' perception of eIDs and interoperability', Fidis, May 2009.

[479] In the light of new cryptographic measures for template protection, including a user specific secret as part of the verification method, this may need to be re-evaluated in specific cases of modern biometric systems. See also *below*.

[480] The risks of biometric central databases include use without knowledge of the data subject (e.g. for surveillance and tracing), function creep (including risk of use for identification purposes, for use of law enforcement, etc.), the use of the characteristics as unique identifier and identity theft.

especially the necessity in a democratic society, is often neglected and the application and the interpretation of these general principles is therefore difficult and uncertain.

Biometric technologies however are further developing and being implemented. At present, it is not possible to foresee all future technologies, and legislation shall take such future developments into account as well.[481] On the other hand, new technical developments may provide effective means to increase the protection of the privacy rights and interests of the data subjects upon the central storage of biometric data. Such developments include methodologies to store only 'biometric pseudonyms' in a central database, whereby one-way (irreversible) calculations are made from the biometric characteristic and additional information, such as a PIN code, user-id or other information.[482] In case of misuse or theft, the 'biometric pseudonym' can be revoked and re-issued.[483] Such new developments, however, are rather recent. Their effective use in the protection of the privacy rights of the data subjects is to be further demonstrated and proven.

➔ For the above mentioned reasons, and awaiting further technical developments for the effective protection of privacy and fundamental rights upon the central storage of biometric data, it is recommended to choose for a *general prohibition to set up central databases with biometric data*. Such prohibition would solve most substantial data protection issues and risks, such as the use of the data contrary to the finality and purpose principle (function creep) and use of the data as unique identifiers and also the privacy risks, such as the use for identification purposes without knowledge of the individual, the use for surveillance purposes and attack of the databases for purposes of identity theft. Without such clear legal provision, uncertainty remains and data controllers remain in principle free to set up central databases. In this case, such central databases will only be scrutinized in case of a complaint with the DAP or legal proceedings, or, in the best case, if the controller submits the database for a prior checking by the DPAs (on a voluntary basis, or, for example, in the case of France, mandatory). In all other cases (and countries), data may be further collected and centrally stored for all types of applications (e.g., in schools).

Only in limited situations, in conformity with the conditions of Directive 95/46/EC and justified on one of the *legislative grounds* set forth in Article 8 ECHR *after analysis of the necessity in a democratic society* and in application of the *proportionality* principle - to be explained and detailed during the legislative procedure in the specific law itself or at least in the preparatory works - *exceptions to this principle could be allowed by legislative measure* for specific types of applications. For some Type I government controlled applications, such exception to the general prohibition laid down by law may be possible by law if it is demonstrated in application of the proportionality principle that there is a pressing social need[484], the database is relevant and sufficient and there are no alternative means, and if the

[481] See, for example, the developments in face recognition techniques.
[482] See, in this regard, also the EU patent application 08169061.2 'Biometric Pseudonyms of a fixed-sized template' of the Berner Fachhochschule für Technik und Informatik HTI (pending).
[483] See also the TrUsted Revocable Biometric IdeNtitiEs project (TURBINE, EU project no. 216339 (2008-2011)) in which locally stored and revocable biometric pseudonyms for various identities are being researched and demonstrated.
[484] For some Type I government controlled applications, such 'pressing social need' to establish a central database could be the need to avoid double enrolment for social benefits or a need to combat fraud, if no alternative means are available and the establishment of the central database proves effective. Such pressing social needs will however in most cases not be present or only in very exception cases (where there is a 'higher

interference remains within proportions (because of applied security measures, restricted and divided data storage, full transparency to the data subjects, strict formulation of the purposes and limited access rights, etc.). Specific legislative provisions could determine additional conditions for such exceptions to the central storage and its use. Such conditions could include, as suggested by *Teletrust* in Germany, that *individuals keep control over the biometric data that are stored centrally*, e.g., by storing the encryption key(s) on the token which remains in the possession of the individual in order to avoid (i) use without the knowledge of the data subject and (ii) function creep. This proposed control, however, will not always be possible in practice.[485] In general, and only under particular conditions, a database could be proportional to the risks incurred by the data subjects, provided the other recommendations including such as relating to information, security and alternative means, are followed.

In other words, regulation or legislation should provide that the set up of a central biometric database[486] is the exception. Every such exception shall be duly motivated and subject to conditions in the legislation providing for such exception. This will in principle also result into a stricter interpretation of the conditions to be fulfilled.

➔ Alternatively, because of the generally admitted risk that biometric characteristics may reveal information relating to health or race, but also because of the special nature and unique characteristics of biometric data, it could also be recommended - and consistent with the existing data protection legislation - to, as a matter of general principle, to prohibit the processing of biometric data *tout court*. Such regulation would hence consist of a *general prohibition* to collect and process biometric characteristics of individuals. Such prohibition would be in line with other general prohibitions set out in the Directive 95/46/EC as a principle, such as the prohibition to collect and process other specified so-called sensitive data and data concerning health or sex life.[487]

*Exceptions* to the fore-mentioned suggested prohibition should only be acceptable under strictly defined conditions which are specific for biometric data processing[488] and if laid down in additional legislation. Such exceptions could include the (a) *local (secured) storage* of biometric data, (b) provided it is in the form of *templates* [489]of the biometric identifiers only,

---

need' than a need of the controller only) for Type II access control applications. Compare also with Court of Justice, Huber v. Germany, 16 December 2008, also discussed above, in which the necessity criterion as laid down in Article 7(e) of the Directive 95/46/EC was a main issue in relation with a central database with personal data of foreign nationals residing on the territory of a Member State (§§ 65-66).

[485] Compare with the central storage of biometric identifiers in Eurodac. The use of a token held by the data subjects may not be possible in practice.

[486] Distinctions may be made between central databases and local central databases. In case these local central databases could be linked or are accessible from a central point, they are equivalent to central databases.

[487] Compare with the definition of sensitive data in the Czech Republic general data protection legislation of 4 April 2000 as amended which explicitly includes biometric (and genetic) data in the definition of sensitive data (Article 4(b)). The data protection legislation of Czech Republic, however, submits the processing of sensitive data to one of the exceptions listed (such as consent, necessity to comply with a legal obligation, etc) without a general prohibition to process sensitive data (Article 9).

[488] These conditions should come in addition to the exceptions (e.g., consent, etc) which apply for the general prohibition to process sensitive data.

[489] The use of templates, however, does not exclude the storage of sensitive personal data (special categories of personal data) in every case.

(c) for specified purposes well defined and (d) after implementation of for biometrics specific *appropriate security measures*.[490] This would in fact mean that the proportionality check is moved from the administrative level to a discussion in parliament.[491]

Existing biometric applications could be granted a limited time period in order be become compliant.[492]

➔ If one of the two suggested general prohibitions, completed with in legislation well defined exceptions, would not be possible or agreeable, at least a *general prohibition* on the *collection and use* of biometric characteristics and/or technologies *without the knowledge* of the individual is recommended in order to avoid that biometric characteristics which leave traces are abused (e.g., use for identification, linking or surveillance, but also for abusing the sample). Such prohibition is needed to protect the fundamental rights and freedoms[493] and to increase public confidence. This prohibition should apply to the private and public sector data controllers, such as cities or communes, equally.[494]

➔ Legislation or regulation *shall also address the need for transparency in biometric systems.* This shall be done by imposing an information obligation upon data controllers which is more extensive than the general information obligation of Directive 95/46/EC and which is specific with regard to the functioning of biometric systems. Legislation could require the mentioning of the identification or verification functionality of the system and clarification as to whether or not the data are stored in a central database. Multi-layered information is an option and could provide the data subject with more insight into the functioning of the system.

➔ Regulation *shall also address the errors and technical failures* of biometric systems. These errors and failures, which are inherent to biometric recognition systems, will confront individuals with the limited functioning of the system. The technical aspects of the functioning of biometric systems have been described in detail in Fidis deliverable 3.10, revealing how the physical measurement step of biometric processing systems is *intrinsically error prone*. This includes several aspects. Fidis D.3.10 warned inter alia for biometric characteristics which are *not very distinctive* and for *oversimplified* systems which reduce

---

[490] For example, for Type I government controlled ID applications, an exception could be made for storage of biometric templates in an identity document held under the control of the individual (such as the epass) to authenticate the link between the document and the holder. For type II access control model applications, an exception could be made for storage of templates in an object where the biometric is held under the control of the individual (such as in an entrance token) for access control purposes only. For the type IV convenience model applications, the biometrics should be stored in an object privately owned and/or used by the individual for convenience purposes. For Type III public –private (mixed) application models, additional conditions may apply as the risk of re-use of the biometric data is in our opinion even higher.

[491] Even in case a parliamentary debate would be unsatisfactory, the regulation would remain subject to judiciary review, such as the review by the *Conseil d'Etat* in France, the State council (*Raad van State/Conseil d'Etat*) or the Constitutional Court (*Grondwettelijk Hof/Court Constitutionel)* in Belgium.

[492] Compare with various DPA decisions which impose that such similar requirements are implemented by processing submitted to them for checking or authorization.

[493] Compare with ECHR, *Peck v. U.K.*.

[494] Such prohibition would in our view also exclude the use of face recognition technology in relation with cameras already installed. A clear legislative provision in this matter however should regulate this issue.

biometric characteristics to a few components with poor separation capabilities. Other errors which need to be taken into account are those errors related to identification systems, because the reference templates overlap too much and the system becomes susceptible to impostor attacks.[495]

In addition to those system errors, system *failures* where the biometric system is unable to process the biometric data shall be taken into account. These failures include failures to enrol, failures to capture and failures to match. As known in general, all biometric systems include in addition false acceptances and false rejections to a certain degree, since the comparison is always calculated on probabilities. The rates for these false results will moreover depend on the threshold set by the operator or user and on the application of the system. These failures sometimes involve ethical questions in so far some groups, such as aged persons or disabled persons, are more affected than others.[496] Furthermore, biometric characteristics do not remain valid indefinitely, and if not renewed from time to time (e.g., voice, face, etc) will for that reason also provide false results. Finally, several biometric techniques are still subject to improvement. Various studies, such as the study of the *Bundeskriminalamt* in Germany of February 2007 for face recognition and the *Biometric Enrolment trial* of the UK Passport service of May 2005, have pointed to such unsatisfactory results.[497]

The legal framework shall hence *explicitly acknowledge* that biometric systems are never 100% certain and shall not disregard the errors and failures of biometric systems. Information about the error rates should be made available to the data subjects. In addition, the rights of the data subjects in case of failure shall be determined. Such rights could include (i) the right for *immediate second* review, at no cost and (ii) the right to use *an alternative system.*[498] Furthermore, the burden of proof should be on the data controller to prove that the data subject is not the person whose identity has been verified and not on the data subject who has to prove his or her identity through a (sometimes failing) biometric system.

This also touches the ethical and human dignity and equality aspects of biometric systems: if human beings are obliged or requested to submit themselves to a biometric system, such system shall not dominate, but shall be at the service of the human beings. A legal framework could take the errors and failures of biometric systems in various ways into account. One possibility is to regulate the technical requirements of systems to be used for specific

---

[495] E. Kindt and L. Müller (eds.), *o.c.*, p. 26.

[496] See e.g., the UK Passport Service, *Biometrics Enrolment Trial*, May 2005, 299 pages. Although the majority of the participants from the sample groups successfully enrolled on the three biometric identifiers which were tested (face, fingerprint and iris), success rates were lower for disabled participants (whereby the general enrolment success rates for for example iris was 90 %, but 61 % for disabled participants).

[497] See the project of the Bundeskriminalamt mentioned in footnote 66. The project which was set up in a real environment, more particular the train station of Mainz, showed that the environment such as darkness and fast movements have a large impact on face recognition and that (at a FAR of 0,1%) (only) about 60 % was recognized. Various factors, such as the progressive replacement of analog camera surveillance systems by digital systems, however, may promise better results. See also, e.g., the study of the UK Passport Service of May 2005 mentioned above, which pointed *inter alia* to the high verification failure rate that occurred with facial biometric verification, which was the least successful identification technology (p. 55). Fingerprint verification was successful in 81 % of the representative samples and 80 % among the disabled group.

[498] An obligation for the controller to address the failure of systems, for example for Type II access control models, is for example foreseen in the Unique Authorization N° 008 of the CNIL.

applications, for example by providing minimum requirements. Another possibility is to set up a certification scheme for specific biometric systems.[499]

➔ Regulation *shall also address the need for restricted access* to biometric data *to authorized users only,* including *audit possibility* of used access to the data, and other additional *security measures* as well.

➔ The need for identity management (IdM) in public and private applications will increase and IdM will become very important in a networked society. Securing the authentication with (revocable) biometrics could be a useful tool. Biometrics, however, only provides one part of the link of a person with (identifying) information about that person. Regulation should therefore pay specific attention to the requirements for enrolment and the harmonization of the sometimes called 'breeding documents' which have to be submitted to prove who a person is.

➔Various aspects of biometric verification are of a technical nature. In case of dispute, for example, in case of abuse, hacking, or identity theft, it would be advisable that courts have judges (and experts) who have obtained a certain specialization in this area in order to ensure qualitative judgments.

➔ Furthermore, the importance of a *public debate* on such a topic as the use of biometrics which affects all human beings, minors and elderly people, foreigners and nationals, fit or disabled, used before only for criminal investigations, and which generalized use includes considerable risks, cannot be underestimated. Such debate has not taken place at the time of the introduction of the epass for all EU country nationals. It has to a limited extent taken place in some countries, but remains overall very underdeveloped and is in particular countries even completely lacking. Such public debate should take place at least when biometric applications are introduced in Type I government controlled application and upon drafting legislation. The challenge for such public debate, however, is to represent the technical aspects in a simplified and objective way and to further first *inform* the public of all aspects of biometrics, including of the balance needed between security and privacy rights, before requesting opinions from data subjects on the use of biometrics.

➔ In addition, and in line with proposals in some countries and the discussions on a notification obligation for security breaches in the ePrivacy Directive, regulation should also provide for notification in case of *security breach concerning biometric data*, especially in case of central biometric databases. As suggested by DPAs, *civil and criminal liability* in case

[499] The use of certification labels is to some extent already practised in some countries, such as in Germany, for products in general and was also proposed for biometric applications in the Netherlands in the *At Face value report* of 1999.

of theft, misuse of biometric data and other security breaches concerning biometric data shall be provided for by appropriate legislation.[500]

The legal recommendations mentioned above may possibly *politically* - in times where security is a top priority of many governments - be difficult to defend. Appropriate measures however, should allow reconciling privacy with security. Increased security does not (always) has to be at the cost of privacy.

[500] See for example, also Switzerland, Privatim, *Guidelines for the data protection compliance review of biometric systems*, 2007, p. 14, reference available at http://www.privatim.ch/content/suche.php?zoom_query=biometrie

# 10 Selected Bibliography

**General**

*Legislation*

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23 November 1995

Council Decision of 8 June 2004 establishing the Visa Information System (VIS), 2004/512/EC, *O.J.* L 213, 15 June 2004

Council Regulation No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 385, 29 December 2004

Regulation (EC) N° 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), *O.J.*L 381, 28 December 2006

Regulation (EC) N° 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, *O.J.* L 218, 13 August 2008

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ* L 350, 30.12.2008

Regulation (EC) N°81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) N° 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Border Code, *O.J.* L 35, 4 February 2009

*Recent proposals*

Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, COM (2007) 619 final, 18 October 2007, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0619:FIN:EN:PDF

*Other legislative documents*

See European Parliament legislative resolution on the 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), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P6-TA-2004-0073+0+DOC+PDF+V0//EN

*Relevant case law*

Court of Justice, *Huber v. Germany*, 16 December 2008

ECHR, *Friedl v. Austria*, 31 January 1995

ECHR, *P.G. and J.H. v. U.K.*, no. 44787/98, 25 September 2001

ECHR, *Peck v. U.K.*, no. 44647/98, 28 January 2003

ECHR, *Perry v. United Kingdom*, no. 63737/00, 17 July 2003

ECHR, *Von Hannover v. Germany*, no. 59320/00, 24 June 2004

ECHR, *Sciacca v. Italy*, no. 50774/99, 11 January 2005

ECHR, *S. and Marper v. United Kingdom* [GC], no. 30562/04, 4 December 2008

*Opinions, Advice, Recommendations and Comments*

Article 29 Data Protection Working Party, *Working document on biometrics, WP 80*, 1 August 2003, 12 p.

Article 29 Data Protection Working Party, *Opinion N° 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)*, WP 96, 11 August 2004

Article 29 Data Protection Working Party, *Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas*, WP 110, 23 June 2005

Article 29 Data Protection Working Party, *Opinion 6/2005 on the Proposals for a Regulation of the European Parliament and of the Council (COM(2005) 236 final) and a Council Decision (COM(2005) 230 final) on the establishment, operation and use of the second generation Schengen information system (SIS II) and a Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)*, WP 116, 25 November 2005

Article 29 Data Protection Working Party, *Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities*

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 June 2007, 26 p.

EDPS, *Opinion on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and*

*investigation of terrorist offences and of other serious criminal offences, O.J.* C97, 25 April 2006

EDPS, *Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, O.J.* C 200, 6 August 2008

EDPS, *Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II)*

EDPS, *Comments on the Communication of the Commission on interoperability of European databases*, Brussels, 10 March 2006

EDPS, *EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step*

Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector

*Studies, projects, deliverables and articles*

Biometric Identification Technology Ethics project (BITE), an EU project N° SAS6-006093, www.biteproject.org.

Bundeskriminalamt, *Forschungsprojekt. Gesichtserkennung als Fahndungshilfsmittel Foto-Fahndung. Abschlussbericht*, Wiesbaden, February 2007

Commission de l'Ethique de la Science et de la Technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques*, Québec (Canada), 2005, 42 p.

Consultative Committee of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data [CETS No. 108] (T-PD), *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, Council of Europe, CM(2005)43, March 2005, available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)43&Language=lanEnglish&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=

DG JRC and IPTS, *Biometrics at the Frontiers : Assessing the Impact on Society*, Sevilla, January 2005, p. 15.

Gasson, M., Meints, M. *et al*., (eds.), *D.3.2. A study on PKI and biometrics*, FIDIS, July 2005,

Hornung, G. 'Biometric Passports and Identity Cards: Technical, Legal and Policy Issues', *European Public Law*, vol 11, issue 4, 2005

Kindt, E. and Müller, L. (eds.), *D.3.10. Biometrics in identity management*, FIDIS, December 2007, 130 p.

Kindt, E., 'Biometric applications and the data protection legislation', *Datenschutz und Datensicherheit* 2007, vol. 3, pp. 166 - 170.

Koops, B.-J. and Goodwin, M., *Strasbourg sets limits to DNA databases*, available at www.tilt.nl. (web commentary)

Meints, M. and Hansen, M. (eds.), *D.3.6. Study on ID Documents*, FIDIS, December 2006, 160 p.

UK Passport Service, *Biometrics Enrolment Trial*, May 2005, 299 p.

De Hert, P., Scheurs, W. and Brouwer, E., 'Machine-readable identity Documents with Biometric Data in the EU - part III - Overview of the Legal Framework', *Keesing Journal of Documents and Identity*, 2007, No. 22, pp. 23-26.

TrUsted Revocable Biometric IdeNtitiEs project (TURBINE) EU project no. 216339 (2008-2011), see www.turbine-project.eu

**Chapter 3 – Belgium**

Commission for the Protection of Privacy, *Opinion upon own initiative concerning the processing of biometric data in the framework of the authentication of persons*, Opinion N° 17/2008 of 9 April 2008, 22 p., available at www.privacycommission.be (in French or Dutch) ('CBPL Opinion on biometrics').

Kindt, E. and Dumortier, J. , 'Biometrie als Herkenning- of Identificatiemiddel', *Computerrecht* 2008, p. 132 *et seq*

Avoine, G. , Kalach K. & Quisquater, J-J., *Belgian Biometric Passport does not get a pass… Your personal data are in danger'*, available on http://www.dice.ucl.ac.be/crypto/passport/index.html ;

Kindt, E., 'Belgisch biometrisch paspoort onveilig', *Computerrecht* 2007, pp. 221 – 223.

**Chapter 4 – France**

CNIL and the University Panthéon-Assas-Paris II, *Information technology: slavery or liberty*, Conference held at the Senate, available at http://www.senat.fr/colloques/colloque_cnil_ senat/colloque_cnil_senat1.html

CNIL, *27e Rapport d'Activité 2006*

CNIL, *28e Rapport d'Activité 2007*

CNIL, *Délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques* available at http://www.cnil.fr/?id=2427

CNIL, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 28 December 2007, 12 p., available at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf

Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé, *Opinion N° 98. Biométrie, données identifiantes et droits de l'homme*, 31 May 2007.

National Consultative Ethics Committee for Health and Life Sciences, *Opinion N° 98. Biometrics, identifying data and human rights*, France, April 2007, 22 p.

Office for the Evaluation of the Scientific and Technological Choices, *Study about the scientific methods of identification of persons based on biometric data and the used technologies*, Assemblée National N° 938/Sénat, N° 355

**Chapter 5 – Germany**

Albrecht, A., Biometrische Verfahren im Spannungsfeld von Authentizitat im elektronische Rechtsverkehr und Personlichkeitsschutz, Nomos, Baden-Baden, 2003

Biermann, H., Bromba, M., Busch, C., Hornung, G. , Meints, M. and Quiring-Kock, G. (eds.) *White Paper zum Datenschutz in der Biometrie*, 2008, available at http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf.

Hornung, G., 'Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues', *European Public Law*, vol. 11, issue 4, 2005

Petermann, T., Scherz, S. and Sauter, A., 'Biometrie und Ausweisdokumente' [Biometrics and Identification Documents], *TAB Arbeitsbericht*, issue 93, 2003, p. 11.

Teletrust, *Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme* [Guideline for the employment of a biometric system], 21 September 2005, available at http://www.teletrust.org/uploads/media/ag6_ak-recht_orientg-betriebsvbg-biometrie_1.2.pdf

**Chapter 6 – The Netherlands**

CBP (before 'Registratiekamer'), *Biometrisch toegangscontrole systeem VIS 2000,* 19 March 2001 *('discopas opinion')*, available at www.cpbweb.nl (last accessed 28th March 2009).

CBP, *Wijziging Paspoortwet* z2001-1368 (invoering biometrie), 16 October 2001.

CBP, *Vragen over de inzet gezichtsherkenning* z2003-1529, 3 February 2004, available at www.cpbweb.nl

Artz, S. and van Blarkom, 'Beveiliging van persoonsgegevens: de WPB. Privacy en Biometrie: een technisch vraagstuk?', *Jaarboek Fraudebestrijding*, 2002.

De Hert, P. and Sprokkereef, A., *The Use of Privacy Enhancing Aspects of Biometrics: Biometrics as a PET (privacy enhancing technology) in the Dutch Private and Semi-public Domain*, 2009, University of Tilburg ('TILT'), 50 p.

Sprokkereef, A., 'Data Protection and the Use of Biometric Data in the EU', S. Fischer Huebner, P. Duquenoy, A. Zaccato, L. Martucci (eds.), *The Future of Identity in the Information Society,* IFIP (International Federation for Information Processing), 2008, Volume 262, Boston Springer, pp 277-284.

Van Kralingen, R., Prins, C. and Grijpink, J., *Het Lichaam als Sleutel. Juridische Beschouwingen over Biometrie* [The body as a key. Legal observations on biometrics], Samson, Alphen ad Rijn, 1997*;*

Prins, C., 'Making our Body Identify for Us: Legal Implications of Biometric Technologies', *Biometric Technology Law - Computer Law and Security Report* , 1998, Vol. 14. no. 3;

Grijpink, J., 'Biometrics and Privacy', *Computer Law and Security Report*, 2001, Vol. 17 no. 3, pp.154-160.

Hes, R., Hooghiemstra T. F. M. and Borking, J.J., *At Face Value. On Biometrical Identification and Privacy*, Registratiekamer, Achtergrond Studies en Verkenningen 15, September 1999, 70 p., available at http://www.cbpweb.nl/documenten/av_15_At_face_value.stm ('*At Face value report*') ;

Brussee, R., Heerink, Leenes, R., Nouwt, S. , Pekarek, M., Sprokkereef, A. and Teeuw, W. *Persoonsinformatie of Identiteit? Identiteitsvaststelling en Elektronische Dossiers in het Licht van Maatschappelijke en Technologische Ontwikkelingen*, 2008, Telematica Instituut, Report TI/RS/2008/034:1-98

Ministry of Home Affairs, *Privacy Enhancing Technologies. Witboek Voor Beslissers*, 2004, R. Koorn *et al.*, The Hague.

**Chapter 7 - Switzerland**

Privatim, *Guidelines for the data protection compliance review of biometric systems,* 2007, 15 p. reference available at *http://www.privatim.ch/content/suche.php?zoom_query=biometrie*

Federal Department Justice and Police (*Département Fédéral Justice et Police*), *Communiqué Passeport biométrique et liberté de voyager: votation populaire en mai prochain*, Bern, Switzerland, 29 October, 2008

Federal Data Protection and Information Commissioner (FDPIC) (*Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten* (EDÖB)/ *Préposé Féderal à la Protection des Données et à la transparence* (PFPDT)), *Guide relatif aux systèmes de reconnaissance biométriques*, November 2008

Federal Data Protection and Information Commissioner (FDPIC) (*Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten* (EDÖB)/ *Préposé Féderal à la Protection des Données et à la transparence* (PFPDT)), *Erhebung biometrischer Daten beim Erwerb einer Dauerkarte in den Sport- und Freizeitanlagen KSS Schaffhausen, Schlussberricht*, April 2006

Federal Data Protection and Information Commissioner (FDPIC) (*Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten* (EDÖB)/ *Préposé Féderal à la Protection des Données et à la transparence* (PFPDT)), *Einsatz von Biometrie beim Check-In und Boarding im Rahmen des Pilotprojektes "Secure Check" der Swissport International AG und Checkport Schweiz AG am Flughafen Zürich-Kloten*, June 2005

The Swiss Data Protection Authorities (*Die Schweizerischen Datenschutzbeauftragen/Les commissaires Suisses à la protection des données) Vernehmlassung. Einführung des biometrischen Passes: Vorentwurf zur Änderung des Gesetzes und der Verordnung über die Ausweise für Schweizer Staatsangehürige*, 26 September 2005, available at http://www.privatim.ch/content/pdf/050926.pdf

Party-independent committee against the Swiss biometric passport and identity card (*Überparteiliches Komitee gegen Biometrische Schweizer Pässe und Identitätskarten*), *FREIHEITSKAMPAGNE.CH*, available at http://www.freiheitskampagne.ch/,

Swiss Federal Court, 1B_71/2007, Probenahme und Erstellung eines DNA-Profils im Rahmen eines Strafverfahrens, 31 May 2007

Swiss Federal Court, 1C_41/2007 /fun, Probenahme und Erstellung eines DNA-Profils, 30 May 2007

Swiss Federal Court, 6S.454/2006 /rod, Refus du sursis à l'exécution de la peine et à l'expulsion (art. 41 CP), 28 December 2006

**Chapter 8 – The United Kingdom**

Anderson, R., Brown, I., Dowty, T., Inglesand, P., Heath, W. and Sasse, A., *Database State*, York, Rowntree Foundation, March 2009

Home Office, *National Identity Scheme Delivery Plan 2008*, available at < http://www.ips.gov.uk/passport/downloads/national-identity-scheme-delivery-2008.pdf>

Home Office, *National Identity Scheme Delivery Plan 2008: A Response To Consultation*, available at http://www.ips.gov.uk/identity/downloads/ConsultReportv2.pdf

House of Commons Home Affairs Committee, *A Surveillance Society? Information Commissioner's Response to the Committee's Fifth Report of Session 2007–08*, available at http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/1124/1124.pdf

House of Commons Justice Committee, *Justice – First Report*, available at < http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf

LSE, *The Identity Project: an assessment of the UK Identity Cards Bill and its implications*, June 2005, available at < http://is2.lse.ac.uk/idcard/identityreport.pdf>, last consulted 23 February 2009

Nuffield Council on Ethics, *The Forensic Use of Bioinformation: Ethical Issues*, September 2007, available at http://www.nuffieldbioethics.org/go/ourwork/bioinformationuse/ publication_441.html

Sullivan, C., 'The United Kingdom Identity Cards Act 2006- Civil or Criminal?', *International Journal of Law and Information Technology*, vol. 15, issue 3, pp 328-330.

# 11 Annex 1: Glossary

| | |
|---|---|
| **AFSJ** | Area of Freedom, Security and Justice |
| **BITKOM** | the German Association for Information Technology, Telecommunications and New Media |
| **CAO** | Collective labor agreement (Belgium) |
| **CBP** | Dutch Data Protection Authority (*College Bescherming Persoonsgegevens)* |
| **CBPL** | Belgian Data Protection Authority (*Commissie Bescherming Persoonlijke Levenssfeer)* |
| **CNIL** | French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés)* |
| **CoE** | Council of Europe |
| **DPA** | Data Protection Authority |
| **EAC** | Extended Access Control (in relation to epassports) |
| **Eurodac** | Central database for the comparison of fingerprints for the effective application of the Dublin Convention (EU) |
| **FDPL** | the Federal Data Protection Law (*Bundesdatenschutzgesetz (*Germany) |
| **FOI** | Freedom of Information Act (The United Kingdom) |
| **ICO** | The Information Commissioner (The United Kingdom) |
| **LSE** | The London School of Economics |
| **NIR** | National Identity Register (The United Kingdom) |
| **NIS** | National Identity Scheme (The United Kingdom) |
| **RFID** | Radio Frequency Identity |
| **SIS** | Schengen Information System |
| **SIS II** | Second generation Schengen Information System |
| **TBG** | Act against terrorism (*Terrorismusbekämpfungsgesetz)(*Germany) |
| **VIS** | Visa Information system |
| **WPPJ** | Working Party on Police and Justice |