EU Biometric Security Policies

Lesson from Number Plate Recognition

Matthias Pocs, LL.M.

Abstract

Biometric technology for crime prevention is emerging. It promises to track down potential terrorists and other dangerous persons but it also entails novel risks. Should the police be allowed to do use this technology in the future, the design of the biometric system is decisive for the protection of fundamental rights. Due to the automation of captures and content of reference databases, people that are somehow related to suspects but are not suspects themselves, may become a target for the police: witnesses, informants, contact persons, victims, etc. This paper assesses how the fundamental rights to privacy and data protection protect these persons and the biometric system needs to be designed in order to ensure this protection. This applies to the international plane as well as national legal orders, for which Germany will serve as an example.[1]

1 Introduction

Cameras are hanging at several places of the railway station and optically capturing faces of people passing them. A large number of persons pass these cameras. When someone is recognized as a wanted person the system notifies a "hit." The notification is created by automatically comparing facial data with the police watch lists. Such a technology has already been tested by the German Federal Criminal Office (*BKA*).[2] Biometric watch list technology promises to create an effective way of tracking down dangerous persons. However, until this technology becomes reality, the automated capture of biometric data needs to be improved.

Not only the test of the BKA shows the resoluteness of developing biometric technology for tracking down criminals. Police authorities already deployed other biometric systems in practice - face in Tampa[3] and iris in the UAE[4] - and respective research projects are funded - 3D facial recognition,[5] fingerprints from luggage,[6]

[1] Acknowledgement: The work in this paper has been funded in part by the German Federal Ministry of Education and Science (Bundesministerium für Bildung und Forschung, BMBF) through the Research Programmes under Contract No. 13N10820 – "Digitale Fingerspuren" (Digi-Dak), http://omen.cs.uni-magdeburg.de/digi-dak/, and Contract No. 13N10814 – "Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen (CamInSens)".

[2] Bundeskriminalamt, final report "Fotofahndung" (English), http://www.bka.de/kriminalwissenschaften/fotofahndung/pdf/fotofahndung_final_report.pdf

[3] Gates, Culture Unbound 2/2010, p. 67.

[4] Daugman/Malhas, International Airport Review 2/2004.

[5] Busch/Nouak, DuD 2008, 126.

and deviant behaviour from video surveillance[7] and the Internet.[8] At the same time, existing biometric databases that contain data about crime scene traces as well as fingerprints and photographs from criminal records, are interconnected - DNA and finger (AFIS[9]) in Prüm[10] - and extended - face and finger in SIS II,[11] finger in Eurodac[12] and VIS,[13] and others.[14]

Due to these developments, it is possible that in the future, laws will be enacted that for example, allow deploying biometric systems at international airports for finding potential terrorists. Such a precautionary data capture, that is, before a danger is caused or a crime is committed, poses new challenges to the law,[15] particularly because biometric characteristics are captured without the data subject having given cause for the capture and a large number of persons are subject to it.

This paper focuses on the future deployment of biometric systems and its impact for on the group of persons that are not only exposed to the automated capture of biometric characteristics but also the storage in reference databases (and thus, to “hits” and possible subsequent measures). In particular, these reference databases comprise European systems like Prüm and SIS II.[16] This paper assesses how the fundamental rights to privacy and data protection protect these persons and the biometric system needs to be designed in order to ensure this protection. These requirements apply to the international plane as well as national legal orders, for which Germany will serve as an example.

[6] Digi-Dak, see acknowledgements above; Hildebrandt et al., Proceedings of BioID 2011, LNCS Vol. 6583, Berlin 2011, p. 286.

[7] ADABTS, FP7 RCN: 91158; ADIS (BMBF (German Federal Ministry of Education and Science) FKZ: 13N10977-9); CamInSens, see acknowledgements above; SAMURAI, FP7 RCN: 89343; APFEL (BMBF 13N10795-801); SUBITO (FP7 RCN: 89391).

[8] Funded with 15m euros, INDECT, FP7 RCN: 89374, http://www.indect-project.eu/, D7.2: biometric data from video and audio; D4.3: combined with text from the Internet.

[9] In Germany administered by BKA, see http://www.bka.de/pressemitteilungen /hintergrund/hintergrund2.html

[10] Prüm Convention, EU Council Doc. 10900/05; EU Council Decisions 2008/615/JHA and 2008/616/JHA, OJ EU L 210, pp. 1 and 12; 2010/482/EU, OJ EU L 238, p. 1.

[11] SIS II EU Council Decision 2007/533/JHA, OJ EU L 205, p. 63; EC Regulation 1987/2006, OJ EU L 381, p. 4.

[12] Eurodac Commission Drafts, 9/2009 & 10/2010; EU Council Conclusions 11004/07, 12.6.2007; EC Regulation 2725/2000/EC, OJ EU 15.12.2000 L 316.

[13] VIS EC Regulation 767/2008, OJ EU 13.8.2008 L 218, 60; EU Council Decision 2008/633/JHA, OJ EU 13.8.2008 L 218 p. 129.

[14] Interpol DNA Gateway Charter, Lyon, using I-24/7; “Next Generation Identification” of FBI replacing IAFIS, see http://heise.de/-1214902.

[15] Pocs, DuD (Datenschutz und Datensicherheit) 2011, 163; Hildebrandt et al., see above; Hornung/Desoi/Pocs, in: Brömme/Busch, Proceedings BIOSIG 2010, Bonn 2010, p. 83; Art. 29 WP: The Future of Privacy (WP168), http://ec.europa.eu/justice_home/fsj/ privacy/docs/wpdocs/2009/wp168_en.pdf, para. 107; challenges with current systems, Heibey/Quiring-Kock, DuD 2010, 332 w. f. r.

[16] This paper is based on the publication Pocs, DuD 2011, 163. However, this pubilcation did not take into account the particular legal issues for the European systems.

2 Specific Technological Features and Risks

The non-suspicious persons that would be subject to the storage in reference databases as well as the automated capture of biometric characteristics would be exposed to specific risks.

2.1 Specific Technological Features

Biometric systems that will be deployed for tracking down criminals are different from other biometric systems for several reasons. First, biometric data captured at the airport or similar places (probes[17]) are compared with a centralized watch list or other reference database (one-to-many comparison) in which the biometric references are stored in a centralized way. Further, the system is used for open set identification, that is, in order to decide whether or not a person belongs to the wanted persons - "hit" or "no hit."

Moreover, it is to the detriment of the data subject if he is successfully identified. In addition, the capture of biometric data is automated. Due to the automation, it is possible to multiply the captures of biometric probes and comparisons with biometric references, in particular, if data are captured in uncontrolled environments in which data subjects do not have to cooperate. Besides, biometric identification systems are subject to a specific error rate.

Concerning the first feature, reference databases may stem from the country that deploys the biometric system or from another Member State, e.g. Prüm system, and the EU, e.g. SIS II. In relation to German police databases, it was observed that due to new police measures which do not require suspicion or a specific danger, the group of data subjects is extended.[18] This group comprises persons from the criminal area, the environment, the "scene" and the social background, beyond the group that is subject to data processing in conventional police work; that is, those who press charges, witnesses, informants, and persons that are in contact with suspicious persons or organisations, or where this is assumed.[19] This development may have taken place in other European countries, too.

The persons that are subject to reference databases may be categorized by occasion for and purpose of recording data about them. The terms for these occasions and purposes are technically implemented by means of key catalogs. In addition, the concepts and terms for occasions and purposes of a search are different from country to country. This difference is crucial if police databases of other Member States or the EU are being used.

Concerning the feature of automation of captures, new applications become feasible. Since the other processes of (biometric) reference database systems, particularly the comparison, is already automated (e.g., AFIS), it is due to the

[17] For terminology, ISO SC37 Harmonized Biometric Vocabulary (SD 2 V12) in SC37 WG 1.

[18] Petri in: Lisken/Denninger, Handbuch des Polizeirechts, 4. Aufl., H. 67 und 68.

[19] BVerfGE (collection of decisions of the German Federal Constitutional Court) 120, 378 (411).

automation of captures that reference databases may be used for precautionary data captures, for checking a large number of citizens.

The only known police measure for which data are collected by means of pattern recognition is car number plate recognition. Some legal implications of this technology application have been decided. For example, the German Federal Constitutional Court (*Bundesverfassungsgericht - BVerfG*) ruled that the wording of the legal basis did not specify the purpose of processing sufficiently precisely.[20] Accordingly, the legal basis allowed the comparison with such reference databases as mentioned above. In practice, captured data were only compared with the database "Object Search" and the national SIS database "NSIS Object Search" from "INPOL,"[21] the information system of the German polices.[22] Due to the missing purpose specification the Court annulled the legal basis.[23]

The question remains open whether or not the deployment of these more specific databases of INPOL is lawful in the case of number plate recognition. Applying this question to biometric systems, one has to establish in particular what persons may be subject to reference databases that are planned to be used for automated capture of biometric characteristics.

2.2 Risks

Should police in the future be allowed to capture biometric characteristics by automatic means, data subjects would be exposed to various risks. The multiplication of captures increases the risk of being exposed to "hits" and possible subsequent measures, disclosure of sensitive information,[24] connecting several databases creating a personality profile,[25] establishing one's whereabouts, time and direction, as well as unlawful access or function creep. The risks of unlawful access and function creep are increased if the captured data are compared in a centralized way. Due to the risk of function creep, data subjects may be exposed to hits and possible subsequent measures.

The risks of being exposed to "hits" and possible subsequent measures are increased if the reference database does not distinguish between nonsuspects and suspects or due to the specific error rate of biometric identification systems. Insufficient distinction between data subjects is particularly detrimental if the purpose of the system deployment is changed. For example, it turned out that in the case of number plate recognition, other objects were pursued afterwards (in Hesse, in 2007, 67 % of "hits" concerned car insurance) than those originally

[20] BVerfGE 120, 378.
[21] §§ 2 (3) and 11 (1) BKA Act.
[22] Government of Hesse, 23.10.2007, http://www. daten-speicherung.de/data/Hessen_ Antworten_2007-10-23.pdf, p. 10.
[23] BVerfGE 120, 378.
[24] Art. 29 WP: WP80, s. 3.7.
[25] Art. 29 WP: WP80, s. 3.2.

planned (the fight against cross-border crime, subsequent crimes like burglary, etc.).[26]

From the experience of number plate recognition, it is to be feared that reference databases are used without being able to limit “hits” and possible subsequent measures to the main target persons. Such technical inability would lead to “hits” and possible subsequent measures and thus be detrimental to persons

- that cannot be attributed a danger or crime,
- of which the suspicion has not sufficiently grown,
- that are not suspicious of a danger to or crime against high-ranking objects of legal protection, and
- that have committed a crime of little content of wrongdoing.

Since “hits” depend on the extent of the reference database, one has to assess what requirements concerning the design of reference databases and distinction between data subjects are set by the fundamental rights to privacy and data protection.

3 Legal Requirements

The deployment of the biometric system could interfere with fundamental rights of the data subjects; e.g., assumption of innocence (due to error rates), non-discrimination, free movement and freedom to travel (in case of tracking and stopping), property (in case of confiscation), right to judicial review (in non-transparent systems), as well as the prohibition of arbitration (in case of unspecified purpose of use). Human dignity may be concerned (if uniform personal identifiers are used to treat data subjects as mere “objects”).

In particular, such a law could interfere with the fundamental rights to privacy and data protection.[27] This requires the processing of personal data according to Art. 2 (a) with Rec. 26 Data Protection Directive 95/46/EC (DPD). The processed data are personal because biometric probes are attributed to biometric references that aim at finding persons.

The principles of the fundamental rights to privacy and data protection are harmonized within the EU. They comprise the principles of lawfulness, purpose specification, necessity and proportionality, data minimization, data accuracy, protection of sensitive data, transparency, access rights of data subjects, accountability, checking by data protection authorities, data security, and privacy

[26] Bodenbenner, NVwZ (Neue Zeitschrift für Verwaltungsrecht) 2010, 679.

[27] EC Directive 95/46/EC, CoE Convention ETS 108, Art. 8 ECHR and ECtHR case law, Art. 16 TFEU and Art. 6 EU Charter; 1980 OECD Privacy Guidelines, 1990 UN Guidelines; 2004 APEC Privacy Framework; in Germany, Art. 2 (1) with Art. 1 (1) German Basic Law and BVerfG case law, lately, BVerfG, 2 BvR 1372/07, para. 18, since BVerfGE 65, 1 (Census Decision).

by design.[28] While drafting law and designing technology, one has to take these principles into account.

Interference with fundamental rights may be justified by objects that promote public interest. Crime prevention and criminal prosecution are such objects of the public interest. According to the principle of necessity, the biometric system needs to be suitable and necessary for achieving the objects. This may be the case because the system deployment allows taking measures for crime prevention and criminal prosecution and the number of captures allows a novel reach of police observation.[29] However, there are even limits for necessary a deployment of a biometric system: On one hand, the legal basis needs to be worded in a way that it is foreseeable for what purposes the biometric system is to be deployed.[30] On the other, disproportionate interferences with fundamental rights need to be avoided.

3.1 Proportionality of "Hits"

In order to assess proportionality, one has to weigh up the gravity of the interference against the importance of the pursued objects. First, persons that have not given cause for the processing of biometric data are subject to the capture of biometric probes. Further, the secretive nature of the system deployment increases the gravity of the interference. Therefore, the data subjects may feel like being watched, because of which data subjects may not exercise his rights freely.[31] Moreover, sensitive data may be revealed. In addition, a large number of persons are subject to the data processing in order to find a criminal (the BVerfG calls this the scatter or "*Streubreite*" of data processing[32]).

These criteria for the gravity of the interference apply to the persons that are only subject to captures and use of biometric probes (in the database, there are no reference relating to them). The gravity of the interference may be reduced by means of legally and technically ensured data erasure. The interference for the persons that are also subject to the use of biometric references is even graver. First, they may be subject to hits and possible subsequent measures for which they have not given cause. Further, hit notification may be falsely attributed to them (data accuracy[33]).

3.2 Purpose Specification

The purpose specification needs to be particularly precise in order to avoid interference for the persons that may be subject to hits and possible subsequent measures. First, it is necessary to exclude hits about persons that cannot be

[28] See fn above.

[29] Accordingly in BVerfGE 120, 378 (428).

[30] E.g., BVerfGE 120, 378 (424).

[31] BVerfGE 120, 378 (402); BVerfG, 2 BvR 1345/03, para. 65; BVerfGE 115, 320 (342); 115, 166 (188); 113, 29 (46); 65, 1 (42).

[32] See e.g. BVerfGE 120, 378 (para. 78).

[33] Data Accuracy, Uptodateness, Completeness according to Art. 6 (d) DPD 95/46/EC and Art. 5 (d) DPC ETS no. 108; also Para. 8 OECD Guidelines 1980.

attributed a danger or crime (witnesses, contact persons, victims, etc.). Further, persons that cannot be attributed a danger or crime anymore, need to be spared; that is, if investigation against them was unsuccessful or residual suspicion does not exist after termination of criminal proceedings. Besides, only specific danger or suspicion may justify notification of a hit. Suspicion is only established if the facts are not irrelevant, exceed mere assumptions, and are based on criminalistic experience.[34]

In addition, the purpose must be specified by explicitly laying down what objects are to be protected by deploying the biometric system. To date, the priority of such objects of legal protection is qualified on the basis of the relevance[35] or particular gravity.[36] As regards their particular gravity, crimes need to be specified in relation to their range of penalties.[37] Concerning danger and crime prevention, the objects of legal protection are specific if the legal basis aims at preventing dangers to the existence or security of the nation or body, life or freedom of a person.[38] Apart from that, the deployment of the biometric system needs to be limited in a way that it depends on the content of wrongdoing in a particular case. Certainly, a high content of wrongdoing may be assumed for particular crimes.[39] However, in some cases even less grave crimes may justify system deployment.[40]

Should biometric systems for finding criminals be deployed in the future, it would be necessary to design the system in a way that allows distinction between the data subjects.[41] This is because interference with the fundamental rights to privacy and data protection caused by processing biometric probes and references as well as notifications of a hit would be particularly grave. For persons that cannot be suspected of crime, legal protection is offered by limiting the data processing to the possibility to attribute a danger or crime, sufficient factual bases, objects of high priority, and contents of wrongdoing. Such purpose specification can only be enforced if the reference database is designed in a way that during data comparison, one can distinguish between the data subjects.

4 Design of Reference Database

Purpose specification for protecting persons from notifications of hits would be ineffective if the biometric reference database would not be designed accordingly. Therefore, it could be necessary to introduce a legal basis that lays down

[34] See e.g. Meyer-Goßner, 50. Aufl., § 100a StPO, Rn. 9.

[35] E.g., BVerfGE 107, 299.

[36] E.g., BVerfGE 109, 279.

[37] BVerfGE 109, 279 (348f.).

[38] BVerfGE 115, 320 (365f.).

[39] BVerfGE 109, 279 (346ff.).

[40] BVerfGE 107, 299 (Abs. 81f.).

[41] This will possibly be provided for in the future data protection directive, COM(2010) 609 final, S. 2.3 para. 3.

safeguards for purpose specification by technology design in a qualified, clear and legally binding way.[42]

4.1 Legal Requirements on Technology Design

Such a requirement may follow from the principle of privacy by design. In accordance with privacy by design, the technology designer is to ensure compliance with data protection law by means of technology design.[43] The principle of privacy by design has already been specified in several instances.[44] The so-called "systemic data protection" is as comprehensive as the principle of privacy by design. In particular, systemic data protection provides that limitation of data access stored in jointly used databases is enforced by placing the database at the disposal of a trustworthy data controller and vesting accessing authorities with user rights.[45]

The principles of "data avoidance" and "data frugality" according to § 3a of the German Data Protection Act provides in particular that data processing systems be designed in a way that if possible (depending on the purpose and appropriateness) data are collected that do not relate to persons, their processing is little and their storage period is short.[46] Thus, the principle of data avoidance and data frugality combine the principles of minimality[47] and privacy by design. For example, this concept is important in order to avoid storage of data about persons that cannot be attributed a crime anymore.[48]

4.2 Distinction between Data Subjects

However, these specific concepts of privacy by design are not sufficient. They are only sufficient in applications for which the individual has given occasional cause. Then, the system may be designed in a way that their extent is reduced on the basis of this occasional cause. If data are captured as a precaution, for finding criminals, data subjects have not given cause for notifications of a hit. In order to be able to distinguish between suspects and other persons, the reference database needs to be designed in a way that allows distinguishing between the data subjects according to the specified purpose.

Notifications of a hit that are not compatible with the purposes result from a design of the reference databases that does not admit a sufficient amount of data in order to notify hits. Necessary data fields are missing. Hence, one is prevented

[42] Following BVerfG, 1 BvR 256/08, para. 225.
[43] Art. 29 WP: WP168, 1.12.2009, para. 46.
[44] Information and Privacy Commissioner of Ontario Canada: Privacy By Design - Take The Challenge 2009, http://www. privacybydesign.ca/content/uploads/2010/03/ PrivacybyDesignBook.pdf; Bygrave, Data Protection Law, The Hague 2002, fn 1234 w. f. r.
[45] Dix in: Roßnagel, Handbuch des Datenschutzrechts 2003; Steinmüller, Informationstechnologie und Gesellschaft 1993, p. 671; Podlech in: Brückner/Dalichau, Festgabe Grüner 1982, pp. 452ff.
[46] Roßnagel in: Eifert/Hoffmann-Riem, Innovationsrecht und Informations- und Kommunikationstechnologien (forthcoming).
[47] According to Art. 6 (c) and (e) DPD and Art. 5 (c) and (e) Convention 108.
[48] See 28th Report 2007 of LfD BW, S. 3, http://www.baden-wuerttemberg.daten schutz.de/lfd/tb/2007/tb-2.htm

from entering the categories of information that are necessary for complying with the specified purpose (e.g. being a suspect or contact person, facts establishing suspicion or mere assumptions). The information about data subjects is insufficient and notifications of a hit are false because according to the specified purpose, the person in question might not be subject to the hit. This violates the principle of data accuracy.

In contrast, one can avoid hits that are incompatible with the specified purpose, by designing the system in a way that it is possible to enter the categories of information that are necessary to distinguish between data subjects in accordance with the purpose. Such a distinction between data subjects would combine the principles of data accuracy and privacy by design.

In order to enter the information that is necessary for avoiding hits that are incompatible with the specified purpose, one has to define specific data fields for the records in the reference database. One could then provide within the system what values the fields have, in order to decide whether or not the particular record is to be used for the data comparison. By means of the data fields and system policy, it is possible to ensure to distinguish between data subjects according to the specified purpose.

It is uncertain whether or not the systems put in practice can fulfil the requirements of such a distinction between data subjects. Since number plate recognition is the first system deployment that is similar to deployment of biometric systems, the design of the reference databases that are actually used, the INPOL databases "Object Search" and "NSIS Object Search," is explored in the following.

The so-called field "N24" allows lay down the "occasional cause" of a search record.[49] The "occasional causes" are: Lost, Car Insurance, Official Cooperation, Other Danger Prevention, Usage, Police Observation, Other Occasional Cause, and "Endangerer." Data fields for further clues add to these "occasional causes." From this it follows that regularly, some of the occasions do not serve objects of particularly high priority. Other occasions are open for various occasions ("Other Danger Prevention"). In addition, the "purpose" of the search record, e.g., securing evidence, property, or cancellation of car registration, is laid down in field "N25."

The occasion "Police Observation" is further broken down into several "occasions:" on one hand, the open occasion "Other Danger Prevention," on the other, individual offences. However, this starting point does not limit police observation to suspects. As for example § 163e of the German Criminal Procedural Code (*StPO*) admits, contact persons may be subject to police observation, too. If instead of "Object Search," the database for persons "Wanted

[49] Government of Hesse, fn 15.

Persons" would be used, which could be the case for biometric systems, also witnesses could be subject in line with Art. 98 SIC[50] and in Germany, § 131a *StPO*.

In consequence, one may observe that the design of the reference databases that are deployed for number plate recognition may not be used in biometric systems. This design would not allow distinction between data subjects according to the specified purpose. Even the combination of the fields N24 and N25 may not limit hits to serious crimes or not further than properties such as "International Criminal" and "Criminal Association." Open occasions like "Other Danger Prevention" has nothing to say about the priority of the object of legal protection. Possibly, one may enter data into the fields for clues to specify the object and content of wrongdoing and whether or not the person is a suspect or a nonsuspect. However, it is doubtful whether or not such data fields may be suitable for deciding if the record in question is to be used for the biometric comparison. This is particularly because the fields are not always mandatory and their values are not standardized. Hence, it would be necessary for deployment of biometric systems to define fields by means of which one may determine the existence of a danger to or crime against particularly high-ranking objects, a crime causing an extremely large extent of damage, and the capacity as a suspect or nonsuspect.

5 Design of Data Exchange

The technical inability could not only follow from the fact that the national database cannot distinguish between the data subjects. It could also follow from data exchange with another Member State or the EU.

5.1 European Data Exchange

There are two models for the European exchange of biometric data that could be used to deploy systems for automated capture of biometric characteristics. On one hand, the EU deploys a watch list system, the SIS and its successors. On the other, DNA and fingerprint systems of several Member States are networked within the Prüm framework.

The European security policies relating to the Prüm framework and Schengen Information System II form part of the security strategy laid down in the Stockholm Programme.[51] Thereupon the Commission adopted the respective Action Plan.[52] SIS II is a successor of the Schengen Information System. In SIS, law enforcement authorities may enter data about persons observed, missed, wanted, etc. (data subjects) and objects according to Arts. 95ff. CIS.[53] For SIS II,

[50] Schengen Implementing Convention, fn 53 below.

[51] EU Council Doc. 17024/09, p. 35 and p. 55.

[52] COM(2010) 171 final, p. 30 and p. 47.

[53] Convention implementing the Schengen Agreement, OJ L 239, 22.09.2000, p. 19, BGBl. 1993 II S. 1010; EU Council reveals statistics about the actual numbers of data subjects and objects, EU Council: C.SIS at 01/01/2010, 6162/10 SIS-TECH 18 SIRIS 22 COMIX 103, 5.2.2010.

the categories of data (fingerprints and photographs) and data subjects are extended.[54] Further, the Prüm system is based on German initiative[55] and was transformed into EU law.[56] It enables law enforcement authorities to indirectly use DNA and fingerprint data held in national databases.

In relation to these policies, it is interesting to observe that the EU has not recognized the novel use of SIS by means of number plate recognition which was already put into practice. In addition to this practice, biometric systems had already been tested in the field. No consideration can be found in policies and legislation for the next generation of information systems. In other words, the EU has not learned its lesson from ANPR. This may result from a view that fails to recognize the interdependence of automated data capture and recording of reference data or expects national and regional legislators to take the initiative.

5.2 Tables of Equivalence

During data exchange, the other State's or EU's database may not sufficiently distinguish between data subjects or the foreign terms for occasions and purposes used in police work may not be accurately linked with the equivalent terms of the own Member State's database. Whereas the first alternative was discussed above, the second one is specific to data exchange with other Member States or the EU. In relation to data exchange, the risk of "hits" and possible subsequent measures can only be reduced by means of distinction between data subjects that is enforced by linking the equivalent terms of two database systems to another.

For example, the integration of the reference database "NSIS Object Search" illustrates this for number plate recognition. This database forms part of SIS. For a long time, SIS was only used for manual ID checks. The novel use of SIS is the deployment of number plate recognition systems that check citizens by automatic means to decide whether or not they are suspicious. Such systems are deployed in the UK, France and Germany.

Although the data are recorded in a central database system, the database "NSIS Object Search" is a copy that is integrated into the national reference database system. In the case of Germany, this is the abovementioned "INPOL." In relation to "NSIS Object Search," the data field "N24" for occasions includes four keys: Covert Car Registration, Targeted Car Check, Lost Car, and Cars Wanted for Criminal Proceedings.[57] Additional information is added in the field "N25" (purposes) in relation to the first two keys. This information is for the police officer in the field. Hence, this field is not used for automated filtering of hits. The fields specify that both keys are equivalent to the key "Police Observation." This

[54] Regulation (EC) 1987/2006, OJ L 381, 28.12.2006, p. 4; EU Council Decision 2007/533/JHA, OJ L 205, 7.8.2007, p. 63.

[55] EU Council Doc. 10900/05 (Prüm Treaty).

[56] EU Council Decisions 2008/615/JHA and 2008/616/JHA, OJ L 210, 6.8.2008, p. 1 and p. 12.

[57] Goverment of Hesse, 1.6.2007, p. 7.

shows where the SIS database distinguishes between data subjects to a larger extent or using different concepts than the German equivalent.

In general, such a table of equivalence is useful for determining whether or not the foreign database system sufficiently distinguishes between data subjects. The table of equivalence shows this if the term or key of the foreign database is linked to several keys of the national database. Using such databases would be unlawful because hits could be notified in breach of the specified purpose whereby subsequent measures could be taken.

The other Member State or the EU should be consulted in order to establish equivalence of terms. Terms are only equivalent if the concepts behind them are the same. The concepts of suspicion, causation of a danger or crime, a sufficient factual basis, high priority of an object of legal protection, and content of wrongdoing may differ from country to country. Consultation about these concepts could be based on legal definitions such as the European Arrest Warrant.

If in the future the police would be allowed to deploy biometric systems for finding criminals, in addition to the distinction between data subjects, the database systems should adapt their design specifically to the data exchange with other Member States or the EU. The system should be designed in a way that links the terms of the other Member State or the EU to the equivalent terms of the own national database. This object could be pursued by drawing up a table of equivalence.

6 Design of the Law

In the EU as well as in Germany, designing the law would be challenging because the legislators for the capture of biometric probes and recording of biometric references would not be the same. In Germany, the reference database system INPOL is administered by the *BKA*; the capturing of car number plates is carried out by the police authorities of the *Länder*. Hence, the legislator of a *Land* which is introducing number plate recognition is not authorized to lay down conditions for recording reference data that are in line with the design that sufficiently distinguishes between the data subjects.

This decentralized state organization may not apply to other Member States. However in the EU, for reference databases of the EU such as SIS II or other Member States within the Prüm framework, the legislators for the biometric capture system and biometric reference database system would never be the same. This shortcoming can only be remedied joint efforts of legislators. Such joint efforts are indispensable if systems for automated capture of biometric characteristics are to be introduced because as shown above, the use of reference databases as currently designed would be unlawful.

From the point of view of the legislator that plans to introduce a biometric system, the law-making process of the respective other legislator needs to be studied. In this case, the EU's law-making processes will be assessed because the

EU regulates the data exchange with the EU, in the Schengen system, and other Member States, in the Prüm framework. Both systems were based on international treaties first and integrated in the EU legal framework afterwards.

6.1 Schengen System

The international treaty concerning SIS is the Schengen Implementing Convention.[58] The SIC is based on the Schengen Convention[59] which provides for certain cross-border policies, for example, abolition of internal borders. These and other legal instruments, the Schengen acquis, were integrated into EC and EU law; this follows from Art. 2 Schengen Protocol.[60]

Therefore, the provisions about the Schengen acquis had to be attributed a legal basis. To this end, the EU Council adopted two decisions on the basis of Art. 2 Schengen Protocol. Whereas the first decision[61] defined the Schengen acquis, the second decision[62] actually attributed legal bases to the Schengen provisions. Only the provisions dealing with SIS (Art. 92 to 119 SIC) were not attributed a legal basis. Certainly, the attribution was debated because in SIS, immigrants (first pillar), on the one hand, and criminals (third pillar) were searched, on the other. However, this double function was no reason for the EU Council to stay inactive.[63] The EU Council stayed inactive because thereby the basic rule of Art. 2 (1) Schengen Protocol applied. Accordingly, the Schengen provisions that are not explicitly attributed a legal basis, fall within the third pillar of EU law. Had the EU Council decided this, the decision could be contested before the ECJ.

6.2 Prüm Framework

Initially, the Prüm framework was introduced outside the EU legal framework. This may result from the fact that its introduction would have not been feasible if all Member States would have participated. However, in contrast to SIS, at the time of introduction of the Prüm framework the participation of all Member States was not necessary. The framework could have been created within the EU legal framework while preserving principles of the rule of law.

As an innovation compared to the Treaty of Maastricht[64] and Rome,[65] the Amsterdam Treaty[66] introduced the legal instrument of the Enhanced Cooperation. Enhanced Cooperation is currently provided for in Arts. 20ff. TEU and Arts. 326ff. TFEU. This instrument refers to agreements that are initiated by Member States. Accordingly, it is left to the Member States to take measures as

[58] Schengen Implementing Convention, see fn 53.

[59] Schengen Agreement OJ EU 2000 L 239, p. 13.

[60] Art. 4 Schengen Protocol, OJ EU 10.11.1997 C 340.

[61] Decision 1999/435/EC, OJ 1999 L 176 p. 1.

[62] Decision 1999/436/EC, OJ 1999 L 176 p. 17.

[63] E.g., Customs Information System, OJ 1995 C 316 p. 33 and OJ 1997 L 82 p. 1; or several SIC provisions like Arts. 76, 126 (3), 128 (2), and 127.

[64] Treaty on European Union, OJ EU 29.7.1992 C 191.

[65] Treaty establishing the European Economic Community, 25.3.1957.

[66] Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and related acts, OJ EU 10.11.1997 C 340.

long as the area in question is not within the exclusive competence of the EU according to Art. 329 (1) TFEU.

In order to establish Enhanced Cooperation, there is a minimum number of Member States that need to participate. The Amsterdam Treaty required a majority of Member States. In 2003, this threshold was lowered to eight Member States by the Nice Treaty,[67] and in 2009, increased to nine Member States by the Lisbon Treaty. At the time when the Prüm Convention was signed, in 2005, the threshold of eight Member States applied. However, the Convention was concluded between seven Member States.

The integration of the Prüm Convention in the EU legal framework is debated. The Convention was concluded outside the EU legal framework. Therefore, there were not the control mechanisms that are necessary for protecting fundamental rights. On one hand, the EU Parliament did not have to be heard. On the other, one could not appeal to the ECJ for judicial review of the Convention. For these reasons, the opinions of the EU Parliament and the European Data Protection Supervisor[68] could not have the full effect.

In conclusion, SIS as well as the Prüm framework is based on the third pillar of EU law. The Lisbon Treaty abolished the pillar structure. However, the existing legal instruments continue to apply. They will be replaced by legal instruments that take into account the current EU primary law. This moment should be seen as an opportunity to lay down appropriate legal safeguards for the fundamental rights to privacy and data protection. Further, it is an opportunity to take into account the novel use of reference databases for automated capture of personal data such as biometric characteristics, so that such use would be lawful.

7 Conclusion

If in the future the police would be allowed to deploy systems that capture biometric characteristics by automatic means, the reference databases would be used intensely. This would lead to a novel risk of "hits" and possible subsequent measures. Hits about persons such as witnesses, contact persons, etc. can only be excluded by technology design. Using the reference databases in their current form would be unlawful. If crime prevention and criminal prosecution are to be rendered more effective, one must also render effective the protection of the fundamental rights of persons that are exposed to hits and possible subsequent measures in breach of the purpose specified by the law.

Rendering legal protection effective is possible. Checking a technology from a data protection point of view strengthens the argument for the deployment of

[67] Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ EU 10.3.2001 C 80.

[68] EDSB, OJ 2007 C 169/02, para. 70; EU Parliament, Legislative Resolution, 7.6.2007, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0228+0+DOC+XML+V0//DE&language=DE

biometric systems. This is because reasonable citizens are interested in both: protection from dangers and crimes as well as protection from consequences of abuse of informational power. If one makes use of the design options, one may lay the foundation for a future that society desires.