Biometric systems in future preventive Scenarios – Legal Issues and Challenges

Dr. Gerrit Hornung, LL.M., Monika Desoi, Matthias Pocs, LL.M.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel
Wilhelmshöher Allee 64-66
34109 Kassel
gerrit.hornung@uni-kassel.de
m.desoi@uni-kassel.de
matthias.pocs@uni-kassel.de

Abstract: The privacy and data protection challenges posed by biometric systems have been discussed in detail in the last years. Both security opportunities and privacy risks however may develop and change with the technical enhancement of the respective systems, which also induces the emergence of new application scenarios. One group of such new scenarios appears to be the prevention of criminal or in other ways dangerous behaviour. From a legal point of view, this brings about new challenges which go well beyond the problems of authentication as such. While some of the features of the scenarios discussed below may not be feasible in the short term, it is apparent that the associated fundamental rights and data protection law problems will have to be addressed in the future. This applies to the international plane as well as to national legal orders, for which Germany will serve as an example in the following.[1]

1 Biometrics, behavioural Pattern Analysis and the Law

From the very beginning of the technical development of biometric systems, this technology has been put into question from the privacy and data protection[2] point of view. This is however in no way a sole characteristic. Rather, it appears that virtually

[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), and Contract No. 13N10814 – "Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen (CamInSens)".

[2] For the purpose of this article, it is not necessary to discuss the different notions of these terms. It has been argued that the two concepts differ to a considerable extend. According to [HeGu06] [GuHe08], privacy should be understood as an opacity tool, guaranteeing non-interference in individual matters by the state and private actors. On the contrary, data protection is construed as an transparency tool, meant to compel government and private actors to "good practices" by focusing on the transparency and accountability of governmental or private decision-making and action. However, this useful distinction may be misleading as regards specific legal provisions, which may serve both or other purposes. In addition, "privacy" may have considerable different meanings in different legal orders, and there are further conceptions such as the German right to informational self-determination ([HoSc09]), which may not fall in just one of the two categories.

every new technology which processes personal data brings about issues of personal privacy and governmental control, of autonomous decision-making and heteronomy of the individual, of societal transparency and clandestine collection of information.

Given this fact however, there are some privacy and data protection risks particularly associated with biometric data, which are due to their inherent characteristics. In short, the most relevant of these risks appear to be the following [Al03, 152 ff.] [Ho04] [Ho05, 85 ff., 179 ff.] [Me07, 1089 ff.]:

- "Identity Theft", i.e. the unlawful capture of biometric characteristics in public or from a database, followed by the use of other persons than the data subject,
- The processing of "additional information" (e.g. on illnesses or likeliness for developing an illness, personal origins and current psycho-social constitution) which may be included particularly in biometric samples (raw data),
- The tracking and continuous surveillance of people's behaviour through frequent biometric identification,
- The collection of biometric data and surveillance without notice of the data subject,
- The linking of several databases using biometric data as a common single identifier, and
- Decision errors (false acceptance and false rejections) which lead to subsequent measures or expectations addressing the "wrong" person.

2 New technological Developments

Biometric systems are subject to permanent development. Biometric systems get better as such (i.e. better failure rates), new biometric characteristics may be included, new application scenarios may become feasible or existing scenarios may shift from the authentication of single data subjects to the authentication of larger social groups. Not all of these developments pose new legal questions. However, even the plain enhancement of the comparison algorithm of a given system or the improvement of its spoof prevention mechanisms may require a new legal assessment, because this leads to an ever stronger link between the data subject and the respective biometric samples. Interestingly, while this significantly reduces some of the aforementioned privacy and data protection risks, other risks may increase at the same time. A strong link may most notably lower the risk of identity theft, but add to the possibilities of tracking and surveillance.

In the future, these new technological developments could enable police authorities to introduce biometric systems for the prevention of crime. Subsequently, two examples of possible scenarios will be given. Some of the features of these scenarios may not be

feasible for the short term, but it is apparent that the associated fundamental rights and data protection law problems will have to be addressed in the future.

2.1 Recognition of Fingerprints on Baggage and Freight

To date, fingerprint recognition appears to take place in two scenarios. On the one hand, there is the "old-fashioned", forensic way of manually collecting fingerprints at crime scenes in order to compare the captured data with existing databases such as the AFIS or with the fingerprints of a known suspect. On the other hand, there are digital biometric authentication systems, where the biometric data of a present person is collected and compared with the reference data on a one-to-one or one-to-many basis.

Technological development appears to allow for a combination of the two in order to digitally collect fingerprint data at everyday objects, i.e. without knowing where exactly the fingerprints are or even whether there are any fingerprints at all.[3] This could significantly enhance police work at crime scenes. At the same time, biometric fingerprint systems may even play a role in new preventive scenarios. The systems could, among other things, even be able to find and scan fingerprints on baggage and freight in the airport in order to singling out dangerous materials in the baggage and freight. To this end, it could automatically detect and collect fingerprints and even further proceed by comparing them with a list of dangerous persons. This procedure is only viable because in respect of fingerprints, one could make use of the already existing automation of fingerprint comparison conducted by national police offices such as the German Federal Criminal Police Office (*Bundeskriminalamt*).

2.2 CCTV, behavioural Pattern Analysis, and Identification

Quite similarly, it appears to be an "old-fashioned", first generation of CCTV systems whereby one or several cameras observe a public space and transmit the data to a control room. Clearly, these systems have ever improved, allowing for higher image quality and the analogous or now digital storage of the data for later analysis.

The next technological step however could bring about major changes as regards both the security opportunities and the privacy risks of CCTV. "Smart" cameras, based on video content analysis may use methods of behavioural pattern recognition to monitor large public areas, e.g. airports, football stadiums and railway stations, and to automatically identify acute threat situations at the moment of their development.[4]

Smart cameras combine image sensors and microcomputers to analyse video content in a single device, so that they are the basis of new video systems. Smart cameras renounce image transmission in favour of essential abstracted environmental information.

[3] The technical and legal issues of such systems are currently being scrutinised within the project "Digitale Fingerspuren (Digi-Dak)" (see above n. 1), http://omen.cs.uni-magdeburg.de/digi-dak/.
[4] The technical and legal issues of such systems are currently being scrutinised within the project "Verteilte vernetzte Kamerasysteme zur in situ-Erkennung Personen-induzierter Gefahrensituationen in öffentlichen Räumen (CamInSens)", (see above n. 1), http://www.caminsens.org/.

Therefore disadvantages of central video system architectures (disaster tolerance, scalability) can be overcome. These smart cameras shall be able to identify moving objects, track them and simultaneously compare their motion to common patterns. If it differs from these common patterns and is subsequently identified as a security threat, private or state security services could be alarmed automatically.

Likewise, smart cameras can be interconnected. Long track logs can be created by linking shorter track logs of several camera places. These long tracks can be interpreted to detect conspicuous movement patterns.

In future, smart camera surveillance systems could easily be combined with biometric techniques of facial recognition or other biometric or non-biometric means of personal identification. There are large numbers of possible applications such as the automatic comparison with watch lists of people under restraining orders or missing person´s reports. Meanwhile technical problems have to be solved. Recognition and tracing of temporary or partly hidden persons and high dynamic scenarios (such as different perspectives and lightings) are issues that must be resolved.

3. New and enhanced Privacy and Data Protection Risks

Both scenarios show that biometric authentication may well go beyond specified situations in which the individual is able to control or at least become aware of the use of his/her biometric data. This brings about problems with the data protection principle of transparency. In particular, this principle protects the individual by requiring the controller to inform the data subject about the collection of personal data. This requirement is enshrined in Articles 10 and 11 of the European Data Protection Directive 95/46/EC (DPD) and the respective national data protection acts. For Germany in particular, police legislation of the German *Länder* likewise provides for a precedence of direct over indirect collection of personal data [Pi07, 226 f.]. As regards biometric systems, this precedence is particularly important since data subjects unintentionally leave their fingerprints on objects and facial data may be captured by cameras in the public domain. Further, indirect and covert collection of biometric data also disables the individual to seek legal remedy against unjustified processing of personal data.

Additionally, large-scale applications may significantly influence the legal assessment as regards the principle of proportionality. While this is already a problem in 1:1 verification scenarios ([WP03, 6 ff.]), it becomes critical in preventive scenarios. By way of example, the German Constitutional Court (*Bundesverfassungsgericht*) has frequently ruled that the question of how many citizens are subject to a technical surveillance measure is of utmost importance for the assessment of its constitutionality (scatter or "*Streubreite*", see e.g. [BV08, para. 78]). In respect of prevention, police authorities may exploit their investigative powers in dangerous and endangered places [Pi07, 244 ff.] and automatically collect data related to numerous persons. In relation to fingerprints, national AFIS throughout the world allow for automated recognition of fingerprints of criminals and immigrants. As to both fingerprints and the human face, most states built up databases for passport and ID card registers, or plan to do so in the future. Germany

appears to be a special case, as fingerprint data has to be deleted after the issuance of the documents, and databases with biometric facial data are being built not centrally, but only at local passport and ID card registers. For the time being, the automatic transfer of this data to German police authorities is restricted to single cases of urgency in which the passport or ID card authorities are not reachable [Ho07, 185]. This follows from both Section 22a of the German Passport Act (*Passgesetz* [PG09]) and Section 25 of the German ID Card Act (*Personalausweisgesetz* [PA10] entering into force in November 2010). It remains to be seen whether this will change in the future.

Associated with the new type of preventive large-scale applications, there may also be a tendency towards 1:N identification. Biometric systems for preventive law enforcement necessitate this identification functionality in order to determine the suspect, that is, they need to include a significant group of the population in order to have successful searches. In general however, identification leads to greater privacy problems than 1:1 verification, because it could allow for the non-transparent surveillance of a large group of people ([Al03, 162 ff.] [Bi02, 44] [WP03, 6 f.] [GoPr03, 69 f., 72] [WHO03, 40] [Ho05, 191 ff.]). Biometric encryption, a means of biometric template protection, is suitable to reduce privacy threats. This approach avoids the storage of biometric data and template data by encrypting a random number on the basis of the collected biometric data (since [TSS96]; lately [Br09]). It is however crucial that the random numbers are not stored in the same database, in order to avoid 1:N identification. Otherwise any biometric characteristic could be combined with every random number and the result of that combination could be compared with reference data. This comparison establishes the association of a biometric characteristic with a data set which may identify a person.

Further, the principle of purpose specification is at stake. Biometric data do not as such tie the processing to a certain purpose. For instance, ID card registries process facial data for the purpose of issuing ID cards and certain CCTV surveillance cameras process data for crime prevention purposes. If biometric data can be extrapolated from the video images, ID card images could be used to identify persons located by means of the camera system. If a fingerprint scanning system would be introduced in airports, the data contained in the national AFIS for the purpose of preventing crimes and illegal claims of asylum and residence could be utilised to identify persons of this group that are located by the fingerprint scanner. In both cases, interoperability appears to lead to additional privacy and data protection concerns.

Data subjects may also become subject to further security measures. As regards the identification after an incident, the severity of this risk depends on the reliability of the biometric system. In prevention scenarios which are based on behavioural analysis however, the decision on further security measures may be influenced or even decided by the technical analysis of people's individual behaviour and the comparison with generalised, "dangerous" types of behaviour. Smart cameras may be able to observe people and their motion and to compare this motion to common patterns in order to alarm private or state security services in the event that the motion differs and is identified as a security threat. In result, concrete measures against persons may take place just because of an automatic process.

The pressure of permanent identification and behavioural analytics by smart cameras may lead to a risk of incursions into the freedom of action and the freedom of decision. The reason is that data subjects who feel like being watched, may abstain from deviant behaviour patterns and accommodate themselves to behavioural adaptations. The new intelligent and self-organising smart cameras could become able to track human routes, so that complete targeted monitoring and tracing in public places becomes feasible.

Clearly, this brings about major legal and ethical problems regarding the general possibilities to describe deviant behaviour, the reliability of the system, its decision structure, and the possibilities of ultimate human decision-making. Therefore, among others, the data protection authorities of the Member States recognise that "the challenges for data protection are immense [and a] future legal framework should in any event address [the tendency] towards a more or less permanent surveillance of all citizens [for example] the combined use of intelligent CCTV-cameras and other tools" [WP09, para. 107].

4. Legal Requirements and Challenges

The risks of the use of biometric systems in future preventive scenarios may lead to violations of several human rights protected by the EU Charter of Fundamental Rights, the European Convention of Human Rights and national constitutions such as the German *Grundgesetz*. These laws do not only include the rights to privacy and data protection, as well as national particularities such as the German right to informational self-determination. Additionally, human dignity may be concerned if biometric characteristics are used as single identifiers by state authorities for treatment of data subjects as mere "objects." Moreover, the special protection of sensitive data (Article 8 DPD) such as health and ethnic information may be applicable at least to some forms of biometric data. Finally, the right to travel and the freedom of movement could be at risk in case that data subjects are tracked and continuously monitored in different places. In addition, property as a fundamental right (in case of confiscation), the right to innocence until proven guilty (if the system or its design suffer from errors), the right to judicial review (in non-transparent systems), and the prohibition of arbitration (in case of unspecified purpose of use) may be violated.

This plurality of possible infringements on basic rights causes difficulties to discuss the use in conformity with privacy and data protection requirements. On the other hand, the general legal data protection requirements have been well discussed and may be applied to new biometric systems as well. As those systems in principle process personal data within the meaning of Article 2 (a) DPD, they are subject to the respective national Data Protection Acts which implement this Directive. Albeit differing in detail, the national acts follow common principles due to the harmonising effects of the European legislation. These principles are frequently (but not in all countries) fostered by fundamental rights of national constitutions such as the German right to informational self-determination, recognised by the *Bundesverfassungsgericht* since [BV83] (on the concept see e.g. [HoSc09]). Thus the following principles are in general also vested with the power of constitutional rights in Germany and other national legal orders.

Accordingly, each citizen has the right to, in principle, decide for him/herself which personal information is to be disclosed in his/her social environment. In short, the processing needs to be based on legislation or effective consent by the data subject, personal data may only be collected and used for specified purposes, the data must be anonymised or deleted once this purpose is accomplished, data must not be processed beyond the absolute minimum required (data minimisation), the interference with personal privacy must be proportional to the purpose, the data processing must be transparent for the data subject, proper organisational and technical security measures must be in place to protect the data, and the data subject enjoys certain rights, e.g. to get their data rectified, locked or erased under certain circumstances. Additionally, there are significant restrictions for the use of "sensitive" data. According to Article 8 DPD, this includes "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".

As regards the new scenarios above, there are some common legal challenges which apply to all EU Member States. First of all, these security applications cannot be based on the consent of the data subjects because they are used to take preventive police measures against the will, and possibly even without notice, of the data subject. Thus there is the need of legislation specifying in detail the circumstances and requirements of the processing of biometric data. In Germany in particular, it is in both cases very doubtful whether the existing police and data protection laws allow for the use of biometrics in the described manner. In contrast, this may be possible in the case of criminal investigation using digital capturing of fingerprints, as this appears to merely replace the analogue measures used hitherto.

In preventive scenarios such as the (even routinely) scanning of baggage and freight in airports and the behavioural analysis and personal tracking of visitors through the use of "intelligent" CCTV systems however, no concrete suspicion of a crime can be established before processing personal data related to a myriad of persons. Police intervention in endangered places requires the establishment of such a suspicion beforehand [Pi07, 244.]. However, since it cannot automatically be determined whether or not a person is dangerous without collecting personal data, a decision of the *Bundesverfassungsgericht* could solve this conflict. In the case of number plate recognition [BV08], the Court ruled that collecting data from car number plates does not interfere with the right to informational self-determination if the data stay anonymous and are instantly and untraceably deleted in case that the comparison with the police search database is negative [BV08, para. 68]. For fingerprint recognition, this could mean that the German legislator is allowed to provide for the scanning of baggage and freight in airports for preventive purposes. It remains to be seen whether other national courts and data protection authorities of other countries will take up this approach.

There has so far been no occasion for the *Bundesverfassungsgericht* to deliberate on the preventive use of a biometric system, and the same appears for other national constitutional courts. Nonetheless, existing data protection legislation might be applicable to preventive biometric scenarios. While the DPD does not include provisions on biometrics or CCTV, some national data protection acts do. By way of example,

following Section 6b of the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) the monitoring of publicly accessible areas using optoelectronic devices under statutory requirement is allowed.[5] Monitoring publicly accessible areas using optoelectronic devices shall be lawful only as far as necessary (1) for public bodies to perform their duties, or (2) to exercise the right to determine who shall be allowed or denied access, or (3) to pursue legitimate interests for specifically defined purposes. Additionally, there must be no indications of overriding legitimate interests of the data subject. Furthermore, suitable measures shall be taken to indicate that the area is being monitored and to identify the data controller.

Section 6b (3) BDSG governs the processing and use of the collected data. Whether the authorisation of this section provides for biometric comparison of the collected data or not has not been investigated so far. Currently under investigation too is the consequence of the new characteristics of the data collected by "smart" CCTV systems. The new technology aims at detecting behavioural patterns, but may also detect sensitive data such as disabilities or ethnic groups on the basis of behavioural patterns or appearance. As Section 6b BDSG was not drafted for these cases, the question will have to be answered whether the law provides for this new level of data processing.

Another common feature of public, large-scale scenarios is the unclear situation as regards the competence for the collection of biometric data, its processing and the possible subsequent danger prevention measures. Even in today's airports, railway stations, sport stadiums and other open venues, the borders between "public" and "private" spheres have been blurred to a considerable extend, leading to complicated models of public-private-partnerships in the domain of public security. From a legal point of view, this raises severe questions of competence and accountability [Gu01] [St97]. It could also come into conflict with the concept of informational separation of powers recognised by the *Bundesverfassungsgericht* in the population census decision (*Volkszählungsurteil*) [BV83, 69]. As regards CCTV systems and fingerprint recognition systems, there need to be clear legal provisions about the data controller, the data collection and transmission between public authorities and possible private actors.

For instance, several bodies may be in charge to control baggage and freight in airports. In Germany, these are the German Federal Police (*Bundespolizei*) as regards controlling baggage, the aviation company as to the freight control, the police authority of the respective *Land* as to the control of airport staff, and both the captain and the *Bundespolizei* as to the control in the airplane [Gi07, 49/54/55/75]. Further, private security firms may be obliged to carry out these control measures (see Sections 8 and 9 of the German Aviation Security Act, *Luftsicherheitsgesetz*). This diversity of the parties involved in the implementation of security measures at national level is recognised by the EU legislator (see Recital 9 of the EC Regulation 2320/2002).

[5] For the United Kingdom, protection against CCTV surveillance is guaranteed by the Data Protection Act 1998 and the CCTV Code of Practice 2008 by the Information Commissioner´s Office. As to France, the loi n°95-73 du 21 janvier 1995, the décret n°96-926, the arrêté du 26 septembre 2006 and especially the décret du 3 aout 2007 apply.

In future, another major legal challenge within the context of biometric systems will relate to court evidence. One example for this could be the conviction of a subject on the basis of the outcome of a biometric comparison: On which threshold of a biometric system could this be based in different settings? In Germany, the Federal Criminal Court (*Bundesgerichtshof*) ruled that even the highly secure DNA analysis must not be the only evidence for the conviction of the accused [BG98]. For prevention scenarios in particular, the requirement for subsequent measures is usually a threat to public safety. So far, it remains completely unclear under which circumstances the existence of such a threat may be solely based on the outcome of a biometric process or technical behavioural analysis.

In the end, the new systems must comply with legal requirements concerning the privacy-friendly technical design. According to the principle of data minimisation (see Article 6 (1) (c) DPD and Section 3a BDSG respectively), the processing of data must not be excessive in relation to the purposes for which they are collected. Thus anonymous or at least pseudonymous data must be used wherever possible. For example, this may be possible in the case of the behavioural analysis in the CCTV setting, where the technical analysis itself can be conducted without personal data and the pictures in control rooms could blur people's faces as long as there is no incident [St05].

5. Conclusion

It has become clear that new technical possibilities of biometric systems lead to new challenges for personal privacy and data protection. At least in Germany, data protection laws do not specifically cover biometric data, which for example represent fingerprints or behavioural patterns of data subjects. In addition, data subjects are so far often not aware of the information quality that is revealed from latent fingerprints and bodily movements.

The amount of the new challenges depends on the respective technical design. Automated collection of biometric data enables law enforcement authorities not only to prosecute the accused but also proactively collect information about an unspecified group of persons. Hence, entire societies may be posed under suspicion if there are no technical and legal safeguards in place. In consequence, citizens may feel of being watched and adapt their behaviour so that they hide individual characteristics.

Technology may on the other hand, depending on the design, also preserve personal privacy and data protection. However, this may be limited in certain scenarios if the sole aim of a biometric system is the identification of an unknown person in a large group of other persons or the mapping of a large amount of newly captured biometric data on a biometric database.

For certain purposes such as prevention of serious crime, a biometric system might be a pressing need for the society. Further, secret collection of data may be necessary for police work. Prevention however, by the very nature of the concept, cannot be restricted to a group that only consists of dangerous persons. Thus, one has to establish procedural

rules that enable data subjects to seek judicial review. In addition, places where data are collected secretly may require a notice to the data subject in order to enable him/her to decide where he/she can behave freely without worrying about the interpretation of that behaviour at the other end of the surveillance system.

The specific aspects of biometric characteristics necessitate a very cautious approach because of the unique and durable relation to the data subject. This is caused by the fact that biometric characteristics can be used to single someone out and do, in principle, not change during the course of the data subject's life. Thus, the data subject may be deprived of choosing his/her role according to the respective situation because others may interconnect different sets of data about him/her. Hence, biometric template protection regimes that utilise renewable and irreversible representations of biometric data may be an option to ensure that data can only be used by a certain authority for a certain purpose in a certain biometric system. This sort of purpose limitation by design could also prevent or reduce the risk of identity theft. Moreover, long-term storage of biometric data may require regular data security measures, for example, fresh re-encryption since state-of-the-art cryptosystems may become ineffective after a certain period of time.

Finally, users of biometric systems for law enforcement purposes need to take error rates into account. From this it follows that the data subjects singled out by the biometric system must not be subject to particularly burdensome consequences of police measures on the sole basis of the biometric recognition or rejection. Rather, the police legislator and the executing officer always have to be aware of the actual efficiency of the recognition mechanisms and the contents of the data pools in use to avoid sanctioning the "wrong" person by putting him/her under suspicion or hindering that person to travel, move freely, and keep his/her property.

The function of the law – particularly the fundamental rights to privacy and informational self-determination, as well as the respective data protection acts – needs to be the protection of the personal rights of the data subjects. To this end, specific provisions for certain application scenarios may be necessary in the future. Furthermore, a legally compliant technology design is able to significantly reduce privacy and data protection risks. The earlier in the process of research and development this takes place, the better the potential outcome for privacy enhancing technologies.

Bibliography

[Al03] Albrecht, A.: Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Nomos, Baden-Baden 2003.

[Bi02] Bizer, J.: Selbstauthentifizierende Ausweiskarte, Datenschutz und Datensicherheit 2002, p. 44.

[BG98] Bundesgerichtshof, Decision of 2 September 1997, Neue Zeitschrift für Strafrecht 1998, p. 97.

[Br09] Breebaart, J.; Yang, B.; Buhan-Dulman, I. ; Busch, C.: Biometric Template Protection. The need for open standards, (Datenschutz und Datensicherheit) 2009, pp. 299-304.

[BV83] Bundesverfassungsgericht, BVerfGE (Collection of decicions), volume 65, pp. 1-71 („Volkszählungsurteil“).

[BV08] Bundesverfassungsgericht, BVerfGE (Collection of decisions), volume 120, pp. 378-433 (number plate recognition), press release in English at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-027en.html.

[Gi07] Giemulla, E.; Rothe, B.: Recht der Luftsicherheit, Springer Verlag, Berlin 2008.

[GoPr03] Golembiewski, C.; Probst, T.: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen (Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag), available at http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, Kiel 2003.

[Gu01] Gusy, C.: Polizei und private Sicherheitsdienste im öffentlichen Raum – Trennlinien und Berührungspunkte, Verwaltungsarchiv 2001, pp. 344-367.

[GuHe08] Gutwirth, S.; De Hert, P.: Regulating Profiling in a Democratic Constitutional State. In (Hildebrandt, M.; Gutwirth, S. Eds.): Profiling the European Citizen. Cross-Disciplinary Perspectives, Springer Verlag, 2008, 271-293.

[HeGu06] De Hert, P.; Gutwirth, S.: Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In (Claes, E.; Duff, A.; Gutwirth, S. Eds.): Privacy and the criminal law, Intersentia, Antwerp/Oxford 2006, pp. 61-104.

[Ho04] Hornung, G.: Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft, Kritische Justiz 2004, pp. 344-360.

[Ho05] Hornung, G.: Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Nomos, Baden-Baden 2005.

[Ho07] Hornung, G.: Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht. Der Gesetzesentwurf der Bundesregierung zur Änderung des Passgesetzes und weiterer Vorschriften, Datenschutz und Datensicherheit 2007, pp. 181-185.

[HoSc09] Hornung, G.; Schnabel, C., Data protection in Germany I: The population census decision and the right to informational self-determination, Computer Law & Security Review 2009, pp. 84-88, also available at http://cms.uni-kassel.de/unicms/fileadmin/groups/w_030405/Gerrit_Hornung/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf.

[Me07] Meints, M.; Biermann, H.; Bromba, M.; Busch, C.; Hornung, G.; Quiring-Kock, G.: Biometric Systems and Data Protection Legislation in Germany. In (Pan, J.-S.; Niu, X.-M.; Huang, H.-C.; Jain, L. C. Eds.): 2008 Fourth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE 2008, pp. 1088-1093.

[PA10] German ID Card Act (*Personalausweisgesetz*), of 18.6.2009, Federal Law Gazette I, p. 1346.

[PG09] German Passport Act (*Passgesetz*) of 20.7.2007, Federal Law Gazette I, p. 1566.

[Pi07] Pieroth, B.; Schlink, B.; Kniesel, M.: Polizei- und Ordnungsrecht, 3rd ed., Verlag C.H. Beck, Munich 2005.

[St97] Stober, R.: Staatliches Gewaltmonopol und privates Sicherheitsgewerbe – Plädoyer für eine Police-Private-Partnership, Neue Juristische Wochenschrift 1997, pp. 889-896.

[St05] v. Stechow, C.: Datenschutz durch Technik. Rechtliche Förderungsmöglichkeiten von privacy enhancing technologies am Beispiel der Videoüberwachung, DUV Verlag, Wiesbaden 2005.

[TSS96] Tomko G. J.; Soutar C.; Schmidt G. J.: Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996 (Priority date: Sept. 7, 1994).

[WHO 03] Woodward, J. D., Jr.; Orlans, N. M.; Higgins, P. T.: Biometrics. Identity Assurance in the Information Age, McGraw-Hill Osborne Media, New York 2003.

[WP03] Article 29 Data Protection Working Party: Working document on biometrics, 12168/02/EN, WP 80, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf, Brussels 2003.

[WP09] Article 29 Data Protection Working Party: The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN, WP168, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf Brussels 2009.