Das aktuelle Thema

Gerrit Hornung
Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft

1. Einführung

Ein Mitarbeiter einer Firma kehrt von einer Auslandsreise zurück. Bei der Einreise am Flughafen präsentiert er in einer automatisierten Vereinzelungsschleuse seinen Reisepass, dessen Chip mit einem kontaktlosen Kontrollgerät ausgelesen wird, blickt kurz in eine Kamera und betritt danach deutsches Territorium. Um sich auf dem Weg zur Firma mit Bargeld zu versorgen, hält er an einer Filiale seiner Bank. Nach dem Einführen seiner EC-Karte blickt der Mitarbeiter in den angebrachten Iris-Scanner und erhält den gewünschten Betrag. Das Betriebsgelände betritt er nach einer Kontrolle, die mit derjenigen an der Grenze identisch ist und nur statt seines Reisepasses den Personalausweis verwendet. An seinem Schreibtisch angekommen, legt der Mitarbeiter seinen Finger auf den Scanner neben seinem PC und beginnt danach, die in der Abwesenheit angekommenen Emails zu lesen.

Dieses Szenario ist teilweise bereits Realität, teilweise wird die Einführung entsprechender Systeme erwogen. Worin liegt der Unterschied zu bisherigen Verfahren der Authentifikation? Der erwähnte Mitarbeiter hat wie bisher gegenüber vier verschiedenen Kontrollstellen eine Aussage über seine Identität getroffen. Hierzu bediente er sich – ebenfalls wie bisher – eines Legitimationsmechanismus. Weder Grenzbeamte noch Bankangestellte noch Pförtner großer Betriebe noch PCs schenken der bloßen Aussage einer Person über ihre Identität Glauben; in aller Regel werden die Sicherungsmittel »Besitz« (z. B. einer Chipkarte) und/oder »Wissen« (eines Passwortes oder einer PIN) eingesetzt.

Biometrische Systeme knüpfen demgegenüber direkt an das Sicherungsmittel »Sein« an, indem sie ein Attribut des Merkmalsträgers unmittelbar aufnehmen und als Legitimationsmechanismus einsetzen.[1] Die Vorteile sind offensichtlich: Zumindest im Grundsatz können weder Gesicht noch Iris noch Finger einer Person vergessen, gestohlen oder missbräuchlich weitergegeben werden. Jenseits der mehr praktischen (deshalb allerdings keinesfalls zu unterschätzenden) Vorteile der Befreiung des Nutzers von Chipkartenflut und persönlichem Passwortmanagement ist es diese unmittelbare Bindung an die Person, die die Biometrie für jeden Authentifikationsvorgang attraktiv macht.

1 Bei bestimmten Kontrollen (z. B. mittels Dokumenten, die über ein Photo verfügen), ist dies auch heute schon der Fall. Die grundlegende Neuerung der Biometrie liegt dann in der Automatisierung des Vorgangs.

Wo liegen dann ihre Probleme? Bei der nächsten Reise stellt der Mitarbeiter bei einem Zwischenstop im Ausland fest, dass der Chip seines Reisepasses äußerlich unmerklich beschädigt ist. Die herbeieilenden Beamten schöpfen Verdacht und unterziehen ihn einer eingehenden Befragung, die dazu führt, dass der Anschlussflug verpasst wird. Nach der um einen Tag verspäteten Rückkehr bemerkt der Mitarbeiter die empörte Stellungnahme des Betriebsrats, der die Installation eines geheimen Gesichtserkennungssystems an einer Vielzahl von Stellen im Betrieb aufgedeckt hat. Der PC wurde vorsorglich in Verwahrung genommen, da es zu Manipulationen an dem biometrischen Sensor gekommen ist und in einigen Fällen der unberechtigte Zugriff auf Daten gelang. Unter den abgerufenen Emails befindet sich eine Nachricht der Bank, dass der Mitarbeiter aufgrund seiner fortschreitenden Augenkrankheit leider in absehbarer Zeit für das Iriserkennungssystem nicht mehr geeignet sein wird und Bargeldabhebungen nur noch gebührenpflichtig am Schalter möglich sein werden.

Dieses Szenario ist hypothetisch. Es verdeutlicht jedoch, dass der Einsatz von Biometrie Probleme mit sich bringen kann. Diese können technischer und organisatorischer, aber auch rechtlicher Natur sein. Folglich darf sich die Implementierung der Systeme nicht ausschließlich nach der technischen Eignung und wirtschaftlichen Machbarkeit bestimmen, sondern muss von Beginn an rechtliche Kriterien mit einbeziehen. Deren Gewichtung wird in Abhängigkeit zur jeweiligen Einsatzumgebung unterschiedlich ausfallen: Der Einsatz von Biometrie kann im einen Fall rechtlich unproblematisch, im anderen rechtlich unzulässig sein. Um die mit der Technik verbundenen Risiken bereits im Vorfeld nach Möglichkeit auszuschließen, sollten jedoch schon auf der Ebene der technischen Gestaltung der Systeme Vorgaben und Regelungsziele insbesondere des Verfassungsrechts einbezogen werden.[2]

2. Grundlagen

Das Wort Biometrie setzt sich zusammen aus den griechischen Bestandteilen bios (Leben) und metron (Maß) und bezeichnet damit die Körpermessung an Lebewesen.[3] Im vorliegenden Zusammenhang kann Biometrie – enger – verstanden werden als die automatisierte Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen.[4] Anfänge wissenschaftlicher Beschäftigung mit der Biometrie finden sich am Ende des 19. Jahrhunderts.[5] Die heutigen Verfahren verwenden einzelne

2 Zum Einsatz von Recht zur Technikgestaltung vgl. grundlegend Roßnagel, Rechtswissenschaftliche Technikfolgenforschung, 1993, 241 ff. und passim. S. ferner ders., ZRP 1992, 55 ff.; ders., Rechtliche Regelungen als Voraussetzung für Technikgestaltung, in: Müller/Pfitzmann (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, 1997, 361 ff.; Steinmüller, Informationstechnologie und Gesellschaft, 1993, 595 ff.

3 Nolde, Grundlegende Aspekte biometrischer Verfahren, in: dies./Leger (Hrsg.), Biometrische Verfahren, 2002, 20; Golembiewski/Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen (Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, abrufbar unter http://www.datenschutzzentrum.de/down load/Biometrie_Gutachten_Print.pdf), 2003, 9.

4 Behrens/Roth, Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt, 2001, 1 f.; Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Biometrische Identifikationssysteme, BT-Drs. 14/10005 (2002), 9. Zu weiteren Begriffsbestimmungen s. etwa Donnerhacke, DuD 1999, 151; Behrens/Roth, DuD 2000, 327 f.; Woodward/Orlans/Higgins, Biometrics. Identity Assurance in the Information Age, 2003, 27; Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, 31 m. w. N.

5 Zur historischen Entwicklung s. Albrecht (Fn. 4), 33 f. m. w. N.; Woodward/Orlans/Higgins (Fn. 4), 25 f.; 45 ff.; Weichert, CR 1997, 369 f.

Körpermerkmale zur Wiedererkennung von Personen; es besteht weder ein technischer noch ein historischer Zusammenhang mit der pseudowissenschaftlichen Klassifizierung von Menschen anhand ihrer Physiognomie in der Zeit des Nationalsozialismus.
Das am meisten verwendete Merkmal ist bislang der Fingerabdruck,[6] daneben gibt es vor allem Systeme für Gesicht, Iris, Handgeometrie, Stimme und Handschrift.[7] Auf eine Darstellung der spezifischen Funktionsweisen und Besonderheiten der jeweiligen Verfahren wird an dieser Stelle verzichtet.[8] Zur Analyse und Bewertung der mit der Biometrie verbundenen Rechtsfragen sind jedoch ein gewisses Grundverständnis des technischen Ablaufs und die Kenntnis über Leistungsfähigkeit und Anwendungsfelder unumgänglich.

2.1. Technischer Ablauf

Biometrische Erkennungssysteme arbeiten im Wesentlichen nach verallgemeinerbaren Prozessabläufen.[9] Um eine Authentifikation (Bezeugung der Echtheit einer Person) mittels biometrischer Merkmale zu ermöglichen, müssen zunächst mit Sensoren Referenzdaten gewonnen werden. Dies geschieht im Rahmen des so genannten Enrolments, das die erstmalige Merkmalsgewinnung, Verarbeitung und Umwandlung, etwaige Extraktions- und Komprimierungsverfahren und die Speicherung der Referenzdaten umfasst. Schlägt der Prozess des Enrolments fehl, so wird der prozentuale Anteil der fehlgeschlagenen Versuche als False Enrolment Rate oder Failure to Enrol Rate (FER) bezeichnet. Ein solcher Vorgang kann zum einen durch Fehler des Systems bedingt sein. Zum anderen gibt es bei den meisten Merkmalen einen gewissen Prozentsatz der Bevölkerung, der diese entweder überhaupt nicht oder nicht in hinreichender Ausprägung für die biometrische Authentifikation besitzt. Die Schätzungen für den Fingerabdruck liegen hier zwischen 1 und 4%.[10] Eigenangaben des Herstellers von Iriserkennungssystemen Iridian gehen für die Iris von 0,6% aus.[11] Beim Gesicht können dagegen, von schwersten Verstümmelungen abgesehen, alle Menschen in die Systeme enroled werden.[12]
Im Rahmen des späteren Vergleichsprozesses (Matching) werden die aktuell beim Merkmalsträger erhobenen Daten mit den gespeicherten Referenzdaten verglichen.

6 Woodward/Orlans/Higgins (Fn. 4), 213, nennen einen Marktanteil von einem Drittel.

7 Erprobt wird daneben die Erkennung von Bewegungsmustern beim Gang, Hand- und Gesichtsvenenmustern, Geruch, Tippverhalten und Ohrmuschelkontur. Zu diesen und anderen »esoterischen« biometrischen Verfahren s. Woodward/Orlans/Higgins (Fn. 4), 115 ff. S. a. den Überblick bei TAB (Fn. 4), 9.

8 S. insoweit die Beiträge in: Jain/Bolle/Pankanti, Biometrics. Personal Identifikation in Networked Society, 1999, Kap. 2–13 und in: Behrens/Roth, Biometrische Identifikation, 2001, II. Teil; sowie Woodward/Orlans/Higgins (Fn. 4), Kap. 3–7; Albrecht (Fn. 4), 39 ff. Ein ideales biometrisches Merkmal sollte universell (bei jedem Menschen vorhanden), einzigartig, permanent und erfassbar sein, s. Jain/Bolle/Pankanti, ebd., 4; TeleTrusT e. V., Kriterienkatalog – Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren (abrufbar unter http://www.teletrust.de/publikat. asp?id=40600), 2002, 7.

9 S. zum Folgenden Behrens/Roth (Fn. 8), 10 ff.; Gundermann/Probst, Biometrie, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Rn. 8 ff.; Albrecht (Fn. 4), 35 ff.; Nolde (Fn. 3), 22; TeleTrusT (Fn. 8), 2 f.; Woodward/Orlans/Higgins (Fn. 4), 28 ff.

10 Sietmann, c't 5/2002, 146 (2–4%); Woodward/Orlans/Higgins (Fn. 4), 22 (1–4%); TAB, Biometrie und Ausweisdokumente (abrufbar unter http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf), 2003, 5 (2%). Gründe sind Abrieb bei körperlich arbeitenden Berufstätigen, Amputationen oder Missbildungen.

11 Ähnlich Bolle/Connell/Pankanti/Ratha/Senior, Guide to Biometrics, 2004, 114 (0,5%). Blinde Menschen sind etwa nicht zum Einsatz des Iris-Scans geeignet, s. Woodward/Orlans/Higgins (Fn. 4), 99.

12 TAB (Fn. 10), 63. Dies war einer der Gründe für die International Civil Aviation Association, den Staaten die Verwendung von Gesichtsdaten in Reisedokumenten zu empfehlen, s. ICAO, Biometrics Deployment of Machine Readable Travel Documents (abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm), 2003, 15.

Hierzu gibt es unterschiedliche Verfahren. Eine Möglichkeit besteht darin, die beim Enrolment gewonnenen Daten komplett aufzubewahren und später abzugleichen. In der Praxis wird jedoch stattdessen mit aufbereiteten Daten gearbeitet. Dies kann auf zwei Arten geschehen: mittels eines standardisierten Datenformats, das aber im Wesentlichen immer noch alle erhobenen Daten enthält (Volldaten oder »image data«, beispielsweise JPEG-, JPEG 2000- oder WSQ-komprimierte Bilder), oder mittels eines extrahierten Datensatzes, der nur einzelne, charakteristische Teile der erhobenen Rohdaten berücksichtigt (Template). Eine letzte Möglichkeit besteht in der Verwendung templatefreier Verfahren.[13] Dabei wird aus den biometrischen Rohdaten ein kryptographischer Schlüssel berechnet und mit diesem ein beliebiger Text verschlüsselt. Dieser wird im Klartext und in seiner verschlüsselten Form als Referenzdatensatz gespeichert. Derartige Verfahren kommen ohne die Speicherung biometrischer Referenzdaten aus.[14]

Die Systeme unterscheiden sich auch hinsichtlich des Speicherungsortes für die Referenzdaten (je nach Verfahren Volldaten, Templates oder Klartext nebst verschlüsseltem Text). Bei einer zentralen Speicherung werden vor Ort die biometrischen Daten erhoben und an eine Recheneinheit gesandt, die das Matching vornimmt. Die Referenzdaten können aber auch dezentral auf einem portablen Medium (in der Regel eine Chipkarte) gespeichert werden. Dann liest entweder eine Kontrolleinheit die Referenzdaten aus und nimmt das Matching vor, oder sie sendet umgekehrt die neu erhobenen Daten an die Karte, und die Überprüfung findet in dieser statt (Matching-On-Card). Außerdem gibt es Verfahren, bei denen das Medium auch über einen Sensor verfügt. Dann kann auf eine Kontrolleinrichtung völlig verzichtet werden.

Eine biometrische Authentifikation kann durch zwei Verfahren geschehen, nämlich durch Verifikation oder Identifikation.[15] Bei der Verifikation findet ein Vergleich der im Einzelfall erhobenen Daten mit einem konkreten Referenzdatensatz statt (1:1). Es wird überprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Die Identifikation hingegen erfolgt durch einen Vergleich mit allen Referenzdaten (1:n). Hierbei wird festgestellt, um welche Person es sich tatsächlich handelt.

Im Unterschied zu einer Passwortkontrolle, die stets ein eindeutiges Ergebnis liefert (1 oder 0; das Passwort ist richtig oder falsch), arbeiten biometrische Verfahren mit relativen Übereinstimmungsgraden, weil wegen der Funktionsweise der Systeme (insbesondere Mess- und Bedienungsfehler) keine vollständige Übereinstimmung erreichbar ist.[16] Eine totale Gleichartigkeit der Datensätze ist allerdings auch nicht erforderlich. Wenn eine hinreichende Unterschiedlichkeit des verwendeten Merkmals vorliegt, kann auch eine niedrigere Übereinstimmung für die Praxis ausreichend sein. Es verbleibt jedoch immer die Möglichkeit, dass bei der Überprüfung fälschlicherweise eine Übereinstimmung oder Nicht-Übereinstimmung ermittelt wird. Die Wahrscheinlichkeit einer ungerechtfertigten Zurückweisung wird als False Rejection Rate (FRR), die einer ungerechtfertigten Akzeptanz als False Acceptance Rate (FAR) bezeich-

13 Vgl. näher Albrecht/Probst, Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme, in: Behrens/Roth (Fn. 8), 39 f.; Gundermann/Probst (Fn. 9), Rn. 24 f.; Probst, Biometrie aus datenschutzrechtlicher Sicht, in: Nolde/Leger (Fn. 3), 124 f.; Albrecht (Fn. 4), 56 f.

14 Es ist allerdings nicht zutreffend, dass hierdurch jede Verwendung personenbezogener Daten entfiele, wie dies bisweilen dargestellt wird. S. dazu Hornung, DuD 2004, 429, 431.

15 S. Probst, DuD 2000, 322; Behrens/Roth (Fn. 8), 10 ff.; Nolde (Fn. 3), 22 f., 26 f.; Woodward/Orlans/Higgins (Fn. 4), 7 f.; Albrecht (Fn. 4), 38.

16 Vgl. Munde, Die Evaluation biometrischer Systeme – Im internationalen Kontext, in: Nolde/Leger (Fn. 3), 148 f.; Albrecht (Fn. 4), 36; Gundermann/Probst (Fn. 9), Rn. 14 ff. Ausführlich zu Fehlermessungen und -berechnungen TeleTrusT (Fn. 8), 9 ff.; Bolle/Connell/Pankanti/Ratha/Senior (Fn. 11), 63 ff., 87 ff., 269 ff. Gründe sind etwa eine zu geringe Ausprägung der Merkmale, Mess- und Bedienungsfehler beim Enrolment und Matching, Probleme bei der Berechnung der Templates und Änderungen der verwendeten biometrischen Merkmale über die Zeit.

net.[17] Die FRR ist damit eine Angabe darüber, wie viel Prozent der an sich berechtigten Nutzer vom System zurückgewiesen werden, während die FAR die Wahrscheinlichkeit dafür angibt, dass ein an sich zurückzuweisender Merkmalsinhaber dennoch fälschlicherweise als Berechtigter identifiziert wird. Beide Raten sind nicht theoretisch herleitbar, sondern müssen immer auf der Basis praktischer Tests bestimmt werden.
FRR und FAR sind vom eingestellten Schwellwert[18] und von der Grundgenauigkeit des Systems abhängig. Je höher der Schwellwert liegt, desto geringer wird die FAR. Eine niedrige FAR ist etwa für die Zugangssicherung zu Hochsicherheitsbereichen erwünscht. Gleichzeitig steigt jedoch die FRR an. Da hierdurch berechtigte Merkmalsträger abgewiesen werden, ist aus ihrer Sicht regelmäßig eine geringe FRR vorteilhaft.[19] In diesem Fall steigt jedoch die FAR an, was zu Sicherheitsproblemen führen kann. Die beiden Fehlerraten beeinflussen sich also gegenseitig.[20]

2.2. Derzeitige Leistungsfähigkeit

Die tatsächliche Leistungsfähigkeit biometrischer Systeme ist relativ schwierig einzuschätzen. Zunächst mangelt es an einheitlichen Testkriterien.[21] Sodann ist den Zuverlässigkeitsangaben der Hersteller meist mit Vorsicht zu begegnen.[22] Daten aus Pilotprojekten beziehen sich häufig auf freiwillige, nicht repräsentativ ausgewählte Probanden, sodass nur eingeschränkt Aussagen über eine Verwendbarkeit für große Nutzergruppen gemacht werden können.[23] Die im Folgenden genannten Fehlerraten sind dementsprechend mit Vorsicht zu betrachten. Sie geben aber zumindest einen Eindruck über die Größenordnung der Fehleranfälligkeit.
Vergleichbare Zahlen sind vor allem für die drei derzeit für Reisedokumente favorisierten Merkmale Iris, Fingerabdruck und Gesicht verfügbar.[24] Die Iriserkennung schneidet in Vergleichstest meist am besten ab.[25] Fehlerraten werden mit 0,01–1,0%

17 Albrecht (Fn. 4), 52; TAB (Fn. 4), 11; Gundermann/Probst (Fn. 9), Rn. 14 ff.; Nolde (Fn. 3), 23 f.; Woodward/Orlans/Higgins (Fn. 4), 35 ff.

18 Dieser legt fest, wie hoch die Übereinstimmung des neuen Datensatzes mit dem Referenzdatensatz sein muss, damit der Betroffene akzeptiert wird.

19 Eine Ausnahme besteht, wenn der Merkmalsträger das biometrische Verfahren selbst zur Zugangssicherung zu eigenen Daten verwendet. In diesem Fall besteht sein vorrangiges Interesse in einer niedrigen FAR.

20 Zu den daraus entstehenden »trade-offs« Bolle/Connell/Pankanti/Ratha/Senior (Fn. 11), 81 ff.

21 TAB (Fn. 4), 20; Albrecht (Fn. 4), 60 m. w. N. Zu Ansätzen vgl. TeleTrusT (Fn. 8); TAB (Fn. 4), 23 ff.; Woodward/Orlans/Higgins (Fn. 4), 186 ff.; Munde (Fn. 16), 145 ff.; Bolle/Connell/Pankanti/Ratha/Senior (Fn. 11), 105 ff. m. w. N.

22 Vgl. etwa die Beispiele bei Albrecht, Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren, 2001, 39; Breitenstein, Überblick über biometrische Verfahren, in: Nolde/Leger (Fn. 3), 39. Nach Aussage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) waren etwa im Projekt BioFace »die Erkennungsleistungen … bei weitem nicht so gut wie sie die Werbung der Systemhersteller ihnen zubilligt[e].«, s. BSI, BioFace. Vergleichende Untersuchung von Gesichtserkennungssystemen (abrufbar unter http://www.bsi.bund.de/fachthem/BioFace/index.htmBSI), 2003, 9.

23 Im Projekt BioP I wurde beispielsweise mit 241 freiwilligen Mitarbeitern des BKA gearbeitet, die zu 95% im Alter zwischen 25 und 59 Jahren und überdurchschnittlich gut ausgebildet waren, s. BSI/BKA/Secunet, Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I (abrufbar unter http://www.bsi.de/literat/studien/biop/index.htm), 2004, 21.

24 Die folgenden Angaben beziehen sich auf den Verifikationsmodus. Das Verfahren der Identifikation erfordert eine größere Unterscheidbarkeit des Merkmals und stellt deshalb höhere Herausforderungen an die Systeme. Im kriminalistischen Bereich wird der Fingerabdruck seit längerer Zeit verwendet (AFIS-System). Auch die Iris kann für die Identifikation eingesetzt werden. Die Gesichtserkennung wurde dagegen sowohl vom BSI (Fn. 22) als auch im Rahmen des Face Recognition Vendor Tests 2002 (abrufbar unter http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf) für einen Abgleich mit großen Datenbanken im Identifikationsmodus als gegenwärtig nicht brauchbar bewertet.

25 Woodward/Orlans/Higgins (Fn. 4), 93.

(FAR) und 0,1–2,0% (FRR) angegeben.[26] Die Raten für den Fingerabdruck liegen etwas höher (FAR von 0,01% bei einer FRR von 5%,[27] bzw. Equal Error Rates um 1%[28]). Bei Gesichtserkennungsverfahren stellte der aus dem Jahre 2002 stammende Face Recognition Vendor Test für das beste System bei einer FAR von 1% eine FRR von 10% fest.[29] Allerdings stieg diese im Außenbereich auf 50% an. Dies entspricht den Ergebnissen des Projekt BioP I.[30]

2.3. Gegenwärtige und künftige Einsatzfelder

Die technische Entwicklung hat eine Vielzahl biometrischer Systeme in den letzten Jahren zur Serienreife gebracht. Ihre denkbaren Einsatzfelder sind bereits jetzt nahezu ubiquitär und erweitern sich ständig. Aufgrund der Bestrebungen zur Verbesserung von Identifizierungsmaßnahmen nach den Anschlägen des 11. September 2001 wird der öffentliche Bereich ein maßgebliches Anwendungsgebiet werden, das nicht nur die Verbrechensbekämpfung,[31] sondern auch Grenzkontrollen,[32] staatliche Identifikationsdokumente[33] und eine EU-weite Zentraldatei der Fingerabdrucksdaten von Asylbewerbern[34] umfassen wird. Im Ausland existieren überdies bereits Systeme zur Vermeidung des Missbrauchs von Sozialleistungen.[35]

Ein wichtiges Einsatzgebiet biometrischer Verfahren sowohl im hoheitlichen als auch im privaten Bereich wird in Zukunft die Zugangskontrolle in Behörden und Betrieben sein. Atomkraftwerke sichern den Zutritt schon seit längerem mittels Biometrie. Am London City Airport läuft ein System im Vollbetrieb, bei dem 1.600 Angestellte mit dem Fingerabdruck Zugang zu Sicherheitsbereichen erhalten.[36] Der Zugang zum Olympischen Dorf der Sommerspiele in Atlanta im Jahre 1996 wurde mittels Handgeometrie gesichert.[37]

26 TAB (Fn. 4), 20. S. a. Bolle/Connell/Pankanti/Ratha/Senior (Fn. 11), 114 f. Die Wahrscheinlichkeit, für zwei Betroffene dasselbe Template zu errechnen, liegt nach Eigenangabe des Patentinhabers Daugman bei $1:10^{78}$, s. Breitenstein (Fn. 22), 49.

27 TAB (Fn. 4), 20.

28 Ergebnis der Fingerprint Verification Competition, s. http://bias.csr.unibo.it/fvc2002/. Allerdings erreichten im Projekt BioFinger (BSI/BKA/IGD, Evaluierung biometrischer Systeme Fingerabdrucktechnologien – BioFinger, abrufbar unter http://www.bsi.de/literat/studien/BioFinger/BioFinger_I.pdf, 2004, 2) nur 8% der am Markt verfügbaren Systeme diesen Wert.

29 S. Fn. 24, 2 f.

30 BSI/BKA/Secunet (Fn. 23), 10.

31 Hierzu wird insbesondere die Fingerabdruckserkennung schon seit längerer Zeit in automatisierter Form eingesetzt, s. ausführlich Woodward/Orlans/Higgins (Fn. 4), 45 ff.

32 Pilotprojekte gibt es in Flughäfen der USA (INSPASS-System, Handgeometrie), in Amsterdam (Iris) und seit dem 13. 2. 2004 in Frankfurt (Iris, s. http://www.bundesgrenzschutz.de/Auto_Grenzkontrolle/index.php).

33 S. näher unten 5.2. Neben allgemeinen Identifikationspapieren ist auch die schnelle Einführung eines einheitlichen Visums zur Einreise in die EU vorgesehen. Pilotprojekte hierzu laufen bei der Visa-Beantragung in Lagos (Fingerabdruck) und Manila (Iris-Scan).

34 EUROCAC-Programm, vgl. VO (EG) Nr. 2725/2000 v. 11. Dezember 2000, ABl. EG L 316 und VO (EG) Nr. 407/2002 v. 28. Februar 2002, ABl. EG L 62, 5. 3. 2002. S. näher Golembiewski/Probst (Fn. 3), 11 f.

35 Die Niederlande geben seit 1997 Asylbewerberausweise mit biometrischen Daten aus, s. Weichert, CR 1997, 369, 373. Einige US-Bundesstaaten setzen Fingerabdrucksverfahren zur Missbrauchsbekämpfung im Sozialhilfebereich ein, und bei der Ausgabe von Hilfslieferungen durch den UN-Flüchtlingskommissar in Pakistan werden Iris-Scans gespeichert, vgl. Woodward/Orlans/Higgins (Fn. 4), 284 ff., 287 f.

36 Zu ähnlichen Plänen in Deutschland vgl. Deutsches Forum für Kriminalprävention (DFK), Airport-Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen (abrufbar unter http://www.kriminalpraevention.de/download-data.htm), 2004, 17 ff.

37 S. Breitenstein (Fn. 22), 63.

Beispiele aus dem privaten Bereich umfassen die Essensausgabe in Kantinen von US-Schulen,[38] die automatische Aktivierung individueller Fahrzeugeinstellungen in Kraftfahrzeugen per Fingerabdruckerkennung, den Einsatz von Iriserkennung bei Geldautomaten und von Stimmerkennung im Online-Banking,[39] die Zugriffssicherung für PCs und Speichermedien mit Hilfe von Fingerabdrucksensoren,[40] Online-Bezahlfunktionen im Handel und in der Gastronomie,[41] sowie Zugangskontrollen für Saisonkarteninhaber in Disney World (Fingerabdruck und Handgeometrie)[42] und im Zoo der Stadt Hannover (Gesicht).[43]

3. Risiken für die Merkmalsträger

Im Vergleich mit bisherigen Methoden der Identifizierung birgt die Verwendung von Biometrie eine Reihe spezifischer Risiken. Ein Problem ist die Frage, inwieweit biometrische Daten Überschussinformationen enthalten, beispielsweise über die Gesundheit des Merkmalsträgers. Derartige Rückschlüsse sind umstritten und geben jedenfalls nur bestimmte Korrelationen an; es ist also nicht möglich, definitive Aussagen zu treffen. Dennoch scheinen gewisse Zusammenhänge zu bestehen.[44] Wenn diese hinreichend gewichtig sind, könnten sich – beispielsweise beim Kontakt mit potentiellen Arbeitgebern oder Versicherungen – negative Folgen für die Betroffenen ergeben.
Zentrale Datenbanken biometrischer Daten erleichtern die Kontrolle großer Personengruppen. Vor den damit verbundenen negativen Folgen für die Ausübung demokratischer Freiheitsrechte hat das Bundesverfassungsgericht schon im Volkszählungsurteil gewarnt.[45] Würde eine Datenbank aller Gesichtsbilder der Bevölkerung eingerichtet,[46] so wäre – bei entsprechendem technischen Fortschritt – der Abgleich mit den Bildaufnahmen einer Demonstration denkbar. Die lebenslange Bindung biometrischer Daten an den Betroffenen erleichtert überdies die fortgesetzte Datensammlung und Profilbildung über eine Person: Ein Ausweichen ist noch nicht einmal durch den Wechsel der Identität im Rahmen von Zeugenschutzprogrammen möglich.[47]
Auch die Intransparenz der Datenverwendung ist problematisch. Einige biometrische Daten können für den Träger unmerklich erhoben werden: durch direkte verdeckte Erhebung (insbesondere beim Gesicht), latente Spuren (Fingerabdruck) oder das Auslesen aus mitgeführten Chipkarten mit kontaktlosen Schnittstellen.[48]

38 Vgl. Albrecht (Fn. 4), 25 m. w. N.
39 S. Albrecht (Fn. 22), 12; Breitenstein (Fn. 22), 62; Woodward/Orlans/Higgins (Fn. 4), 337 ff., 345 f.
40 Es gibt inzwischen eine Reihe von USB-Speichern, die über derartige integrierte Sensoren verfügen.
41 Vgl. Ziegler, c't 12/2003, 38. S. a. Albrecht (Fn. 22), 14; http://www.heise.de/newsticker/meldung/39192/.
42 S. Hadley, EMBO reports 2004, 124, 125; Woodward/Orlans/Higgins (Fn. 4), 67 f.
43 http://www.heise.de/newsticker/meldung/36097. S. a. Golembiewski/Probst (Fn. 3), 10.
44 Es werden beispielsweise Zusammenhänge zwischen bestimmten Fingerabdrucksmustern und chronischen Magen-Darm-Beschwerden, Leukämie, Rubella-Syndrom und Brustkrebs genannt. Aus Irisdaten sollen sich Erkenntnisse über Erkrankungen wie Diabetes, Arteriosklerose, Bluthochdruck und AIDS ergeben. S. näher Woodward/Orlans/Higgins (Fn. 4), 202 f.; Gundermann/Probst (Fn. 9), Rn. 26.; Albrecht (Fn. 4), 173. Umstritten sind Zusammenhänge zwischen Fingerabdruck und Homosexualität (Hall/Kimura, Behavioral Neuroscience 1994, 1203 ff.) oder ethnischer Herkunft (Gundermann/Köhntopp, DuD 1999, 143, 150). Jedenfalls lässt sich beispielsweise aus Gesichtsinformationen auf diese Herkunft und das Geschlecht schließen.
45 »Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.«, s. BVerfGE 65, 1 (43).
46 Der Bund Deutscher Kriminalbeamter fordert etwa eine EU-weite Fingerabdrucks-Datenbank sämtlicher Bürger, vgl. http://www.heise.de/newsticker/data/pmz-03.11.03-000/.
47 Probst (Fn. 13), 120 f.; Albrecht (Fn. 4), 186.
48 Bei derartigen Radio Frequency (RF)-Interfaces kann je nach Funktionsweise des Chips und der Antenne der Datensatz auch aus großen Entfernungen ausgelesen werden.

Gravierende Nachteile können sich ergeben, wenn ein Betroffener temporär oder dauerhaft nicht zur biometrischen Authentifikation geeignet ist. Dazu kann es durch körperliche Verletzungen und zu geringe Merkmalsausprägung kommen.[49] Bei – nie auszuschließenden – Falschzurückweisungen besteht die Gefahr, in Verdacht zu geraten, weitere Zugangsversuche unternehmen zu müssen oder letztlich sogar insgesamt abgelehnt zu werden.

Wenn biometrische Verfahren perspektivisch im Rechtsverkehr eingesetzt werden (EC-Automaten, Verfahren der elektronischen Signatur), ergibt sich die Frage der Verteilung technischer Risiken. Die Verwender könnten versucht sein, diese durch AGB auf die Nutzer abzuwälzen. Je nach Einschätzung der Überwindungssicherheit durch die Rechtsprechung wird diese – vergleichbar den Fällen des EC-Kartenmissbrauchs[50] – Beweislastregeln für Fälle des non liquet aufstellen, die den Einwand der Nichtpräsentation des Merkmals durch den Inhaber in bestimmten Fällen ausschließen.

4. Anforderungen des Datenschutzrechts

Wenn Angaben über biometrische Merkmale zur Authentifizierung verwendet werden, sind die zum Enrolment und Matching erhobenen Daten regelmäßig personenbezogen. Einschränkungen ergeben sich bei der Verwendung autarker Chipkarten mit Sensoren, bei der Speicherung der Referenzdaten in großen, anonymisierten Datenbanken und beim Einsatz templatefreier Verfahren.[51] Im Normalfall finden jedoch aufgrund des Personenbezugs die verfassungsrechtlichen Anforderungen des Grundrechts auf informationelle Selbstbestimmung[52] und die einfachgesetzlichen Vorgaben des Datenschutzrechts Anwendung.

In Betracht kommt auch ein Verstoß gegen Art. 1 Abs. 1 GG. Zwar greift die Verwendung des menschlichen Körpers zur Wiedererkennung in spezifischen Kontrollsituationen nicht in den Kernbereich menschlicher Existenz ein.[53] Dies würde sich bei weitreichenden Überwachungsmaßnahmen jedoch anders darstellen. In einem hypothetischen System einer zentralen Speicherung aller Gesichtsdaten einer Bevölkerung, die mit einer sehr großen Zahl von – technisch weiterentwickelten – Überwachungskameras im öffentlichen Raum gekoppelt wäre, könnte ein Bewegungsprofil jedes einzelnen Individuums über einen unbeschränkten Zeitraum erstellt werden. Ein derartiges Vorgehen würde gegen die Menschenwürdegarantie verstoßen, unabhängig davon, dass nur ein einzelnes biometrisches Merkmal verarbeitet würde und dem Bürger noch die Unüberwachtheit seines privaten Bereichs verbliebe.

49 Beispiele sind Schnitte oder Brüche beim Finger, verschiedene Augenkrankheiten oder Gesichtsverletzungen. Zur grundsätzlichen Nichteignung s. bereits oben 2.1.

50 Hierzu und zur Vergleichbarkeit mit der Biometrie, Albrecht (Fn. 4), 112 ff.

51 Vgl. ausführlich Hornung, DuD 2004, 429 ff. Außerhalb des normalen Ablaufs der Systeme kann der Personenbezug biometrischer Daten zweifelhaft sein, s. ebd. Dieser Aspekt bleibt im Folgenden außer Betracht.

52 Nach Gundermann/Probst (Fn. 9), Rn. 64 ff. greift die Verwendung des menschlichen Körpers noch in einen »weiteren, bislang noch nicht klar definierten Bereich« des allgemeinen Persönlichkeitsrechts ein mit der Folge, dass allgemeine Ermächtigungsgrundlagen zur Erhebung von Daten nicht zu einer Erhebung gerade biometrischer Daten ausreichen. Zum selben Ergebnis kommt man – dogmatisch überzeugender –, wenn man in der spezifischen Natur der biometrischen Daten und der spezifischen Art der Datenerhebung einen besonders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung sieht, der so wesentlich ist, dass der parlamentarische Gesetzgeber eine eigene Entscheidung hierüber treffen muss.

53 Ebenso Gundermann/Probst (Fn. 9), Rn. 51 ff. Zum Kriterium des Kernbereichs s. Höfling, in: Sachs (Hrsg.), GG, 3. Auflage 2003, Art. 1 Rn. 16 m. w. N.; Zippelius, in: Bonner Kommentar, Stand Mai 2004, Art. 1 Rn. 16.

Für das Recht auf informationelle Selbstbestimmung sind in der Judikatur des Bundesverfassungsgerichts und der Literatur grundlegende Prinzipien herausgearbeitet worden.[54] Es darf nur auf der Basis einer Einwilligung oder einer gesetzlichen Grundlage beschränkt werden, die dem überwiegenden Allgemeininteresse dient. Die Datenverwendung muss erforderlich sein. Ihr Zweck ist genau zu regeln, und die Zweckbestimmung begrenzt die zulässige Datenverwendung. Nach dem Prinzip der informationellen Gewaltenteilung sind Datenverarbeitungsbereiche für unterschiedliche Zwecke technisch und organisatorisch zur trennen, um Machtkonzentration durch unkontrollierte Verfügung über Informationen vorzubeugen. Datenverarbeitungssysteme sind so zu gestalten und auszuwählen, dass sie keine oder so wenig wie möglich personenbezogene Daten erheben, verarbeiten und nutzen. Daten sind grundsätzlich offen und beim Betroffenen selbst zu erheben (Transparenzprinzip); dieser hat Auskunftsrechte und ist vor einer Einwilligung genau aufzuklären. Schließlich ist die Bildung weitreichender Datenprofile über den Betroffenen unzulässig.

In Anwendung dieser Grundsätze ist vor dem Einsatz von Biometrie zunächst nach alternativen Sicherungsmitteln zu suchen, da andere Authentifikationsmethoden regelmäßig weniger eingriffsintensiv sind. Erfolgt der Einsatz, so ist eine präzise Zweckbestimmung (beispielsweise zur Erkennung am Betriebseingang) zu treffen. Nachträgliche Zweckänderungen bedürfen dann einer neuen Einwilligung oder normativen Ermächtigung. Die Zweckbestimmung hat auch Regeln für die Dauer der Datenspeicherung und die Datenlöschung zu enthalten.

Bei der Auswahl des Systems sind vor allem die Kriterien der Flüchtigkeit, der Mitwirkungsbindung und des Gehalts an Überschussinformationen zu berücksichtigen. Nicht flüchtige Merkmale, die in der Umgebung hinterlassen werden, lassen eine Datenerhebung auch nach langer Zeit zu. Systeme, die keine Mitwirkung der Betroffenen erfordern, kommen mit dem Transparenzprinzip in Konflikt. Überschussinformationen können nachteilige Entscheidungen (potentieller) Vertragspartner verursachen. Allerdings führen diese Kriterien nicht in jedem Fall zu eindeutigen Entscheidungen, weil verschiedene biometrische Merkmale spezifische Risiken aufweisen: So wird beispielsweise der Fingerabdruck in der Umgebung hinterlassen, das Gesicht kann in weitem Umfang verdeckt erhoben werden, die Iris scheint die meisten Informationen über die Gesundheit zu enthalten.

Vor dem Hintergrund der Risiken zentraler biometrischer Referenzdatenbanken sind diese nur zulässig, wenn kein dezentrales System verfügbar ist oder die spezifische Aufgabe eine solche Datenbank erfordert.[55] Der Einsatz von Chipkarten mit (Fingerabdruck-)Sensoren ist vorzugswürdig, weil so der Karteninhaber die alleinige Datenhoheit über die Referenzdaten und die neu erhobenen Merkmalsinformationen hat.[56] Volldatensätze dürfen nur gespeichert werden, wenn eine Verwendung von Templates nicht möglich ist.[57] Die Verwendung templatefreier Verfahren ist – wenn technisch

54 Nach wie vor maßgeblich ist insoweit das Volkszählungsurteil (BVerfGE 65, 1). S. ferner BVerfGE 78, 77 (85); 84, 192 (195) und zum Folgenden z. B. Simitis, in: ders., BDSG, 5. Auflage 2003, Einl. Rn. 30 ff.; Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, 2001, 70 ff.; Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, 1998, 85 ff.; Trute, Verfassungsrechtliche Grundlagen, in: Roßnagel (Fn. 9).

55 S. Bizer, DuD 2002, 44; Albrecht (Fn. 4), 159 ff., 162 f.; Golembiewski/Probst (Fn. 3), 69 f., 72; Woodward/Orlans/Higgins (Fn. 4), 40.

56 Das bloße Matching auf der Karte hat demgegenüber geringere Vorteile, weil immer durch Dritte neue Daten zum Matching erhoben werden, bei denen die Gefahr des Missbrauchs besteht.

57 S. a. Albrecht (Fn. 4), 173 f.; TAB (Fn. 4), 44 f. Templates sind dann datensparsamer, wenn bei ihrer Berechnung substantielle Bestandteile der Volldaten entfernt werden. Zwar bestehen in aller Regel Möglichkeiten der Rückwärtskonstruktion (s. Bromba, On the reconstruction of biometric raw data from template data, abrufbar unter http://www.bromba.com/knowhow/temppriv.htm, 2003). Vollständig entfernte Informationen können jedoch nicht mehr ermittelt werden.

möglich – vorzuziehen, weil damit zwar nicht jede Verwendung personenbezogener Daten, immerhin aber die Speicherung biometrischer Referenzdaten vermieden wird. Schließlich sind die biometrischen Daten auf technischem Wege gegen missbräuchliche Verwendungen zu schützen. Orientierung bietet insoweit die Anlage zu § 9 BDSG.[58]

Unter gleichheitsrechtlichen Gesichtspunkten ist zu fordern, dass biometrische Systeme diskriminierungsfrei implementiert werden. Bei einer dauerhaften oder vorübergehenden Nichteignung zur Authentifikation (s. o.) liegt eine Ungleichbehandlung vor. Diese ist schwerwiegend, weil sie durch die Betroffenen nicht beeinflusst werden kann.[59] Außerdem kann es bei der Erkennungsleistung zu diskriminierenden Unterschieden kommen.[60] Biometrische Systeme sind deshalb ohne effektive Rückfallsysteme unzulässig. Eine Möglichkeit sind manuelle Nachkontrollen, die ohne größere zeitliche Verzögerungen erfolgen.

Im einfachgesetzlichen Datenschutzrecht können je nach Einzelfall vor allem § 6 b und § 6 c BDSG einschlägig sein. § 6 b BDSG regelt die Videoüberwachung öffentlich zugänglicher Räume. Die Norm ist deshalb beispielsweise auf Anlagen im Betrieb nicht anwendbar. Auch ist nicht jede Videoüberwachungsanlage ein biometrisches System.[61] Es erscheint allerdings denkbar, dass künftig im öffentlichen Raum entsprechende Gesichtserkennungssysteme eingesetzt werden. In diesem Fall beschränkt § 6 b BDSG die Zulässigkeit auf die Aufgabenerfüllung öffentlicher Stellen und die Wahrnehmung des Hausrechts oder »berechtigter Interessen«.[62] Außerdem dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Beobachtung ist transparent zu machen, bei einer Zuordnung der Daten zu einer Person ist diese zu benachrichtigen, und die Daten sind nach Zweckerreichung unverzüglich zu löschen.

Die Transparenzpflichten des § 6 c BDSG finden auf »mobile personenbezogene Speicher- und Verarbeitungsmedien« (§ 3 Abs. 10 BDSG) Anwendung. Chipkarten mit biometrischen Daten sind hiervon erfasst, wenn sie mit Matching-On-Card Prozessen arbeiten oder über Sensoren verfügen.[63] In diesem Fall bestehen für die ausgebenden und diejenigen Stellen, die Verfahren auf das Medium aufbringen, ändern oder hierfür bereithalten, bestimmte Unterrichtungspflichten.[64] Außerdem müssen sie Geräte zur Wahrnehmung des Auskunftsrechts unentgeltlich zur Verfügung stellen. Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, sind für den Betroffenen eindeutig erkennbar zu machen.

58 Dazu z. B. Ernestus/Geiger, in: Simitis (Fn. 54), § 9 Rn. 1 f.; Heibey, Datensicherung, in: Roßnagel (Fn. 9).

59 Zu diesem Kriterium vgl. BVerfGE 88, 87 (96); 91, 389 (401).

60 Es gibt Berichte darüber, dass Gesichter von Männern um bis zu 9% besser erkannt werden als die von Frauen (Ergebnis des Face Recognition Vendor Tests, Fn. 24, 3), die Erkennungsleistung mit dem Lebensalter steigt (ebd.) und einige Algorithmen Schwierigkeiten bei der Erkennung von Menschen dunkler Hautfarbe haben (Breitenstein, Fn. 22, 46). Unterschiedliche ethnische Gruppen haben unterschiedliche Fingerabdruckscharakteristika (Woodward/Orlans/Higgins, Fn. 4, 32 m. w. N.). Bei der Iriserkennung führen die Vorgaben der Bilderfassung mitunter zu Problemen für Menschen aus Fernost (Breitenstein, Fn. 22, 49).

61 Dazu ist vielmehr erforderlich, dass die Gesichter der erfassten Personen automatisiert mit Referenzdaten abgeglichen werden und nicht nur eine Überwachung durch eine Kontrollperson vor einem Monitor erfolgt.

62 S. ausführlich Bizer, in: Simitis (Fn. 54), § 6 b Rn. 1 ff. m. w. N.

63 Vgl. Hornung, DuD 2004, 15, 16.

64 S. näher Hornung, DuD 2004, 15, 18 ff. m. w. N.

Der Einsatz von Biometrie wird in Zukunft insbesondere am Arbeitsplatz und in hoheitlichen Identifikationsdokumenten erfolgen. Perspektiven eröffnen sich auch für Verfahren der elektronischen Signatur. Diese Bereiche weisen spezifische Probleme auf.

5.1. Biometrie am Arbeitsplatz

Für biometrische Systeme am Arbeitsplatz ist zwischen kollektiver und individueller arbeitsrechtlicher Lage zu differenzieren. Das BAG hat in einem Beschluss vom 27. Januar 2004[65] entschieden, dass Mitbestimmungsrechte des Betriebsrats gemäß § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG bestehen. Das gilt auch dann, wenn das biometrische System in einem Kundenbetrieb des Arbeitgebers installiert ist und dieser seine Beschäftigten anweist, unter diesen Bedingungen dort Wartungsarbeiten durchzuführen.

Die Rechte der einzelnen Beschäftigten bestehen unabhängig von der Mitbestimmungspflicht. In Ermangelung eines besonderen Arbeitnehmerdatenschutzgesetzes finden die allgemeinen Regeln Anwendung. Gemäß § 4 Abs. 1 BDSG ist eine Erlaubnisnorm oder eine Einwilligung des Betroffenen erforderlich. Letzteres ist im Betrieb weitgehend unrealistisch, weil eine einheitliche Gestaltung der betrieblichen Abläufe gewährleistet sein muss. Eine gesetzliche Ermächtigung enthält § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wenn die Datenverwendung der »Zweckbestimmung« des Vertragsverhältnisses dient. Wann das im Arbeitsverhältnis gegeben ist, ist im Einzelnen streitig.[66] Möglich ist auch eine Datenverwendung auf der Basis von Tarifverträgen und Betriebsvereinbarungen.[67]

In allen diesen Fällen ist allerdings eine Abwägung zwischen dem Informationsinteresse des Arbeitgebers und dem Anspruch der Beschäftigten auf Schutz und Förderung der freien Entfaltung der Persönlichkeit aus § 75 Abs. 2 BetrVG erforderlich. Die Norm ist unter Berücksichtigung grundrechtlicher Wertungen auszulegen und geht mit dem Förderungsgebot über ein reines Abwehrrecht hinaus. Insbesondere der Arbeitgeber ist danach verpflichtet, die Arbeitsbedingungen im Betrieb positiv datenschutzfreundlich zu gestalten.[68]

Im Grundsatz wird man davon ausgehen müssen, dass das Direktionsrecht des Arbeitgebers und seine Befugnis zur Gestaltung der betrieblichen Abläufe auch die Einrichtung biometrischer Zugangskontrollen umfasst. Es bestehen jedoch Einschränkungen. In dem erwähnten Fall des BAG war beispielsweise der Kunde des Arbeitgebers offenbar bereit, den Zugang auch ohne biometrische Kontrolle zu eröffnen. Dann fehlt es bereits an der Erforderlichkeit des Einsatzes. In anderen Konstellationen kann allerdings eine mögliche Gefährdung der Kundenbeziehung zu berücksichtigen sein. Der Betriebsrat muss nach § 2 BetrVG bei der Ausübung seines Mitbestimmungsrechts die mögliche Beeinträchtigung betrieblicher Belange bedenken.

65 1 ABR 7/03, DuD 2004, 433 ff.

66 Vgl. etwa Hanau/Hoeren, Private Internetnutzung durch Arbeitnehmer, 2003, 52, 58; Däubler, Internet und Arbeitsrecht, 2001, Rn. 217; Raffler/Hellich, NZA 1997, 862; Post-Ortmann, RDV 1999, 106; Bijok/Class, RDV 2001, 54. Jedenfalls müssen die Zwecke konkret festgelegt werden und die Datenverwendung muss zu ihrer Erreichung tatsächlich erforderlich (im Sinne des Fehlens sinnvoller und zumutbarer Alternativen) sein.

67 Diese sind »Rechtsvorschriften« i. S. v. § 4 Abs. 1 BDSG, s. BAG, DB 1986, 2080, 2082.

68 Hanau/Kania, in: Dieterich/Hanau/Schaub (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 2001, § 75 BetrVG Rn. 9.

Kommt man zu dem Ergebnis, dass die Einrichtung eines biometrischen Systems (beispielsweise für den Zugang zu Hochsicherheitsbereichen) im Grundsatz erforderlich ist, so ist im zweiten Schritt nach der zulässigen Gestaltung zu fragen. Hierfür gibt es in der Rechtsprechung bislang keine Kriterien für biometrische Systeme im eigentlichen Sinne. Allerdings lassen sich Grundgedanken aus Entscheidungen zur Videoüberwachung übertragen, nach denen eine heimliche Kontrolle am Arbeitsplatz aufgrund der besonderen Situation (Abhängigkeitsverhältnis, täglicher Aufenthalt) grundsätzlich ebenso unzulässig ist wie eine lückenlose und dauerhafte Kontrolle.[69]
Im Übrigen sind die erläuterten Anforderungen des Datenschutzrechts hinsichtlich der Zweckbestimmung, der Definition von Löschungsregeln, der Merkmalsauswahl, der Vermeidung zentraler Datenbanken, des Einsatzes von Templates und templatefreien Verfahren und der Gewährleistung der Datensicherheit zu berücksichtigen (s. o. 4). Gerade im betrieblichen Bereich wird sich das Interesse des Arbeitgebers häufig auf die Prüfung der grundsätzlichen Zutrittsberechtigung beschränken. In diesem Fall dürfen nach dem Erforderlichkeitsprinzip keine Daten über individuelle Prüfvorgänge erhoben und weiterverwendet werden.[70]
Wenn ein Betriebsrat besteht, so sollte die Regelung des Einsatzes von Biometrie – da ohnehin Mitbestimmungsrechte bestehen – sinnvollerweise in einer Betriebsvereinbarung erfolgen.[71] Hierdurch wird für Arbeitgeber und Beschäftigte Rechtssicherheit und Transparenz geschaffen. Außerdem stärkt die kollektive Partizipation am Entscheidungsprozess die Akzeptanz der Biometrie im betrieblichen Alltag.

5.2. Hoheitliche Identifikationsdokumente

Nach den Anschlägen des 11. September 2001 hat eine Vielzahl von Staaten weltweit Programme zur Implementierung von Biometrie in Identitätspapieren gestartet.[72] Diese werden durch die Standardisierungsaktivitäten der International Civil Aviation Association (ICAO) und politischen Druck der USA begleitet, die ursprünglich von den Staaten des Visa-Waiver-Abkommens unter Androhung der Aufkündigung verlangt hatten, ab Oktober des Jahres 2004 Pässe mit biometrischen Daten auszugeben.[73] Die Frist ist mittlerweile bis zum 26. Oktober 2005 verlängert worden. In Deutschland besteht eine Regelung in den §§ 1 Abs. 4 PersAuswG, 4 Abs. 3 PassG und einer Reihe von ausländerrechtlichen Bestimmungen.[74] Die letzte Gruppe bleibt im Folgenden ausgeklammert.[75]

69 BAG DB 1988, 403; LAG BW, BB 1999, 1439; LAG Köln, BB 1997, 476. Bei überwiegenden schutzwürdigen Interessen des Arbeitgebers kann im Einzelfall auch eine heimliche Überwachung zulässig sein, wenn diese das einzig mögliche Mittel zur Rechtsverfolgung – beispielsweise bei einem konkreten Verdacht auf (erhebliche) Straftaten – ist.

70 Hierzu können z. B. die Templates von Mitarbeitern ohne Zuordnungsliste gespeichert und bei der Einlasskontrolle lediglich geprüft werden, ob das präsentierte Merkmal in der Datenbank enthalten ist, s. Gundermann/Köhntopp, DuD 1999, 143, 147. Zumindest zwischen den Matchingvorgängen besteht dann für die speichernde Stelle bei ausreichender Größe der Datenbank keine Möglichkeit der Herstellung eines Personenbezugs.

71 Hierbei könnten sich durch die Entwicklung von Musterbetriebsvereinbarungen wertvolle Hilfestellungen für kleine und mittlere Betriebe ergeben. Dazu gibt es derzeit Aktivitäten des Arbeitskreises Recht der AG 6 des Teletrust e. V. unter Leitung von Frau Astrid Albrecht (BSI).

72 S. zum Folgenden insbes. Roßnagel/Hornung, Kapitel Datenschutzrechtliche Anforderungen; Erfüllung der Anforderungen, in: Reichel/Roßnagel/Müller (Hrsg.), Der Digitale Personalausweis, 2004, i. E.

73 Vgl. Sec. 303 (c) Enhanced Border Security and Visa Entry Reform Act.

74 Das betrifft Aufenthaltsgenehmigung (§ 5 Abs. 4 AuslG), Ausweisersatz (§ 39 Abs. 1 AuslG), Bescheinigung über die Duldung (§ 56 a AuslG), Fiktionsbescheinigung (§ 69 Abs. 2 AuslG) und Asylbescheinigung (§ 63 Abs. 5 AsylVG). Alle Bestimmungen wurden durch das Gesetz zur Bekämpfung des internationalen Terrorismus vom 11. Januar 2002 (BGBl. I 2002, 361) eingeführt.

75 Diese weist eine Reihe von Besonderheiten auf. So kann z. B. eine zentrale Datenbank zur Vermeidung von Doppelbeantragungen im Visaverfahren – im Unterschied zu Personalausweis und Pass (s. u.) – er-

Nach aktueller Rechtslage »dürfen« Pass und Personalausweis künftig »neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht« des Inhabers enthalten. Lichtbild, Unterschrift, weitere biometrische Merkmale und alle übrigen Angaben zur Person dürfen auch in verschlüsselter Form eingebracht werden. Eine bundesweite Datenbank der biometrischen Daten wird untersagt. §§ 1 Abs. 5 Satz 1 PersAuswG, 4 Abs. 4 Satz 1 PassG bestimmen, dass »die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form ... sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung ... durch Bundesgesetz geregelt« werden. Nach §§ 3 Abs. 5 PersAuswG, 16 Abs. 6 PassG dürfen die verschlüsselten Merkmale und Angaben nur »zur Überprüfung der Echtheit des Dokuments und zur Identitätsprüfung ausgelesen und verwendet werden«. Außerdem besteht ein Auskunftsanspruch des Inhabers über den Inhalt der verschlüsselten Daten.

Diese Rechtslage ist in sich widersprüchlich: Ist zur Einführung biometrischer Merkmale noch ein weiteres Gesetz erforderlich, so dürfen Personalausweis und Pass diese Merkmale gegenwärtig gerade nicht enthalten. Wenn insoweit vertreten wird, die Regelungen enthielten eine Ermächtigungsgrundlage zur Einführung biometrischer Merkmale,[76] so ist dies bereits vor dem Hintergrund der gesetzgeberischen »Ankündigungen« in §§ 1 Abs. 5 Satz 1 PersAuswG, 4 Abs. 4 Satz 1 PassG klar unzutreffend. Noch kritikwürdiger sind Auffassungen, die in unzulässiger Weise verfassungsrechtliche Kategorien wie den Gesetzesvorbehalt mit einem Gesetz vermengen, das eine unvollständige, aus grundrechtlicher Sicht bedenklich unbestimmte und weitere gesetzgeberische Schritte ankündigende Bestimmung enthält.[77] Es wird etwa formuliert, aus den erwähnten Normen ergebe sich, dass die weiteren Einzelheiten durch Bundesgesetz geregelt werden müssten,[78] oder sogar, diese sähen »einen Gesetzesvorbehalt ... vor«.[79] Der Gesetzesvorbehalt ist jedoch ein verfassungsrechtlicher Grundsatz, der für die Einführung biometrischer Merkmale in hoheitlichen Identifikationsdokumenten unabhängig von einfachgesetzlichen Normen besteht.[80]

Im Ergebnis sind die Normen im Personalausweis- und Passgesetz ohne jede Rechtswirkung: Vor und nach ihrer Einführung ist eine Erweiterung um biometrische Daten unzulässig; die verfassungsrechtlich noch zu schaffende Ermächtigungsgrundlage wird das geltende Recht aufgrund der lex posterior-Regel ohnehin verdrängen. Die gegenwärtigen Regelungen erklären sich daraus, dass nach den Anschlägen des 11. September 2001 eine politische Mehrheit für eine Aufnahme biometrischer Daten

forderlich sein. Zu den Regelungen zum Einsatz von Biometrie bei Ausländern im Terrorismusbekämpfungsgesetz s. etwa Huber, NVwZ 2002, 787 ff.; Weichert, DuD 2002, 423 ff.; Golembiewski/Probst (Fn. 3), 39 ff., 45 ff.; TAB (Fn. 10), 106 ff.

76 So Stock, Biometrie und innere Sicherheit, in: DFK, Arbeitskreis Kriminalprävention und Biometrie. Workshop-Dokumentation vom 30. September 2002, 7; TeleTrusT (Fn. 8), 38. S. a. Petermann, TAB-Brief Nr. 24 (2003), 19, 21; TAB (Fn. 10), 4, 15 (die Einbringung der Daten könne »jetzt vorgenommen« werden) und TAB (Fn. 4), 3, 7, 47 (es sei »die Möglichkeit geschaffen worden ... biometrische Merkmale ... in Ausweispapiere ... aufzunehmen«).

77 Vgl. auch die Kritik bei Nolte, DVBl. 2002, 573, 576; Koch, Freiheitsbeschränkung in Raten? Biometrische Merkmale und das Terrorismusbekämpfungsgesetz, HSFK-Report 5/2002, 8 ff.

78 Albrecht (Fn. 4), 188; Golembiewski/Probst (Fn. 9), 49, 57. Ähnlich TAB (Fn. 10), 94 (»Festlegung auf das Erfordernis einer gesetzlichen Grundlage«).

79 TAB (Fn. 4), 7.

80 Lediglich dann, wenn unter verfassungsrechtlichen Gesichtspunkten die Einführung biometrischer Merkmale keine (oder keine über §§ 1 Abs. 4 PersAuswG, 4 Abs. 3 PassG hinausgehende) gesetzliche Grundlage benötigen würde, könnte das geltende Recht eine Art Sperrwirkung für die Exekutive entfalten, die man dann – allerdings terminologisch ungenau – als »Gesetzesvorbehalt« bezeichnen könnte. Da jedoch aus verfassungsrechtlicher Sicht eine weitaus genauere Regelung erforderlich ist, besteht für die Einführung der biometrischen Merkmale, unabhängig vom geltenden Recht, ein verfassungsrechtlicher Gesetzesvorbehalt.

in Ausweisdokumente vorhanden war, in der Eile der Zeit aber keine konkreten Umsetzungsentscheidungen treffen konnte oder wollte. Das rechtfertigt es aber nicht, politische Absichtserklärungen in Gesetzesform zu gießen.[81]

Jenseits der Anforderungen an die Ermächtigungsgrundlage bestehen für die verfassungsrechtliche Zulässigkeit der Einführung von Biometrie in Ausweispapiere eine Reihe von Besonderheiten.[82] Effektive Rückfallsysteme sind noch wichtiger als in anderen Applikationen, weil die Papiere auch für ältere, technisch nicht versierte oder behinderte Mitbürger nutzbar sein müssen. Aufgrund der Anwendung auf die gesamte Bevölkerung ist ein Merkmal zu wählen, welches nach Möglichkeit allgemein verwertbar ist. Das spricht für die Verwendung des Gesichtes. Es ist allerdings zweifelhaft, ob damit die sonstigen Probleme dieses Merkmals (relativ hohe Fehlerraten, Problem der intransparenten Erfassbarkeit) ausgeräumt werden können.

Nach geltendem Recht sind nicht nur zentrale Datenbanken, sondern jede Speicherung außerhalb der Dokumente unzulässig.[83] Fraglich ist, ob dies auch verfassungsrechtlich abgesichert ist. Zentrale und dezentrale Datenbanken sind für einzelne Kontrollvorgänge unter Verwendung von Pass oder Personalausweis weder geeignet noch erforderlich. Im Ausland werden zentrale biometrische Register mitunter zur Verhinderung der Vergabe von Mehrfachidentitäten eingesetzt. Hierfür gibt es in Deutschland wegen des hochentwickelten Meldewesens jedoch keine Notwendigkeit. Bei einer Erweiterung der Pass- und Personalausweisregister um biometrische Daten könnte im Fall einer Neubeantragung auf diese Informationen zugegriffen werden. Hierzu bietet sich aber als milderes Mittel die Neuerhebung an. Diese ist schon aus Gründen der Merkmalsveränderung über die Zeit und wegen der zu erwartenden technischen Veränderungen der Verfahren erforderlich.

Schließlich kommt ein Einsatz zur Verbrechensbekämpfung in Frage. Denkbar wäre etwa der Abgleich von Fingerabdruckspuren oder Videoaufnahmen eines unbekannten Täters mit der Gesamtdatenbank zum Zweck der Aufklärung einer schweren Straftat. Umgekehrt könnte bei der Fahndung nach einer namentlich bekannten Person das biometrische Datum von der Registerbehörde an die Polizei übermittelt und dann in den Fahndungsbestand eingespeist werden. Ein solches Vorgehen wäre zur Aufklärung einer gewissen Zahl von Straftaten geeignet und erforderlich; fraglich ist jedoch die objektive Zumutbarkeit. Einerseits würden in einer Zahl von Kriminalfällen zusätzliche Fahndungserfolge erzielt. Diesem Vorteil steht jedoch der Nachteil der Einrichtung einer zentralen Datenbank gegenüber, die von jedem Bürger Zeit seines Lebens ein unveränderbares und zur allgemeinen Überwachung geeignetes Kennzeichen vorhalten würde. Dies ist deshalb unzumutbar, weil nur eine kleine Zahl von Bürgern straffällig wird. Die Möglichkeit zusätzlicher Fahndungserfolge rechtfertigt nicht, die konkrete Gefahr der Verwendung biometrischer Merkmale als allgemeines Personenkennzeichen in Kauf zu nehmen.[84] Im Ergebnis ist die Speicherung biometrischer Daten außerhalb der Identifikationsdokumente (mit Ausnahme kurzzeitiger Verarbeitungsschritte bei Herstellung und Ausweisprüfung, auf die eine unmittelbare Löschung zu folgen hat) unzulässig.

81 Zur Kritik am überschnellen Gesetzgebungsverfahren auch Koch (Fn. 77), 33; Schaar, MMR 2001, 713 f.

82 S. ausführlich Roßnagel/Hornung (Fn. 72); Hornung, Biometric Identity Cards, in: Paulus/Pohlmann/Reimer, Securing Electronic Business Processes, 2004, 47 ff.; Golembiewski/Probst (Fn. 3).

83 Das folgt für bundesweite Dateien aus §§ 1 Abs. 5 Satz 2 PersAuswG 4 Abs. 4 Satz 2 PassG, für Personalausweis- und Passregister aus dem abschließenden Charakter von §§ 2 a PersAuswG, 21 PassG, für übrige Register aus §§ 3 Abs. 2 PersAuswG, 16 Abs. 2 PassG.

84 S. Roßnagel/Hornung (Fn. 72); Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DuD 2002, 247, unter 4 und 5. Nicht umsonst hat das BVerfG für den Aufbau einer begrenzten Gendatenbank Vorbestrafter hohe Anforderungen formuliert (BVerfGE 103, 21 ff., hierzu Faber, RDV 2003, 278, 280 ff.). Für die hier in Rede stehende Datenbank müssen noch höhere Anforderungen gestellt werden, weil die

Einige der allgemein formulierten datenschutzrechtlichen Anforderungen stoßen aufgrund des weltweiten Einsatzes von Reisedokumenten auf große Schwierigkeiten. Für eine Vielzahl von Merkmalen ist die internationale Standardisierung der Templatestrukturen noch nicht abgeschlossen, und insbesondere bei der Gesichtserkennung erscheint dies in absehbarer Zeit auch nicht realistisch. Da die einzelnen Staaten nicht für die Dokumente jedes anderen Staates verschiedene Prüfgeräte oder -algorithmen vorhalten können, tendiert die ICAO zur Verwendung von Volldatensätzen. Da dies jedoch eingriffsintensiver ist, ist zumindest ein verstärktes staatliches Engagement in der Template-Standardisierung zu fordern. Immer dann, wenn für das verwendete Merkmal Template-Standards verfügbar sind, müssen diese verwendet werden.

Zur Absicherung der Daten kommen im Normalfall Verschlüsselung und elektronische Signatur in Frage. Mit der elektronischen Signatur wird zwar nicht die Vertraulichkeit, wohl aber die Integrität der Daten gesichert. Ihr Einsatz setzt jedoch ein weltweites, interoperables Schlüssel- und Zertifikatsmanagement voraus, welches bisher nicht existiert.[85] Die Verschlüsselung – die in kleinen Anwendungen unbedingt zu fordern ist – wird in ihrer Wirksamkeit gemindert, weil es unrealistisch ist, die verwendeten Schlüssel dauerhaft geheimzuhalten, wenn sie weltweit verteilt und an einer Vielzahl von Kontrollstellen vorgehalten werden müssen. Allerdings ergibt sich zumindest ein Schutz gegen alltägliche Angriffe (insbesondere durch Privatleute). Dieser ist umso wichtiger, als die ICAO kontaktlose (RF-)Schnittstellen empfiehlt, die ohne entsprechende technische Absicherungen für den Betroffenen unmerklich angesteuert werden können.

Kontrovers diskutiert wird derzeit der Einsatz der biometrischen Daten auf Identifikationsdokumenten im privaten Bereich, der beispielsweise im betrieblichen Umfeld denkbar wäre. Personalausweis und Pass können nach §§ 4 PersAuswG, 18 PassG auch im nichtöffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden, jedoch ist eine Verwendung zum automatischen Abruf und zur automatischen Speicherung personenbezogener Daten unzulässig.[86] Von Ausnahmen abgesehen, ist deshalb de lege lata der Gebrauch biometrischer Daten nicht möglich.[87] Eine Änderung dieser Regelung wäre verfassungsrechtlich akzeptabel, wenn die Freiwilligkeit der Anwendung gesichert wird und eine gegenseitige Authentisierung mit einem Lesegerät erfolgt, welches zuvor zertifiziert wurde. In diesem Fall kann der Ausweisinhaber sichergehen, dass seine Daten nicht über das zum Matching erforderliche Maß hinaus gespeichert oder gar weitergegeben werden. Ein strafbewehrtes Verbot könnte außerdem dem Missbrauch der Daten entgegenwirken. Aus staatlicher Sicht stellt der Zugriff Privater auf die elektronisch gespeicherten Daten kein Problem dar, wenn deren Integrität – beispielsweise durch eine elektronische Signatur – sichergestellt wird.

gesamte Bevölkerung betroffen wäre und im Unterschied zu einer Datenbank Vorbestrafter die übergroße Mehrheit der Betroffenen keinen Anlass für die Datenspeicherung gegeben hätte.

85 Ein Vorschlag hierzu wurde von der ICAO unterbreitet, vgl. PKI Digital Signatures for Machine Readable Travel Documents. Technical Report, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm, 2003.

86 S. näher Medert/Süßmuth, Personalausweisrecht des Bundes und der Länder, 3. Auflage 1998, § 4 Rn. 1 ff.

87 Auch nach geltendem Recht wäre der Einsatz eines hoheitlichen Identifikationsdokuments wohl rechtmäßig, das über einen Sensor verfügt und die Daten auf der Karte abgleicht. Das ist zwar auch eine automatische Speicherung von Daten, wird aber nicht vom Normzweck des Verbots erfasst, weil die Datenverarbeitung unter ausschließlicher Kontrolle des Inhabers abläuft. Da der Einsatz dieser Art biometrischer Systeme aufgrund von Sicherheitsbedenken für staatliche Dokumente unwahrscheinlich ist, wird diese Ausnahme aber nicht relevant werden.

Im Bereich des elektronischen Rechtsverkehrs findet sich in § 15 Abs. 1 Satz 1, 3 SigV eine ausdrückliche Regelung für biometrische Verfahren. Diese können anstelle der bislang üblichen PIN zur Aktivierung von Signaturkarten und damit zur Abgabe rechtsverbindlicher und beweiskräftiger elektronischer Willenserklärungen eingesetzt werden.[88] Voraussetzung ist allerdings, dass sie eine »dem wissensbasierten Verfahren gleichwertige Sicherheit« bieten.

Perspektivisch ist der Einsatz von Biometrie im Rechtsverkehr unter dem Gesichtspunkt der Rechtssicherheit zu begrüßen, weil die Authentizität abgegebener Erklärungen gestärkt wird: Durch die unmittelbare Bindung der Merkmale an die Person des Signaturschlüssel-Inhabers ist eine Verwendung der Karte durch Dritte (beispielsweise nach dem Ausspähen oder der freiwilligen Weitergabe der PIN) nicht möglich.[89] Allerdings gibt es bislang kein biometrisches Verfahren, dem eine »gleichwertige Sicherheit« attestiert worden ist, und es ist zweifelhaft, ob dies in näherer Zukunft der Fall sein wird.[90]

6. Notwendigkeit gesetzlicher Regelungen?

Derzeit existiert kein allgemeiner gesetzlicher Rahmen für den Einsatz von Biometrie. Im hoheitlichen Bereich ist dieser grundsätzlich auch entbehrlich, weil aufgrund der Anforderungen des Gesetzesvorbehalts und der Wesentlichkeitslehre[91] präzise Einzelfallregelungen durch den parlamentarischen Gesetzgeber erforderlich sind. Dieser hat entsprechende Entscheidungen im geltenden Pass- und Personalausweisrecht »angekündigt«, im Ausländerrecht allerdings auf eine Rechtsverordnung des Bundesministers des Innern übertragen. Da hinsichtlich des Schutzes des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Recht auf informationelle Selbstbestimmung kein Unterschied zwischen Deutschen und Ausländern besteht,[92] ist diese Regelung wegen Verstoßes gegen den Gesetzesvorbehalt verfassungswidrig.[93]

Im Bereich des elektronischen Rechtsverkehrs beugt die Regelung in der Signaturverordnung einer ungerechtfertigten Technikgläubigkeit durch die Gerichte vor, indem sie den Einsatz von Biometrie nur nach Durchlaufen eines Prüf- und Bestätigungsverfahrens zulässt. Dies reduziert die Haftungsrisiken für die Anwender. Außerhalb des Signaturverfahrens erscheint die Anwendung der freien Beweiswürdigung dagegen angemessen, weil sie den Gerichten Flexibilität gibt, die gerade bei der rechtlichen

88 S. zur elektronischen Signatur Roßnagel, in: ders., Recht der Multimedia-Dienste. Kommentar zum IuKDG und zum MDStV, Einl. SigG m. w. N. Rechtlich gesehen ist die (qualifizierte) Signatur ein Äquivalent zur eigenhändigen Unterschrift. Sie ersetzt gemäß (von Ausnahmen abgesehen) die Schriftform und ist regelmäßig prozessual beweiskräftig. S. etwa für den Bereich des Zivilrechts §§ 126 Abs. 3, 126 a BGB, 292 a ZPO.

89 Vgl. ausführlich Albrecht (Fn. 4), 64 ff., 104 ff.

90 Problematisch ist insbesondere, dass Signaturkarten in sehr unterschiedlichen Umgebungen einsetzbar sein müssen, von denen einige (insbesondere der heimische PC-Arbeitsplatz) nur schwer gegen Angriffe abzusichern sind. Solange dies nicht gewährleistet ist, ist aber zumindest eine Kombination von PIN und Biometrie ein gangbarer Weg.

91 BVerfGE 61, 260 (275); 88, 103 (116). Im Bereich der Biometrie müssen hier die genaue Art der Daten, ihre Speicherungsform (Volldatensatz oder Templates), ihr Speicherungsort (auf einem Identifikationsdokument; ob und wenn ja wo und in welcher Form in staatlichen Dateien), die weitere Verwendung im Rahmen von Kontrollen und eventuelle Zugriffsrechte in einem Parlamentsgesetz geregelt werden.

92 Vgl. Kunig, in: von Münch/Kunig, Grundgesetz-Kommentar, 5. Auflage 2000, Art. 2 Rn. 39.

93 Ebenso Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Positionspapier zum Antiterrorgesetz der Bundesregierung (abrufbar unter http://www.datenschutzzentrum.de/material/themen/divers/anti terr.pdf), 2001, 22; Golembiewski/Probst (Fn. 3), 47 f. S. a. die Nachweise in Fn. 75.

Beurteilung einer neuen Technologie zur Findung sachgerechter Lösungen unabdingbar ist.[94]

Die Analyse hat gezeigt (s. o. 4.), dass sich allgemeine datenschutzrechtliche Grundsätze in Anforderungen an die Gestaltung biometrischer Systeme konkretisieren lassen. Insofern erscheint eine allgemeine Regelung zur Biometrie nicht unbedingt erforderlich. Sie könnte allerdings Transparenz für die Betroffenen schaffen und überdies die unbefriedigende Situation beseitigen, dass §§ 6 b, 6 c BDSG auf einige biometrische Systeme anwendbar sind, auf andere jedoch nicht.[95] Eine vergleichbare Transparenzregel für die Einrichtung biometrischer Systeme würde für einheitliche Unterrichtungspflichten der verantwortlichen Stelle sorgen. Sie könnte sich an § 6 c BDSG orientieren, also eine Unterrichtung über die Identität und Anschrift der zuständigen Stelle, die genaue Funktionsweise des Systems und die Ausübung von Betroffenenrechten beinhalten sowie normieren, dass die Datenerhebung und Weiterverarbeitung (insbesondere das Matching) für den Betroffenen eindeutig erkennbar sein müssen. Mit einer derartigen Grundsatznorm würde nicht nur das Recht der Betroffenen auf informationelle Selbstbestimmung gestärkt, sondern auch die Akzeptanz der Biometrie.

7. Ausblick

Biometrische Verfahren befinden sich derzeit in parallelen Prozessen der technischen Weiterentwicklung und der ersten Implementierung in Massenverfahren. Vor diesem Hintergrund ist eine verstärkte Beobachtung der Entwicklung dieser Technologie erforderlich, um im Rahmen von Technikfolgenabschätzungsprozessen ihre Auswirkungen auf Individuum und Gesellschaft erfassen zu können. So bietet sich die Chance, auf eine datenschutzfreundliche Gestaltung der Systeme und Verfahren hinzuwirken. Da dies deren Akzeptanz entscheidend befördern könnte, ist eine entsprechende Gestaltung auch im Interesse von Entwicklern und Anbietern. Insofern eröffnet sich die Möglichkeit eines produktiven Diskurses mit Datenschutzexperten, Verbraucherschutz- und anderen Interessengruppen.

94 Albrecht (Fn. 4), 147.

95 S. o. 4. Insbesondere die nur teilweise Anwendbarkeit von § 6 c BDSG ist wenig sinnvoll. Für den Nutzer macht es unter Datenschutzgesichtspunkten etwa wenig Unterschied, ob das Matching auf der Karte oder in der Peripherie abläuft. In beiden Fällen werden (im Unterschied zum Sensor auf der Karte) in der Peripherie biometrische Rohdaten erhoben, die entsprechende Missbrauchsmöglichkeiten mit sich bringen.