Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen

Stand Juli 2003

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
Dr. Claudia Golembiewski, Dr. Thomas Probst

Inhaltsverzeichnis

Zusammenfassung

Der Gesetzgeber hat mit dem zum 1. Januar 2002 in Kraft getretenen Terrorismusbekämpfungsgesetz Regelungen geschaffen, die die Aufnahme biometrischer Merkmale in Pässe und Personalausweise von Bundesbürgern sowie in „Ausländerausweise“ ermöglichen. Die nähere Ausgestaltung der Regelungen wird für den Bereich des Pass- und Personalausweiswesens einem Ausführungsgesetz überlassen. Im Bereich des Ausländer- und Asylrechts bleibt die Konkretisierung der inhaltlichen Vorgaben einer Rechtsverordnung im Sinne des Art. 80 Abs. 1 Satz 2 Grundgesetz überlassen. Das vorliegende Gutachten untersucht die aus einer Aufnahme biometrischer Merkmale in die entsprechenden Identifikationspapiere resultierenden verfassungs- und europarechtlichen Fragestellungen und definiert datenschutzrechtliche Anforderungen, die an die Umsetzung der gesetzlichen Vorgaben zu stellen sind.

Nach einer Einführung in die Problemstellung werden im zweiten Kapitel die mit dem Einsatz biometrischer Verfahren verbundenen rechtlichen Aspekte untersucht. Da biometrische Daten als personenbezogene Daten einzuordnen sind, die den datenschutzrechtlichen Vorschriften unterliegen, werden die aus dem Personenbezug biometrischer Daten folgenden datenschutzrechtlichen Konsequenzen beleuchtet. In diesem Zusammenhang werden die an Einschränkungen des Rechts auf informationelle Selbstbestimmung zu stellenden Anforderungen in Bezug auf biometrische Verfahren konkretisiert. So bedarf die Erhebung, Verarbeitung und Speicherung biometrischer Daten einer verfassungsgemäßen gesetzlichen Grundlage, die dem Zweckbindungsgrundsatz genügt. Eine Speicherung biometrischer Merkmale auf Vorrat zu unbestimmten Zwecken ist unzulässig. Des Weiteren hat der Gesetzgeber bei der Schaffung der Ausführungsvorschriften den Grundsatz der Datenvermeidung und Datensparsamkeit zu berücksichtigen und sich insoweit bei der Realisierung der Vorgaben des Terrorismusbekämpfungsgesetzes an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Biometrische Merkmale dürfen auch nicht verwendet werden, um Persönlichkeitsprofile über die Betroffenen zu bilden.

Auf europäischer Ebene existieren ebenfalls Vorgaben. Allerdings lassen sich diesen keine spezifischen Anforderungen für den nationalen Gesetzgeber entnehmen, die bei der Ausgestaltung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise bzw. „Ausländerausweise“ zu erfüllen wären. Europarechtliche Vorschriften verpflichten den Gesetzge

ber insbesondere nicht zur Aufnahme biometrischer Merkmale in entsprechende Dokumente, noch regeln sie die dabei gegebenenfalls zu beachtenden Einzelheiten.
Im dritten Kapitel wird der Regelungsinhalt der mit dem Terrorismusbekämpfungsgesetz geschaffenen Vorschriften zur Aufnahme biometrischer Merkmale dargestellt.

Im vierten Kapitel werden anhand der Regelungen über die Aufnahme biometrischer Merkmale von Bundesbürgern und Ausländern die Defizite der Vorschriften erörtert. So wird die vom Gesetzgeber vorgenommene Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ in Frage gestellt, da diese sich unter dem Aspekt der Falscherkennung bzw. Falschakzeptanz biometrischer Systeme als nicht unproblematisch erweist. An die Leistungsfähigkeit biometrischer Systeme sind hohe Anforderungen zu stellen. Diese müssen insbesondere für den Masseneinsatz geeignet sein. Bei der Auswahl der biometrischen Merkmale ist zu berücksichtigen, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen über den Merkmalsträger anfallen können. Die Speicherung von Templates ist daher gegenüber der Speicherung von Rohdaten vorzugswürdig. Die Minimierung der Nebenwirkungen für den Betroffenen ist aus Gründen der Verhältnismäßigkeit notwendig.

Während dem im Datenschutzrecht geltenden strengen Zweckbindungsgrundsatz hinsichtlich der Zwecke der Verwendung der biometrischen Merkmale von Bundesbürgern Rechnung getragen ist, erweisen sich die für Ausländer geltenden Vorschriften als nicht vereinbar mit diesem Grundsatz.

Unter dem Gesichtspunkt der Erforderlichkeit sowie der Datenvermeidung und Datensparsamkeit ist eine Speicherung der biometrischen Daten ausschließlich in der Verfügungsgewalt der Betroffenen ausreichend zur Zweckerreichung und damit geboten.

1 Einleitung

Während biometrische Verfahren in der Vergangenheit eher mit Spionage- und Science-Fiction-Filmen in Verbindung gebracht oder allenfalls im Zusammenhang mit dem Zutritt zu Hochsicherheitsbereichen genannt wurden und Detailkenntnisse über die Funktionsweise derartiger Verfahren ausschließlich Experten vorbehalten waren, nehmen die Meldungen über biometrische Systeme in der Medienberichterstattung mittlerweile einen festen Anteil ein. So wird über die Möglichkeiten des Einsatzes biometrischer Verfahren in den unterschiedlichsten Lebensbereichen berichtet. Sie sollen es ermöglichen, dass der Einzelne anhand seiner charakteristischen Körpermerkmale von einem biometrischen System erkannt wird. Zu denken ist in diesem Zusammenhang beispielsweise an - teilweise euphorische - Berichte über biometrische Erkennungssysteme, die die Authentifizierung gegenüber Computersystemen vornehmen können, Bezahlsysteme auf der Grundlage biometrischer Merkmale, die in Zukunft Kreditkarten überflüssig machen oder aber biometrische Systeme, die die Eingabe der Geheimzahl an Geldautomaten ersetzen sollen.

Das Verhältnis von Datenschützern zur Biometrie ist als ambivalent einzustufen. Während zum einen die Möglichkeit, die Identifizierung jedes Einzelnen mithilfe biometrischer Systeme zu jeder Zeit vorzunehmen, eine eher unbehagliche Vorstellung hervorruft, so erscheint es doch auf der anderen Seite unter Aspekten der Datensicherheit als verlockend, sich mithilfe der Biometrie gegenüber Computersystemen authentifizieren zu können, ohne sich Passwörter, PINs etc. merken und immer darauf achten zu müssen, diese stets geheim zu halten.

Neben den genannten Einsatzszenarien ist die Biometrie im Zusammenhang mit den Anschlägen vom 11. September 2001 und der sich daran anschließenden Debatte über Terrorismusbekämpfung in den Blickpunkt des öffentlichen Interesses gerückt. Biometrische Erfassungssysteme werden in diesem Zusammenhang als besonders viel versprechend für eine effektive Terrorismusbekämpfung angesehen. Mit dem zum 1. Januar 2002 in Kraft getretenen Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) wurden konkrete gesetzliche Grundlagen geschaffen, die die Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie in Ausweisdokumente für Ausländer erlauben. Die Umsetzung dieser Vorschriften bedarf allerdings im Bereich des Pass- und Personalausweiswesens für Bundesbürger noch eines Ausführungsgesetzes, das die Modalitäten der Aufnahme biometrischer Merkmale zu regeln hat. Im Unterschied hierzu hat der Gesetzgeber hinsichtlich

der Aufnahme biometrischer Merkmale in Ausweisdokumente für Ausländer eine Rechtsverordnung für ausreichend erachtet. Eine solche Rechtsverordnung ist noch nicht erlassen.

Die Modalitäten der Umsetzung der Vorschriften des Terrorismusbekämpfungsgesetzes und insbesondere die an die Regelungen zu stellenden datenschutzrechtlichen Anforderungen bilden den Schwerpunkt der vorliegenden Darstellung.

2 Grundsätzliches

Im Folgenden soll zunächst ein Überblick über den gegenwärtigen Einsatz biometrischer Verfahren gegeben werden. Um die datenschutzrechtliche Relevanz biometrischer Systeme beurteilen zu können, wird des Weiteren kurz die grundsätzliche technische Funktionsweise biometrischer Verfahren beschrieben. Schließlich werden die mit dem Einsatz biometrischer Verfahren verbundenen verfassungs-, datenschutz- und europarechtlichen Fragen erörtert.

2.1 Überblick über den Stand des Einsatzes biometrischer Verfahren

Der Begriff *Biometrie* stammt aus dem Griechischen und leitet sich aus den griechischen Worten *bios* (= Leben) und *metrein* (= messen) her. Er wird im Zusammenhang mit der zahlenmäßigen Beschreibung und Vermessung im Bereich der Biologie, insbesondere der medizinischen Statistik, verwendet. Erst seit kürzerer Zeit wird er häufiger mit der automatischen Vermessung des menschlichen Körpers und einer damit möglichen automatisierten (Wieder-) Erkennung in Verbindung gebracht.[1]

2.1.1 Wo kommen biometrische Verfahren bereits zum Einsatz?

Biometrische Verfahren kommen in den unterschiedlichsten Bereichen zum Einsatz. Zum einen handelt es sich um Zutritts- bzw. Zugangskontrollsysteme, zum anderen handelt es sich um biometrische Verfahren, die zum Zwecke der Identifizierung oder der Verifizierung eingesetzt werden. Die Zutrittssicherung stellt mittlerweile eine klassische Anwendung biometrischer Systeme dar. Sie kommt beispielsweise in Rechenzentren, (militärischen) Hochsicherheits- oder in Kontrollbereichen im Kernenergiesektor zum Einsatz. Bei der Zugangssiche

[1] *Probst*, Biometrie, in: *Bäumler/Breinlinger*/*Schrader* (Hrsg.), Datenschutz von A-Z, Ziff. B 1100.

rung wird eine Authentisierung mithilfe biometrischer Daten, entweder allein oder in Kombination mit einem Passwort, gegenüber einem Computersystem vorgenommen. Daneben kommen als Einzelanwendungen biometrische Verfahren auch im „Convenience-Bereich" zum Einsatz (z.B. PIN-Ersatz am Mobiltelefon oder Kindersicherung am Videorekorder).[2]

Im Zoo von Hannover wird seit April 2003 eine neue Gesichtserkennungsanlage eingesetzt, die dem Zweck dient, den Missbrauch der ca. 60.000 Dauerkarten zu verhindern. Die bereits im Mai 2001 installierten optischen CMOS-Fingerabdruck-Scanner, die mit der EDV und dem Kassensystem verknüpft waren, erwiesen sich bald als Fehlinvestition. Insbesondere bei ungünstigen Witterungsverhältnissen im Winter verweigerten die Scanner häufig den Dienst, weil es nicht gelang, ein brauchbares Fingerlinien-Abbild zu erzeugen, aus dem sich die benötigten Templates extrahieren und für den Abgleich mit den Referenzdatensätzen heranziehen ließen. Bei Kindern, die insgesamt ca. die Hälfte der Zoobesucher ausmachen, scheiterten die Geräte häufig bereits beim Erfassen des Referenzdatensatzes, dem sog. Enrollment. Nach nur knapp zwei Jahren wurde deswegen im Zoo von Hannover auf den Einsatz dieser Technik wieder verzichtet. Die seit kurzem im Einsatz befindliche Gesichtserkennungsanlage, die sog. ZN-Face-Engine, ein NT-Server mit MS-SQL-Datenbanksystem, in der die Protokolle sämtlicher Enrollment- und Authentifizierungsvorgänge verarbeitet und gespeichert werden, wird als sehr viel versprechend angesehen.[3] Es handelt sich bei der eingesetzten Technik nach Herstellerangaben um das „weltweit meistverkaufte Zutrittskontrollsystem auf der Basis von Gesichtserkennung".[4] Ob sich die Investition von geschätzten 120 000 Euro allerdings auch tatsächlich gelohnt hat, werden die nächsten Monate zeigen, wenn das System täglich zehntausend Besucher bewältigen muss.[5]

Gerade nach den Anschlägen vom 11. September 2001 wird im Zusammenhang mit den Maßnahmen zur Terrorismusbekämpfung biometrischen Systemen, die der Identifikation bzw. Verifikation dienen, besondere Aufmerksamkeit geschenkt. Als Beispiel für ein bereits bestehendes biometrisches Verfahren zur Identifizierung lässt sich das vom Bundeskriminalamt betriebene System AFIS (automatisiertes Fingerabdruck-Identifizierungssystem) anführen, das in einer Datenbank daktyloskopische Angaben aus Straf- und Asylverfahren enthält.

---

2 *Probst*, Biometrie, in: *Bäumler/Breinlinger/Schrader* (Hrsg.), Datenschutz von A-Z, Ziff. B 1100.; siehe ausführlich auch *Petermann/Sauter*, Biometrische Identifikationssysteme, S. 61ff.

3 Eine ausführliche Beschreibung der Technik bei *Ziegler*, c't 2003, S. 26ff.

4 Meldung bei Heise Online vom 14.04.2003 (abrufbar unter http://www.heise.de/newsticker/data/pmz-13.04.03-000/).

5 *Ziegler*, c't 2003, 26 (28).

Das System befindet sich seit 1992 im Einsatz und ermöglicht eine digitalisierte Speicherung und Recherche von Fingerabdrücken. Zur Identifizierung von Straftätern werden die am Tatort aufgefundenen Fingerabdruckspuren, die in der Datei gespeichert werden, mit den auf Grund erkennungsdienstlicher Behandlungen erhobenen und zur vorbeugenden Straftatbekämpfung gespeicherten Fingerabdrücken verglichen.[6] In dem System AFIS sind Personendatenbestände mit Angaben zu allen zehn Fingern gespeichert. Des Weiteren ist ein Spurendatenbestand mit nicht persönlich zugeordneten Fingerabdrücken enthalten.[7] AFIS wird nicht nur für polizeiliche, sondern auch für ausländerrechtliche Zwecke genutzt. Seit dem Jahre 1993 schreibt § 16 Asylverfahrensgesetz (AsylVfG) vor, dass Asylbewerber, die keine unbefristete Aufenthaltsgenehmigung besitzen und das 14. Lebensjahr vollendet haben, sich erkennungsdienstlich behandeln lassen müssen. Die Vorschrift dient dem Zweck, die mehrfache Antragstellung unter unterschiedlichen Identitäten zu verhindern. Während § 41 Ausländergesetz (AuslG) die erkennungsdienstliche Behandlung von Ausländern nur dann zulässt, wenn Zweifel an der Identität des Ausländers bestehen, gilt dies weder für Asylsuchende noch für Kriegs- und Bürgerkriegsflüchtlinge, die mit Einfügung des § 41a Ausländergesetz (AuslG) im Jahre 1997 den Asylsuchenden gleichgestellt wurden. Die Vorschrift dient insoweit nicht dem Zweck, die zum Erfassungszeitpunkt zweifelhafte Identität eines Ausländers für eine konkrete Entscheidung festzustellen, sondern vielmehr der vorbeugenden Sammlung von Daten, um die Identität des Ausländers bei einer zukünftigen Entscheidung feststellen zu können.[8] Der Kreis der Normunterworfenen wird damit gegenüber anderen Ausländern deutlich schlechter gestellt, weil bei diesen eine erkennungsdienstliche Behandlung nur dann in Betracht kommt, wenn Zweifel an der Identität bestehen. Diese flächendeckende Erfassung bestimmter Personengruppen wirft im Hinblick auf das grundrechtlich garantierte Recht auf informationelle Selbstbestimmung der Betroffenen erhebliche Bedenken auf.

Mit dem Namen EURODAC wurde auf europäischer Ebene ebenfalls eine AFIS-Datei eingerichtet. Nach In-Kraft-Treten der EURODAC-Verordnung am 11. Dezember 2000[9] befindet sich diese gemeinsame Datei seit Januar 2003 europaweit im Einsatz. Bis zum nächsten Jahr

---

6 Vgl. hierzu und zur Funktionsweise der Auswertung von Fingerabdrücken in AFIS *Werner*, in: *Bäumler/Breinlinger/Schrader* (Hrsg.), Datenschutz von A-Z, Ziff. A600.

7 *Weichert*, DuD 1999, 167 (167).

8 GK-AuslR, § 41a Rn.2.

9 Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens (ABl. EG L316 v. 15.12.2000) sowie Verordnung (EG) Nr. 407/2002 des Rates vom 28. Februar 2002 zur Festlegung von Durchführungsbestimmungen zur Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkomens (ABl. EG L 62/1 vom 5.3.2002).

soll das System ca. zwei Millionen Antragsteller verwalten, etwa 500 000 Datenvergleiche pro Sekunde ermöglichen und mit einer Genauigkeit von 99,9% arbeiten.[10] Standort der Datenbank ist Luxemburg. In dieser Datenbank werden die biometrischen Daten von Erwachsenen und Kindern, die das 14. Lebensjahr erreicht haben, gespeichert. EURODAC soll klären, wann und in welchem Land Asylbewerber zum ersten Mal eingereist sind. Mithilfe von EURODAC soll verhindert werden, dass Asylbewerber Doppelanträge in mehreren Ländern stellen. Die Europäische Kommission schätzt, dass Doppelanträge ein Fünftel der jährlich ungefähr 400 000 Asylfälle ausmachen. Wird von EURODAC festgestellt, dass ein Asylbewerber bereits einen Asylantrag in einem anderen EU-Staat gestellt hat, so wird er in das Land zurückgeschickt, das die Registrierung vorgenommen hat, so genannter Herkunftsmitgliedsstaat.[11]

Der Umgang mit den im Rahmen von EURODAC verarbeiteten Daten lässt sich der EURODAC-Verordnung entnehmen. Eine Regelung über die Datenspeicherung enthält Art. 5 der EURODAC-Verordnung. Nach Art. 5 Abs. 1 werden in der zentralen Datenbank folgende Daten gespeichert: Herkunftsmitgliedsstaat, Ort und Zeitpunkt der Stellung des Asylantrags (a); Fingerabdruckdaten (b); Geschlecht (c); vom Herkunftsmitgliedsstaat verwendete Kennnummer (d); Zeitpunkt der Abnahme der Fingerabdrücke (e); Zeitpunkt der Übermittlung an die Zentraleinheit (f); Zeitpunkt der Eingabe der Daten in die zentrale Datenbank (g); Angaben zu dem/den Empfänger(n), an den/die die Daten übermittelt wurden, sowie Zeitpunkt(e) der Übermittlungen(en). Da in der europäischen Datenbank lediglich eine Speicherung der Muster der Rillen auf den Fingern der Immigranten vorgenommen werde, der Name sowie die Herkunft dagegen anonym bleibe, sei der Datenschutz nach Aussage des EU-Kommissars *Antonio Vitorino* gesichert.[12]

2.1.2 Welche Arten von Daten werden verarbeitet?

Biometrische Verfahren werten entweder physiologische oder verhaltenstypische Merkmale einer Person aus. Verschiedene Merkmale haben sich als gut geeignet für die biometrische Überprüfung erwiesen. Hierzu gehören z.B. Gesicht, Retina, Finger, Handgeometrie, Venen

---

[10] *Ohne Verfasser,* Computerwoche 4/2003, S. 33.

[11] Zur Inbetriebnahme von EURODAC: Meldung bei Heise Online vom 15.01.2003 (abrufbar unter http://www.heise.de/newsticker/data/anw-15.01.03-002/); DANA 1/2003, S. 23f.

[12] Eurodac, Aktuelles Lexikon, SZ vom 16.01.2003, S. 2.

muster auf dem Handrücken, Körpergeruch, Ohr, DNA, Unterschrift, Sitzverhalten, Gang, Tippverhalten an der Tastatur sowie Stimme und Sprechverhalten.[13]

Das Grundprinzip einer biometrischen (Wieder-) Erkennung ist stets gleich: Zunächst wird mithilfe von Sensoren (z.B. Kameras, Mikrofonen, Tastaturen, aber auch Spezialsensoren zur Aufnahme von Gerüchen oder Fingerabdrücken) ein Referenzmuster elektronisch erfasst und gespeichert – die Person wird in das System „eingelernt" (auch „Enrollment"). Dies kann auch ohne Kenntnis der Person geschehen, etwa bei der Aufnahme von latenten Fingerabdrücken oder Gesichtsaufnahmen von Fotos, Phantombildern oder Videoaufnahmen in das System. Für die Wiedererkennung einer Person werden erneut biometrische Merkmale erfasst und mit den bereits gespeicherten Referenzdaten verglichen. Im Falle einer Übereinstimmung ist die Erkennung erfolgreich.

Üblicherweise werden die aufgenommenen *Rohdaten* (z.B. Tonaufnahmen, Videoaufnahmen), die eine mehr oder weniger direkte Erkennung durch Menschen zulassen, zu einem *Template* weiterverarbeitet. Dies ist ein relativ kleiner Datensatz, der Parameter eines mathematischen Modells der Rohdaten enthält, beispielsweise Koordinaten von sog. *Minutien* (u.a. Verzweigungen oder Enden von Fingerabdrucklinien).[14] Er enthält (in komprimierter Form) die für einen Vergleich notwendigen Daten, erlaubt aber üblicherweise keine unmittelbaren Rückschlüsse auf die beschriebene Person. Ein solches Template wird beim Einlernen gespeichert. Bei allen weiteren Benutzungen des Gerätes werden erneut Rohdaten erfasst, ein neues Template berechnet und mit dem gespeicherten verglichen. Der Vergleich erfolgt stets mithilfe von Templates, auf die die Vergleichsalgorithmen angewendet werden.

Die übliche Speicherung eines Templates anstelle der Rohdaten stellt lediglich eine Rationalisierung dar, um Speicherplatz und Vorverarbeitungszeit zu sparen. Denkbar wäre es auch, das Rohdatum als Referenz zu speichern und erst bei einem anstehenden Vergleich aus diesem ein Template für den Vergleichsvorgang zu berechnen. Festzuhalten ist, dass es für die Funktionsweise biometrischer Verfahren nicht erforderlich ist, biometrische Rohdaten zu speichern.

---

[13] *Busch/Daum*, in: c't 5/2003, 156 (156).

[14] Ausführlich zu den technischen Grundlagen der Erfassung biometrischer Merkmale und der Datenverarbeitung innerhalb eines biometrischen Systems *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.1.1, S. 7ff.

Notwendig wäre dies lediglich, wenn im Laufe des Betriebes die zur Berechnung der Templates verwendeten Algorithmen geändert werden sollen, ohne eine erneute Aufnahme der Rohdaten bei den Benutzern durchzuführen: In diesem Fall könnten bereits gespeicherte (alte) Rohdaten (die mehr Informationen als Templates enthalten) verwendet werden, um mit den neuen, ggf. verbesserten Algorithmen neue Templates zu berechnen. Ob dieses Vorgehen realistisch ist, darf bezweifelt werden, denn vermutlich ist der Qualitätsverlust auf Grund der Alterung von Rohdaten in Anbetracht der Gültigkeitsdauer von Ausweispapieren (5-10 Jahre) größer als der Vorteil verbesserter Algorithmen. Eine Aufnahme aktueller Rohdaten (sog. Re-Enrollment) dürfte Erfolg versprechender sein.

Darüber hinaus sind so genannte *templatefreie Verfahren*[15] denkbar, die aus den biometrischen Daten einen (eindeutigen) kryptographischen Schlüssel generieren. Der Schlüssel selbst wird nicht gespeichert, sondern stattdessen mit ihm verschlüsselte Zufallsdaten. Eine Authentifizierung erfolgt dann durch eine erfolgreiche Entschlüsselung. Bei Realisierung mit geeigneten kryptographischen Techniken kann verhindert werden, dass der Schlüssel (und damit die biometrischen Daten) rekonstruierbar ist oder für eine Authentifizierung übermittelt werden muss.

2.1.3 Denkbare künftige Einsatzszenarien für biometrische Verfahren

Einen weiten Anwendungsbereich biometrischer Verfahren werden in Zukunft die Identifikation sowie die Verifikation auf Grund biometrischer Merkmale im Bereich von Grenzkontrollen einnehmen. Gerade nach den Terroranschlägen vom 11. September 2001 wurde vielfach der Ruf nach Ergänzung der bisherigen Verfahren auch um biometrische Systeme laut. Ob und inwieweit die gegenwärtig bestehenden biometrischen Systeme bereits geeignet sind, in diesen Bereichen zum Einsatz zu gelangen, bedarf einer präzisen Beobachtung. Es gilt auch die Anforderungen zu formulieren, die an derartige Systeme zukünftig zu stellen sind. Angesichts der gegenwärtig noch festzustellenden hohen Fehlerquoten (siehe hierzu unten Abschnitt 2.1.4) stellt sich die Frage, welche Toleranzbereiche im Einsatzbereich biometrischer Verfahren zu akzeptieren sind.

Es lassen sich viele Beispiele für Entwicklungen im Bereich des Einsatzes biometrischer Verfahren zum Zwecke der Erleichterung der Identifikation bei Grenzkontrollen nennen. So ar

[15] *Probst,* Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler*, *v. Mutius*, Anonymität im Internet, S. 179-190, Kap. 4 mit Literaturangaben.

beitet in Deutschland gegenwärtig die Bundesdruckerei an sog. „Border Management Lösungen“. Die Bundesdruckerei entfaltet in diesem Bereich auch Aktivitäten auf internationaler Ebene. Bei der Entwicklung fälschungssicherer ID-Karten kommen verschiedene Möglichkeiten zum Einsatz, um den Sicherheitsstandard zu erhöhen. Als Sicherheitsbasis dienen nach Aussage der Bundesdruckerei das spezielle Papier, das Kartenrohmaterial, der Sicherheitsdruck, variable Merkmale und die Personalisierung der Karten. Die in die Karte geladenen Daten böten den Vorteil, dass eine Manipulation der Daten immer mit einer Beschädigung des Materials verbunden sei. Auch zusätzliche personalisierte Informationen wie die Hand- und Gesichtsgeometrie oder Fingerabdrücke ließen sich in die ID-Karte einbringen.[16] Neben ID-Dokumenten bietet die Bundesdruckerei u.a. auch Systeme zur Authentifizierung, Verifizierung und Identifizierung von Dokumenten bzw. Personen für Grenz- und Zutrittskontrollen an. Hierzu gehören z.B. Gesichtserkennungssysteme, Fingerprintsysteme und intelligente Kamerasysteme für die Echtzeit-Kontrolle in Sicherheitsbereichen.[17]

Der von der Bundesdruckerei entwickelte und kürzlich auf der Computermesse CeBIT 2003 vorgestellte sog. „Verifier“ ist ein Lesegerät, das die automatische Dokumentenkontrolle ermöglicht. Er soll Grenzkontrollen teilweise automatisieren, indem er prüft, ob das Dokument echt ist. Anhand der Sicherheitsmerkmale und maschinenlesbarer Informationen prüft er die Authentizität eines Dokumentes. Der „Verifier“ bietet mehrere Funktionalitäten und Anwendungsbereiche. Er ermöglicht die biometrische Identifikation von Personen und Dokumenten.[18] Das Gerät soll die Klärung der Frage vornehmen, ob das bei einer Grenzkontrolle vorgelegte Reisedokument echt ist. Sofern Pässe mit einem für den Bürger unsichtbaren Bild des Inhabers im Deckel des Passes versehen würden, könnte ein Grenzbeamter mithilfe des „Verifiers“ in weniger als einer Sekunde auslesen, ob der Besitzer auch der Inhaber des Dokumentes ist. Als biometrisches Verfahren wird in diesem Zusammenhang die Gesichtsgeometrie zu Grunde gelegt.[19]

---

16 Imagebroschüre, herausgegeben von der Bundesdruckerei GmbH: Identifikationskarten und ID-Systeme für die Zukunft, S. 8.

17 Imagebroschüre, herausgegeben von der Bundesdruckerei GmbH: Border Management Solutions, S. 7 (abrufbar unter http://www.bundesdruckerei.de/de/downl/downl_dok/border_d.pdf).

18 Imagebroschüre, herausgegeben von der Bundesdruckerei GmbH: Border Management Solutions: Der Verifier, S. 3/4 (abrufbar unter http://www.bundesdruckerei.de/de/downl/downl_dok/veri_d.pdf).

19 *Filser*, in: SZ vom 11.03.2003.

2.1.4 Wie zuverlässig sind biometrische Verfahren?

In den Medien wird häufig der Eindruck erweckt, als seien biometrische Verfahren die Lösung vieler Probleme. Doch biometrische Verfahren weisen durchaus Schwachstellen auf. Auch biometrische Verfahren können keine hundertprozentig sicheren Ergebnisse liefern. Bereits bei der Erfassung mittels Scanner, Kamera oder Fingerabdruck-Sensor bestehen beträchtliche Schwankungen der Rohdaten, so dass aus dem Vergleich der aufgenommenen Prüfdaten mit dem abgespeicherten Referenzmuster nicht immer sichere Ergebnisse resultieren. Die Ergebnisse biometrischer Verfahren sind mit statistisch verteilten Fehlern behaftet, die von der Art des verwendeten biometrischen Merkmals, der technischen Implementierung und nicht zuletzt der Population abhängen[20].

Bei der sehr häufig verwendeten Fingerabdruck-Messung kann es zu Störungen kommen, da die Qualität durch Hautfeuchtigkeit, Poren, flache Rillenprofile, Narben und Rückstände von Staub oder Fett erheblich beeinträchtigt wird.[21] Neben der Fingerabdruck-Messung erfreut sich die biometrische Gesichtserkennung großer Beliebtheit. Sie kommt anders als der Fingerabdruck ohne unmittelbaren Körperkontakt aus, jedoch bleibt in der Praxis die Zuverlässigkeit der Auswertung von Videoaufnahmen auf charakteristische geometrische Gesichtsmerkmale hinter der von Fingerabdrücken zurück, da die Qualität des Videobildes und damit die Erkennungssicherheit durch verschiedene Faktoren erheblich beeinträchtigt wird.

Kürzlich wurde das Scheitern eines im Juli 2002 begonnenen Pilotprojektes zur elektronischen Passbild-Überprüfung von Flugreisenden am Nürnberger Flughafen[22] vom bayerischen Staatsministerium des Innern bestätigt und damit der Versuch einer so genannten biometrischen Gesichtsfelderkennung beendet. Ziel des Projektes war die bessere Erkennung falscher Pässe. Mit dem System sollte im Verdachtsfall das vorgelegte Passbild mit dem Gesicht des Einreisenden verglichen werden. Doch habe es nach Aussage des Innenministeriums Probleme gegeben, weil das Programm ideale Lichtbedingungen verlangt hätte. Derzeit leiste der Prototyp des Modells nach Aussage eines Ministeriumssprechers „weniger als das geschulte

---

[20] Vgl. hierzu *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.3.1, S. 29ff.

[21] *Sietmann*, in: c't 5/2002, 146 (147).

[22] Zu dem Projekt: DANA 4/2002, S. 21.

Auge eines Polizisten.[23]“ Systematische Untersuchungen über die Qualität der derzeitigen Grenzkontrollen sind nicht bekannt.

Es gibt allerdings auch Berichte darüber, dass durch neu entwickelte Verfahren die Fehl-Erkennungsrate gegenüber herkömmlichen Gesichtserfassungssystemen deutlich abgesenkt werden könne und diese Verfahren auch erheblich schwerer zu täuschen seien.[24]

Fehlerraten

Fehlerhafte Ergebnisse biometrischer Verfahren werden danach unterschieden, ob eine fehlerhafte Erkennung einer unberechtigten Person (Falschakzeptanz, *false match*) oder eine fehlerhafte Nicht-Erkennung eines Berechtigten (Falschzurückweisung, *false rejection*, *false non-match*) erfolgt. Der Anteil der fehlerhaften Ergebnisse wird als FAR (*false acceptance rate*) oder FMR (*false match rate*) bzw. FRR (*false rejection rate*) oder FNMR (*false non match rate*) bezeichnet[25].

Einen Eindruck über die derzeitige Qualität von Gesichts- und Fingerabdruckerkennungverfahren erlauben die internationalen Wettbewerbe „Face Recognition Vendor Test 2002“[26] und „Fingerprint Verification Competion 2002, FVC2002.“[27]

In einem kürzlich veröffentlichten Test von Gesichtserkennungssystemen wurden aktuelle Zahlen über Falscherkennungen publiziert. Bei einer angenommen Falschakzeptanzrate (FAR) von 1% wurden von den besten Geräten bei einem 1:1-Vergleich (Verifikation) ca. 90% der Berechtigten erkannt und 10% abgewiesen[28]. Dies entspricht einer Falschzurückweisungsrate (FRR) von 10%. Die Ergebnisse beziehen sich auf einen Datensatz von Frontalaufnahmen bei Visa-Anträgen bei US-Behörden, die unter vergleichbaren Bedingungen aufgenommen wurden.[29] Beim Vergleich gleichtägiger Innenaufnahmen betrug die Erkennungsrate bis zu 95% (bei 1% Falschakzeptanzrate); wurden Innen- und Außenaufnahmen gemischt,

---

23 Meldung bei Heise Online vom 18.03.2003(abrufbar unter http://www.heise.de/newsticker/data/jk-18.03.03-006/).

24 Siehe Meldung bei Heise Online vom 28.02.2003 zu einer am Siemens-Forschungszentrum München-Neuperlach entwickelten Verfahrensweise, nach der der Gesichtserkennung ein dreidimensionales Bild zu Grunde gelegt wird (abrufbar unter http://www.heise.de/newsticker/data/jk-28.02.03-000/).

25 Siehe insbesondere *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.3.1, S. 29ff.

26 http://www.frvt.org/FRVT2002/

27 http://bias.csr.unibo.it/fvc2002

28 FRVT2002: Overview and Summary. Abb. 5, S. 7.

29 FRVT 2002: Evaluation Report, Kap. 6, S. 15f.

sank die Rate auf 50%.[30]. Im Bereich der Fingerabdruckverfahren lagen die besten Ergebnisse bei einer 1%igen FAR bei ca. 0,15% Falschzurückweisungen[31].

Neben der Zuverlässigkeit biometrischer Verfahren sind auch Aspekte der Sicherheit derartiger Verfahren von entscheidender Bedeutung. Zum einen ist zu fordern, dass ein biometrisches Verfahren Sicherheit vor Überwindung bietet, d.h. Mechanismen enthält, die davor schützen, dass es Unbefugten ermöglicht wird, ein biometrisches System mit falschen biometrischen Daten zu manipulieren. Ein biometrisches Verfahren muss darüber hinausgehend Erkennungssicherheit bieten, d.h. gewährleisten, dass bei der Identifikation von Merkmalsträgern Fehler des Systems weitgehend ausgeschlossen werden. Entscheidend dürfte es in diesem Zusammenhang darauf ankommen, dass bereits der Prozess der Einbringung biometrischer Daten in ein System angemessenen Sicherheitsvorkehrungen genügt. Die an Systeme zur Identitätsfeststellung im Bereich des Pass- und Personalausweiswesens sowie im Ausländerrecht zu stellenden Sicherheitsanforderungen werden in der nachfolgenden Darstellung in Kapitel 4 eingehend erörtert werden.

2.2 Datenschutz- und europarechtliche Rahmenbedingungen biometrischer Verfahren

2.2.1 Personenbezug biometrischer Daten

Für die datenschutzrechtliche Beurteilung des Einsatzes biometrischer Verfahren bedarf es einer Klärung der Frage, ob und inwieweit biometrische Daten personenbezogene Daten der jeweiligen Merkmalsträger darstellen. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Eine Person ist bestimmt, wenn sich aus den Angaben ergibt, dass sie sich auf diese Person und nur auf diese beziehen. Hierbei ist es unerheblich, in welcher Weise die Bezugsperson identifiziert und der Bezug dargestellt wird.[32] Personenbezogene Daten liegen aber nicht erst dann vor, wenn eine Person bestimmt ist, sondern vielmehr bereits dann, wenn sie bestimmbar ist, d.h. wenn die Person zwar nicht durch die Daten allein (eindeutig) identifiziert wird, jedoch mithilfe anderer Informationen festgestellt werden kann.[33]

---

[30] FRVT2002: Overview and Summary. Abb. 6, S. 8.

[31] Ergebnisse des FVC 2002 abrufbar unter http://bias.csr.unibo.it/fvc2002/results/resultsAvg.asp; dort schnitt der Algorithmus PA15 mit einer FNMR von 0,15% bei einer FMR von 1 ab (dort als FMR100 bezeichnet, s. http://bias.csr.unibo.it/fvc2002/perfeval.asp).

[32] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 20.

[33] *Dammann*, in: *Simitis* (Hrsg.), BDSG, § 3 Rn. 21.

Ob biometrische Daten personenbezogene Daten darstellen, lässt sich nicht pauschal beantworten. Vielmehr bedarf es einer Differenzierung zwischen den verschiedenen oben dargestellten Arten biometrischer Daten. Die Frage, ob bzw. ab welchem Verarbeitungsstadium biometrische Daten personenbezogene Daten sind, wird in der Literatur unterschiedlich beurteilt: Während *Albrecht*[34] alle biometrischen Rohdaten als personenbezogene Daten auffasst, differenzieren *Gundermann/Probst*[35] zwischen solchen Rohdaten, die mit den menschlichen Sinnen ohne weitere Hilfsmittel einer Person zugeordnet werden können (etwa Gesicht und Stimme) und weniger offenliegenden Rohdaten, die zur Zuordnung technische Hilfsmittel oder spezielle Kenntnisse erfordern (z.B. Fingerabdrucklinien)[36]. Template-Daten sind für sich genommen einem Pseudonym vergleichbar[37] und werden erst dadurch personenbezogen, dass sie mit zusätzlichen Identifizierungs- bzw. Adressierungsinformationen zusammengebracht werden können.

Biometrische Daten können zudem als besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG (sog. sensitive Daten) anzusehen sein. Bestimmte biometrische Rohdaten können einen Zusatzgehalt an Informationen enthalten, die u.U. Diagnosen auf bestimmte Krankheiten zulassen.[38] Diese Daten unterliegen besonderen Verarbeitungsanforderungen (vgl. §§ 13 Abs. 2, 28 Abs. 6 bis 9, 29 Abs. 5 BDSG).

Für die den Gegenstand der nachfolgenden Darstellung bildende Aufnahme biometrischer Daten in Ausweispapiere von Bundesbürgern bzw. „Ausländerausweise“ ist die Diskussion darüber, ob bzw. ab welchem Verarbeitungsstadium biometrische Daten als personenbezogene Daten anzusehen sind, nicht relevant: Hier besteht der Sinn gerade darin, zu den bereits vorhandenen identifizierenden personenbezogenen Daten weitere (in diesem Fall biometrische) Daten hinzuzufügen, die dadurch ihrerseits personenbeziehbar werden. Dies geschieht

---

34 *Albrecht,* Biometrische Verfahren, Kapitel Persönlichkeitsschutz und Recht auf informationelle Selbstbestimmung bei Verwendung biometrischer Daten, § 2 I 1 (i.E).

35 *Gundermann/Probst:* Biometrie, Rz 43 ff.

36 Den Unterschied dürfte die menschliche Fähigkeit ausmachen, sich Gesichter, Namen, Zahlen, Stimmen, Schriftart etc. zu merken und sie wiederzuerkennen. Bei Fingerabdrücken, Irismustern o.ä. besteht Merk- und Wiedererkennungsfähigkeit nicht.

37 *Probst,* Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler*, *v. Mutius*, Anonymität im Internet, S. 179-190.

38 Vgl. näher hierzu unten 4.3.1.1.2.; siehe zur Thematik auch *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.1.4 und 1.1.5, S. 18ff.

unabhängig von der Verarbeitungsform der biometrischen Daten (Rohdaten bzw. Templates). Die biometrischen Daten sind daher personenbezogen im Sinne der Datenschutzgesetze.[39]

Auch die in Abschnitt 2.1.2 diskutierten *templatefreien Verfahren,* mit deren Hilfe sich anonyme oder pseudonyme biometrische Systeme realisieren lassen[40], führen bei der beabsichtigten Aufnahme der Daten in Ausweispapiere nicht zu einer Aufhebung des Personenbezuges: Ebenso wie bei der Aufnahme von biometrischen Rohdaten oder Templates in Ausweise ist es auch ihre Bestimmung, eine Zuordnung des Ausweispapiers zum Besitzer nachzuweisen. Daher sind sie an die Identitätsdaten des Ausweisinhabers gekoppelt und somit personenbezogen.[41]

2.2.1.1 Datenschutzrechtliche Konsequenzen aus dem Personenbezug biometrischer Daten

2.2.1.2 Verfassungsrechtliche Folgerungen für das Recht auf informationelle Selbstbestimmung

Seit dem für das gesamte Datenschutzrecht richtungsweisenden Volkszählungsurteil aus dem Jahre 1983 sieht das Bundesverfassungsgericht die verfassungsrechtliche Grundlage des Rechts auf informationelle Selbstbestimmung im Allgemeinen Persönlichkeitsrecht in Verbindung mit der Menschenwürde verortet. Danach wird unter den Bedingungen der modernen Datenverarbeitung der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[42] Mit dem Recht auf informationelle Selbstbestimmung sind eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was und bei welcher Gelegenheit über

---

[39] *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.1.2, S. 14ff.

[40] Siehe *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap. 1.1.2.4, S. 17; *Probst,* Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler*, *v. Mutius*, Anonymität im Internet, S. 179-190, Kap. 4.

[41] Eine Gestaltung ohne Personenbezug ist aber denkbar, wenn die Ausweise selbst keine Identitätsdaten, sondern lediglich Berechtigungen („credentials“) wie etwa „Mindestalter 18“, „Berechtigung zum Führen von Kraftfahrzeugen der Klasse B“, „Berechtigung zum Eintritt in Sicherheitsbereich“ etc. enthielten.

[42] BVerfGE 65, 1 (1. Leitsatz; 43); ständige Rechtsprechung, vgl. BVerfGE 103, 21 (32f.); 84, 192 (194) jeweils m.w.N.

sie weiß.[43] Da das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet wird, sind Eingriffe in dieses Recht unter den vom Bundesverfassungsgericht aufgestellten Vorgaben grundsätzlich möglich. Im 2. Leitsatz des Volkszählungsurteils hat das Bundesverfassungsgericht ausgeführt: „Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.[44] Mit dem Grundsatz der Normenklarheit sind allzu unbestimmte Rechtsbegriffe oder Generalklauseln in Gesetzen allerdings unvereinbar.[45] Der Bürger muss erkennen können, für welche konkreten Zwecke des Verwaltungsvollzuges seine personenbezogenen Daten bestimmt und erforderlich sind.[46]

Das Recht auf informationelle Selbstbestimmung verbietet es grundsätzlich, personenbezogene Daten eines Betroffenen zu erheben, verarbeiten oder zu nutzen. Dieses Verbot wird erst dann aufgehoben, wenn die Verarbeitung durch eine gesetzliche Grundlage gerechtfertigt wird, die den durch das Bundesverfassungsgericht aufgestellten Anforderungen genügt. Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist auch dann zulässig, wenn der Betroffene in die Datenverarbeitung eingewilligt hat (vgl. § 4 Abs. 1 BDSG). Allerdings muss es sich hierbei um eine freiwillige und informierte Einwilligung des Betroffenen handeln.[47] An die Einwilligung sind strenge Anforderungen zu stellen. So ist eine Einwilligung nur dann wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (vgl. § 4a Abs. 1 BDSG). Als Zulässigkeitsvoraussetzung kann eine Einwilligung nur so lange tauglich sein, wie der Betroffene auch wirklich die Möglichkeit hat, selbst darüber zu befinden, ob und unter welchen Bedingungen die sich auf seine Person beziehenden Angaben benutzt werden dürfen.[48]

---

43 BVerfGE 65, 1 (43).
44 BVerfGE 65, 1 (2. Leitsatz).
45 *Tinnefeld*, in: *Tinnefeld/Ehmann*, Datenschutzrecht, I. Teil, Kap. 4.1.2., S. 86; vgl. BVerfGE 92, 191 (197).
46 BVerfGE 65, 1 (62).
47 *Bizer*, in: *Schulte* (Hrsg.), Handbuch des Technikrechts, S. 582.
48 *Simitis*, in: *Simitis* (Hrsg.), BDSG, § 4a Rn. 2.

2.2.1.3 Verhältnismäßigkeitsgrundsatz und Grundsatz der Zweckbindung

Sofern eine gesetzliche Grundlage den Eingriff in das Recht auf informationelle Selbstbestimmung legitimiert, sind an das einschränkende Gesetz besondere Anforderungen zu stellen. Einschränkungen des Rechts auf informationelle Selbstbestimmung sind nur zulässig, wenn der Grundsatz der Verhältnismäßigkeit beachtet wird. Diesem aus dem Rechtsstaatsprinzip abgeleiteten Grundsatz räumt das Bundesverfassungsgericht nicht erst seit dem Volkszählungsurteil Verfassungsrang ein.[49] Im Einzelnen bildet der Grundsatz der Verhältnismäßigkeit eine Grenze für die Einschränkung von Grundrechten auf Grund von bestehenden Gesetzesvorbehalten oder kollidierendem Verfassungsrecht.[50] Er besteht aus den Teilgeboten der Geeignetheit, der Erforderlichkeit und der Verhältnismäßigkeit im engeren Sinne.[51] Im Hinblick auf Einschränkungen des Rechts auf informationelle Selbstbestimmung wird der Grundsatz der Verhältnismäßigkeit vom Bundesverfassungsgericht konkretisiert. So schreibt das Gericht die Begrenzung der Daten auf den gesetzlich bestimmten Zweck vor.[52] Es lässt sich daher sagen, dass sich der Verhältnismäßigkeitsgrundsatz im Bereich des Datenschutzes zum Grundsatz der Zweckbindung verdichtet hat.[53] Dieser Grundsatz gilt nicht lediglich für die zwangsweise Erhebung, sondern vielmehr immer dann, wenn das Grundrecht durch eine gesetzliche Regelung berührt wird.[54] Jede Datenverarbeitung und –nutzung darf nur ganz bestimmten von vornherein festgelegten Zwecken dienen, die vorher bekannt sein müssen. Grundsätzlich muss daher bei jeder Datenverarbeitung bereits feststehen, für welche Zwecke die Daten verarbeitet und genutzt werden sollen, und dass eine Änderung dieser Absichten lediglich unter ganz bestimmten, einschränkenden Bedingungen zulässig ist. Weiterhin ist erforderlich, dass diese Zwecke den Betroffenen bekannt sind.[55]

Bildet eine Einwilligung des Betroffenen die rechtliche Grundlage der Erhebung und weiteren Verarbeitung der personenbezogenen Daten, so beschränkt diese auch die Art und den Umfang der Befugnis der verantwortlichen Stelle, die erhobenen Daten zu verarbeiten und zu nutzen auf die von dem Betroffenen gewollten Zwecke. Die Daten verarbeitende Stelle darf die Daten demnach nur zu dem (primären) Zweck verarbeiten und nutzen, zu dem sie sie er

---

[49] Vgl. *Jarass/Pieroth*, GG, Art. 20 Rn. 80ff. mit zahlreichen Nachweisen aus Rechtsprechung und Literatur.
[50] *Jarass/Pieroth*, GG, Art. 20 Rn. 81 m.w.N.
[51] *Jarass/Pieroth*, GG, Art. 20 Rn. 83ff. jeweils m.w.N.
[52] BVerfGE 65, 1 (46); vgl. ferner BVerfGE 103, 21 (33) m.w.N.
[53] *Tinnefeld*, in: *Tinnefeld/Ehmann*, Datenschutzrecht, I. Teil, 4.1.2, S. 87.
[54] *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, S. 71*; Simitis*, NJW 1984, 398 (402); ebenso Konferenz der Datenschutzbeauftragten des Bundes und der Länder, DÖV 1984, 504 (505).
[55] *Breinlinger*, in: *Bäumler/Breinlinger/Schrader*, Datenschutz von A-Z, Zweckbindung, Z 240.

hoben hat. Für die Verarbeitung zu anderen (sekundären) Zwecken bedarf es einer gesonderten Rechtsgrundlage oder einer erneuten Einwilligung des Betroffenen.[56] Sofern die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten durch eine gesetzliche Grundlage legitimiert wird, muss der Rechtsgrundlage der Zweck der Erhebung und der weiteren Verwendung zu entnehmen sein.[57]

Aus der vom Bundesverfassungsgericht geforderten Zweckbindung folgt zusätzlich der Grundsatz der informationellen Gewaltenteilung. So dürfen einer Stelle der öffentlichen Verwaltung nicht gleichzeitig Aufgaben übertragen werden, die zueinander im Widerspruch stehen. Vielmehr gebietet die informationelle Gewaltenteilung, dass eine Informationsweitergabe lediglich im Rahmen der zugewiesenen Aufgaben und Funktionen stattfindet, die sich gegenseitig nicht ausschließen.[58]

Bedeutung erlangt in Bezug auf die Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie in Ausländerpapiere die Frage, welche Stellen Zugriff auf die biometrischen Daten haben sollen. Außerdem kommt es auf die Art ihrer Speicherung an. Während für den Bereich des Pass- und Personalausweiswesens gesetzlich geregelt ist, dass eine bundesweite Datei nicht eingerichtet wird[59], besteht eine derartige Regelung für den Bereich der Ausländerpapiere nicht. Es stellt sich in diesem Zusammenhang die Frage, ob und inwiefern eine Vernetzung dieser Daten erfolgen soll, um einen Abgleich mit anderen Datenbeständen zu ermöglichen.

Welche Anforderungen aus dem Zweckbindungsgrundsatz an ein die Vorgaben des Terrorismusbekämpfungsgesetzes konkretisierendes Ausführungsgesetz im Bereich des Pass- und Personalausweiswesens bzw. diese Anforderungen konkretisierende Ausführungsverordnung für „Ausländerausweise“ zu stellen sind, wird im Rahmen der nachfolgenden Darstellung unter 4.3.2.2 beleuchtet werden.

---

[56] *Bizer*, in: *Schulte* (Hrsg.), Handbuch des Technikrechts, S. 583.
[57] *Bizer*, in*: Schulte* (Hrsg.), Handbuch des Technikrechts, S. 583.
[58] *Podlech*, in: AK-GG, Art. 2 Abs. 1 Rn. 82; *Tinnefeld*, in: *Tinnefeld/Ehmann*, Datenschutzrecht, I. Teil, 4.1.2, S. 88; BVerfGE 65, 1 (64, 69).
[59] § 4 Abs. 4 Satz 2 PassG, § 1 Abs. 5 Satz 2 PAuswG.

2.2.1.4 Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken

Das Bundesverfassungsgericht hat im Volkszählungsurteil das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken ausdrücklich betont. Eine derartige Vorratsdatenspeicherung wäre mit dem Grundsatz der Zweckbindung nämlich nicht zu vereinbaren. Ein Zwang zur Angabe personenbezogener Daten setzt nach Auffassung des Bundesverfassungsgerichts voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Das Gericht hat in seinem Volkszählungsurteil festgestellt, dass eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken mit dem Grundgesetz nicht zu vereinbaren wäre. Alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, müssten sich auf das zum Erreichen des angegebenen Ziels erforderliche Minimum beschränken.[60] Das Gericht hat das „Gebot einer konkreten Zweckumschreibung und das strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ für Datenerhebungen zu nichtstatistischen Zwecken im Volkszählungsurteil ausdrücklich betont.[61] Mit dem Verbot einer Datensammlung auf Vorrat soll verhindert werden, dass Daten gespeichert werden, ohne dass ein aktueller oder künftiger Bedarfsfall klar umschrieben wäre.[62]

Da es sich bei der Speicherung biometrischer Merkmale in Pässen, Personalausweisen und auch in „Ausländerausweisen“ um eine Vorratsdatenspeicherung handelt, die der besseren Identifizierung von Bundesbürgern bzw. Ausländern dienen soll, ist es erforderlich, von vornherein die Zweckbestimmung der Verarbeitung der biometrischen Daten präzise festzulegen. Bei der Konkretisierung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Regelungen ist ein besonderes Augenmerk darauf zu richten, durch klare Abgrenzung der Zwecke eine unbestimmte Vorratsdatenspeicherung zu vermeiden.

Als Beispiel für eine unbestimmte Vorratsdatenspeicherung lässt sich im Bereich des Ausländer- bzw. Asylverfahrensrechts die in § 41 Abs. 2 Sätze 2-4 AuslG und in § 16 Abs. 2 Sätze 3-5 AsylVfG vorgesehene Sprachanalyse anführen, deren gesetzliche Grundlagen ebenfalls mit dem Terrorismusbekämpfungsgesetz geschaffen wurden. Nach den genannten Vorschriften darf zur Bestimmung des Herkunftsstaates oder der Herkunftsregion das gesprochene Wort des Ausländers aufgenommen werden. Dass diese Sprachanalyse mit der Bekämpfung

---

60 BVerfGE 65, 1 (46).
61 BVerfGE 65, 1 (47).
62 *Weichert*, in: *Kilian/Heussen*, Computerrechts-Handbuch, Stand: März 2002, Ziff. 130 Rn. 39 m.w.N.

des Terrorismus bzw. generell von Straftaten zu tun haben soll, leuchtet zunächst nicht ein. Die Aufbewahrungsfrist dieser Sprachproben beträgt zehn Jahre. Diese Frist wirft die Frage auf, weshalb die Proben nicht nach Erstellung der Herkunftsgutachten und der Zuordnung der Sprache zu einer Region gelöscht werden. Die Unterlagen sollen allerdings auch *„zur Feststellung der Identität oder Zuordnung von Beweismitteln für Zwecke des Strafverfahrens oder zur Gefahrenabwehr*“ genutzt werden dürfen.[63] Hierbei handelt es sich um eine Vorratsdatenspeicherung, die sich auf zunächst unverdächtige Personen bezieht und insoweit als anlasslos anzusehen ist. Die weitere Aufbewahrung der Sprachproben stellt sich als unverhältnismäßig dar ist daher als verfassungswidrig anzusehen.[64]

2.2.1.5 Systemdatenschutz; Grundsatz der Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit wurde im novellierten BDSG in § 3a gesetzlich verankert[65]. Nach dieser Vorschrift haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen (§ 3a Satz 1 BDSG). Nach dem Willen des Gesetzgebers soll die Regelung dazu führen, dass durch den gezielten Einsatz datenschutzfreundlicher Technik die Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen reduziert werden.[66] Es handelt sich um einen Grundsatz, der Ausdruck des sog. Systemdatenschutzes ist, mit dem die Unterstützung des Datenschutzes durch Technik umgesetzt wird. Der Systemdatenschutz dient dazu, den Herausforderungen durch dynamische Technikentwicklung, allgegenwärtige elektronische Datenverarbeitung, für den Einzelnen unübersichtliche Strukturen, unbemerkte Datenerhebungen und undurchschaubare Verarbeitungsformen zu begegnen.[67] Die Anforderungen des Konzeptes des Systemdatenschutzes zielen auf eine technische und organisatorische Gestaltung des gesamten Systems der Datenverarbeitung.[68]

Der neu geschaffene § 3a BDSG stellt eine Zielvorgabe dar. Der Gesetzgeber überlässt es der verantwortlichen Stelle, auf welche Weise sie das Ziel der Datenvermeidung und Datensparsamkeit erreichen will. Die Vorgabe ist darauf gerichtet, eine Vermeidung bzw. Reduktion der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu erreichen. Hierbei ist die

---

63 § 78 Abs. 3 Satz 1 AuslG, § 16 Abs. 5 Satz 1 AsylVfG.
64 *Weichert*, DuD 2002, 423 (425).
65 Das Schleswig-Holsteinische Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz – LDSG) enthält eine derartige Regelung in § 4 Abs. 1 bereits seit dem Jahre 2000.
66 BT-Drucks. 14/4329, S. 30.
67 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, S. 39.

Gestaltung und Auswahl der Datenverarbeitungssysteme an dem Ziel auszurichten, entweder *keine* (Datenvermeidung) oder *so wenige personenbezogene Daten wie möglich* (Datensparsamkeit) zu erheben, zu verarbeiten und zu nutzen.[69] Der Grundsatz darf nicht mit dem Grundsatz der Erforderlichkeit verwechselt werden. Die Erforderlichkeit stellt eine rechtliche Anforderung an den Umfang der Datenverarbeitung, die aus dem rechtlich geregelten Zweck abgeleitet wird, dar und beschränkt diese in jedem Einzelfall. Sie stellt insoweit eine Zulässigkeitsvoraussetzung der Datenerhebung, -verarbeitung und -nutzung dar. Dagegen sind die Regelungen zur Datenvermeidung und Datensparsamkeit als Gestaltungsanforderungen an IT-Systeme anzusehen. Sie sind so zu gestalten, dass auch „technikbedingt" keine für die Zweckerreichung nicht erforderlichen personenbezogenen Daten erhoben, verarbeitet und genutzt werden. Das Ziel der Datenvermeidung kann allerdings auch durch Abstufungen auf der Ebene der Verarbeitungsschritte, insbesondere des Erhebens, Speicherns, Veränderns, Übermittelns (Verarbeitens) oder Nutzens erreicht werden. Als Beispiel lässt sich der Fall anführen, personenbezogene Daten zu erheben und zu speichern, aber ohne Personenbezug an Dritte zu übermitteln.[70] Ein Beispiel für die weitere in der Vorschrift genannte Alternative der Datensparsamkeit wäre der Fall, dass personenbezogene Daten lediglich kurzzeitig oder vorübergehend erhoben und gespeichert, aber unmittelbar nach ihrer Nutzung wieder gelöscht werden.[71]

Bei der Realisierung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise und „Ausländerausweise" ist der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten. Angesichts der mit der Aufnahme biometrischer Merkmale in diese Identifikationspapiere verbundenen Risiken für das Recht auf informationelle Selbstbestimmung muss bereits bei der Schaffung der die Regelungen des Terrorismusbekämpfungsgesetzes umsetzenden Vorschriften darauf geachtet werden, möglichst datensparsame Verfahren vorzusehen bzw. das Augenmerk darauf zu richten, trotz Erreichung des vorgesehenen Zwecks so wenig wie möglich überhaupt personenbezogene Daten zu erheben und zu verarbeiten.

2.2.1.6 Rechte der Betroffenen

Besondere Bedeutung kommt im Rahmen des Datenschutzrechts den Rechten der Betroffenen zu. Nach der Rechtsprechung des Bundesverfassungsgerichts gewährleistet das Grundrecht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen, selbst über die Preisgabe

---

68 *Bizer*, in*: Schulte* (Hrsg.), Handbuch des Technikrechts, S. 591.
69 *Bizer*, in: *Simitis* (Hrsg.), BDSG, § 3a Rn. 51.
70 *Bizer*, in: *Simitis* (Hrsg.), BDSG, § 3a Rn. 57f.
71 *Bizer*, in*: Simitis* (Hrsg.), BDSG, § 3a Rn. 64.

und Verwendung seiner persönlichen Daten zu bestimmen." Er hat ein Recht, „zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß".[72] Dem Einzelnen von der Datenverarbeitung Betroffenen muss eine größtmögliche Transparenz staatlicher Datenverarbeitung geboten werden. Die Rechte der Betroffenen bilden als Verfahrensrechte einen elementaren Bestandteil des Datenschutzrechts. Von fundamentaler Bedeutung ist das Recht des Betroffenen auf Auskunft über seine Daten. Mithilfe des Auskunftsanspruchs ist es dem Betroffenen möglich zu überprüfen, ob die verantwortliche Stelle rechtmäßig Daten über ihn verarbeitet. In Kenntnis der zu seiner Person verarbeiteten Daten kann der Betroffene von den weiteren ihm eingeräumten und unabdingbaren Kontroll-, Abwehr- und Gestaltungsrechten wie Berichtigung, Sperrung, Löschung und Widerspruch Gebrauch machen.[73] Sowohl das BDSG als auch die verschiedenen Landesdatenschutzgesetze enthalten jeweils einen eigenen Abschnitt, in dem die Rechte der Betroffenen gesetzlich normiert sind.

Sofern Personalausweise und Pässe von Bundesbürgern bzw. Identitätspapiere von Ausländern mit biometrischen Merkmalen versehen werden, bedarf es gleichzeitig der Schaffung von Verfahrensvorschriften, die den Betroffenen Transparenz hinsichtlich der über ihre Person erfolgenden Datenverarbeitung gewährleisten und die Rechte der Betroffenen wahren.

2.2.1.7 Verbot der automatisierten Einzelentscheidung

Gemäß § 6a Abs. 1 BDSG ist die Zulässigkeit automatisierter Einzelentscheidungen, die sich ausschließlich auf die automatisierte Verarbeitung personenbezogener Daten stützt, begrenzt. Mit dieser Regelung wurde Art. 15 der Europäischen Datenschutzrichtlinie umgesetzt. Das darin geregelte Verbot der Entscheidung ausschließlich auf der Grundlage automatisiert gespeicherter Daten kann aber nach den den Maßstäben des § 6a Abs. 2 BDSG durch flankierende Maßnahmen modifiziert werden.[74]

Ob die in der Gesetzesbegründung zu § 6a BDSG postulierte Nicht-Anwendbarkeit von § 6a BDSG auf biometrische Verfahren[75] grundsätzlich haltbar ist, darf bezweifelt werden[76]. So kommt es etwa im Beispiel einer biometriegestützten Grenzabfertigung auf die genauen De

---

[72] BVerfGE 65, 1 (43).
[73] *Mallmann*, in: *Simitis* (Hrsg.), BDSG, § 19 Rn. 1.
[74] *Gundermann/Probst*, Biometrie Rz. 71; *Bäumler/Gundermann/Probst*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kap 1.3.4.
[75] BT-Drucks. 14/4329, S. 37.
[76] Siehe auch *Albrecht*, Biometrische Verfahren, Kapitel Persönlichkeitsschutz und Recht auf informationelle Selbstbestimmung bei Verwendung biometrischer Daten, § 2 VII b.

tails des Abfertigungs-Prozederes an: Werden biometrische Verfahren lediglich als Hilfsmittel bei der manuellen Grenzkontrolle eingesetzt, dürfte § 6a BDSG nicht einschlägig sein, ebenso bei einer halb-automatisierten Grenzkontrolle, bei der ein manueller Eingriff bei „Problemfällen“ (Gerätedefekte, Abweisungen) vorgesehen ist.[77] Ist aber diese Eingriffsmöglichkeit faktisch beschränkt, etwa weil das biometrische Verfahren eine „Abweisung“ meldet, ein manueller Vergleich der biometrischen Daten nicht möglich ist (z.B. bei Fingerabdrücken) und de facto die Entscheidung „Abweisung“ des Verfahrens durch das Personal vor Ort kritiklos übernommen wird (werden muss), dürfte der Schutzzweck des § 6a BDSG vor undurchschaubaren automatisierten Entscheidungen greifen.

Dies bedeutet, dass biometrische Verfahren und Abläufe bei der Kontrolle so gestaltet werden müssen, dass ein manuelles Eingreifen möglich ist und das Verfahren zu keinen unzumutbaren Benachteiligungen (etwa lange Wartezeiten, Rechtfertigungsnotwendigkeit des Betroffenen und somit ein de-facto-Beweislastumkehr etc.) führt.

2.2.1.8 Biometrisches Personenkennzeichen

Biometrische Merkmale sind auf Grund ihrer Unveränderbarkeit geeignet, als Personenkennzeichen zu verwendet zu werden, da sich mit ihrer Hilfe eine Vielzahl unterschiedlicher Dateien verknüpfen ließe. Ende der 60er-Jahre fanden Bestrebungen statt, jedem Bürger ein Personenkennzeichen zuzuweisen und damit zentrale Datenbestände mit der Möglichkeit der Verknüpfung einzuführen. Wegen der Gefahr der Bildung von Persönlichkeitsprofilen wurden die Personenkennzeichen bereits in der Mikrozensus-Entscheidung des Bundesverfassungsgerichts für unzulässig erklärt.[78] Auch im Volkszählungsurteil stellte das Bundesverfassungsgericht die Verfassungswidrigkeit noch einmal ausdrücklich fest.[79] Das Verbot einheitlicher Personenkennzeichen dient präventiv der Verhinderung des Zusammenführens von Daten aus unterschiedlichen Bereichen, z.B. zur Erstellung von Persönlichkeitsprofilen.[80] Grundsätzlich eignen sich auch biometrische Merkmale als Personenkennzeichen.[81] Technisch lassen sich die personenbezogenen Daten einer Person mit den aus den biometrischen Merkmalen generierten Templates zusammenführen, so dass eine Verknüpfung dieser Daten möglich ist.[82] Aus

---

77 Siehe auch GAO-03-174 Biometrics for Border Security, S. 98ff.
78 BVerfGE 27, 1 (6); zur Geschichte des Personenkennzeichens auch *Weichert*, RDV 2002, 170 (172).
79 BVerfGE 65, 1 (53).
80 *Weichert*, in: *Kilian/Heussen*, Computerrechts-Handbuch, Ziff. 130, Rn. 38.
81 *Weichert*, CR 1997, 369 (372).
82 Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 17.

datenschutzrechtlicher Sicht wäre eine unbegrenzte Verwendung der biometrischen Merkmale auf Pässen und Personalausweisen für Bundesbürger oder „Ausländerausweisen“ zum Zwecke der Zusammenführung verschiedener Datenbestände daher als unzulässig anzusehen. Es bedarf daher einfachgesetzlicher Nutzungseinschränkungen.[83]

2.2.1.9 Folgerung

Biometrische Daten sind personenbezogene Daten, die den datenschutzrechtlichen Vorschriften unterliegen. Die Erhebung, Verarbeitung und Speicherung biometrischer Merkmale bedarf einer verfassungsgemäßen rechtlichen Grundlage, die dem Zweckbindungsgrundsatz genügt, eine Speicherung biometrischer Merkmale auf Vorrat ist unzulässig. Es dürfen lediglich diejenigen Daten gespeichert werden, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind. Bei der Schaffung der Ausführungsvorschriften zur Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie „Ausländerausweise“ hat der Gesetz- bzw. Verordnungsgeber den Grundsatz der Datenvermeidung und Datensparsamkeit zu berücksichtigen. Er ist gehalten, sich bei der Realisierung der Vorgaben des Terrorismusbekämpfungsgesetzes an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Den Betroffenen muss hinsichtlich der staatlichen Datenverarbeitung eine größtmögliche Transparenz geboten werden. Insbesondere ist ihnen ein Auskunftsrecht über ihre Datenverarbeitung einzuräumen. Biometrische Merkmale dürfen nicht verwendet werden, um Persönlichkeitsprofile über die Betroffenen zu bilden.

2.2.2 Europarechtliche Grundlagen

Soweit die Regelungen des Terrorismusbekämpfungsgesetzes Angelegenheiten des Europäischen Gemeinschaftsrechts[84] berühren, ist zu überprüfen, inwiefern das Recht der Europäischen Gemeinschaften verbindliche Ausgestaltungsvorgaben trifft. Ähnlich wie das nationale Verfassungsrecht den Staatsorganen die Beachtung des Grundrechts auf informationelle Selbstbestimmung auferlegt, müssen die Gemeinschaftsorgane und die Mitgliedstaaten im Rahmen des Gemeinschaftsrechts die Vorgaben der Grundrechte beachten.

---

[83] *Weichert*, in: *Kilian/Heussen*, Computerrechts-Handbuch, Ziff. 130, Rn. 38.

[84] Grundsätzlich bezeichnet „Gemeinschaftsrecht“ das Recht der Europäischen Vertragsgemeinschaften EGV, EAGV und EGKS, während das Recht der „Europäischen Union“ den Dachvertrag EUV mit einbezieht. Mangels Erforderlichkeit für die Ergebnisfindung wird vorliegend jedoch begrifflich nicht zwischen dem Recht der Europäischen Union und dem Gemeinschaftsrecht unterschieden.

Zu berücksichtigen ist dabei, dass die Europäische Datenschutzrichtlinie[85] keine unmittelbare Anwendung findet bei Tätigkeiten, die Titel V und VI des EU-Vertrages betreffen.[86]; insoweit fallen insbesondere Vorschriften über die öffentliche Sicherheit, die Sicherheit des Staates sowie strafrechtliche Normen aus dem unmittelbaren Regelungsbereich der Richtlinie heraus. Das allgemeine Pass- und Personalausweisrecht unterliegt danach nicht den Umsetzungsvorgaben der Europäischen Datenschutzrichtlinie.

2.2.2.1 Gemeinschaftsrechtliches Grundrecht auf Datenschutz – inhaltliche Vorgaben

Von Beginn seiner Grundrechts-Rechtsprechung an hat der Europäische Gerichtshof (im Folgenden: EuGH) anerkannt, dass der *Schutz personenbezogener Daten Grundrechtsqualität* genießt.[87]

In Bezug auf die Verarbeitung personenbezogener Daten zieht die Rechtsprechung des EuGH in erster Linie Art. 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) heran, berücksichtigt aber zugleich die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten sowie weitere Rechtsquellen, namentlich Rechtsakte und Verlautbarungen der Unionsorgane und die Genfer Flüchtlingskonvention.[88] Durch diese Rechtsprechung und durch Legislativakte der Gemeinschaft wird ein unionsspezifischer Grundrechtsschutz[89] geschaffen, der in einigen Bereichen über den Grundrechtsschutz der EMRK und der Mitgliedstaaten hinausgeht, in anderen Belangen allerdings auch zurückbleibt. Anders als Art. 8 EMRK, der seinem Wortlaut nach nur das Privat- und Familienleben schützt, wird im Recht der Europäischen Gemeinschaften ein Grundrecht auf Datenschutz ausdrücklich bekräftigt, vgl. auch Art. 8 der Charta der Grundrechte der Europäischen Union (EuGrC). Die EuGrC wurde auf dem Rat von Nizza von den Staats- und Regierungschefs zwar proklamiert, jedoch nicht in den EU-Vertrag aufgenommen. Die Frage der Rechtsverbindlichkeit der EuGrC ist noch nicht abschließend geklärt. Zu berücksichtigen ist auch, dass die EuGrC keine unmittelbar einklagbaren Rechte enthalten soll.[90] In Art. 52 Abs. 3 wird jedoch verdeutlicht, dass die EuGrC diejenigen grundrechtlichen Prinzipien benennt, die als

---

85 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 L 281/31.

86 Art. 3 Abs. 2 erster Spiegelstrich, Erwägung 13 EG DSRL.

87 EuGH vom 12.11.1969, Rs. 29/69 = EuGHE 1969 S. 419 ff. (Stauder vs. Ulm).

88 Vgl. Art. 6 Abs. 2 EUV.

89 Ausführlich dazu *Petri*, Europol 2001, S. 112 ff.

90 Vgl. Erläuterung des Präsidiums der Grundrechtekommission zu Art. 52 Abs. 2 EuGrC, EU-Dok. CHARTE 4473/00.

unionsspezifische Ausgestaltung der EMRK anzusehen sind.[91] Dementsprechend gründet das in Art. 8 EuGrC proklamierte unionsrechtliche Grundrecht auf Datenschutz im Wesentlichen auf Art. 286 EG[92], die Richtlinie 95/46/EG,[93] [94] Art. 8 EMRK und die Europäische Datenschutzkonvention 1981[95].[96]

Soweit ersichtlich hat der EuGH zur Entscheidungsfindung bislang noch nicht ausdrücklich auf Art. 8 EuGrC Bezug genommen. Sowohl die Schlussanträge verschiedener Generalanwälte[97] als auch das Europäische Gericht erster Instanz[98] haben aber ungeachtet des Art. 51 Abs. 2 EuGRC die Bekräftigungsfunktion der Charta bereits anerkannt. Selbst bei zurückhaltender Beurteilung des Verbindlichkeitsmaßstabes der EuGrC wird man deshalb die in Art. 8 EuGrC genannten Maßstäbe *als gesicherte Orientierungspunkte* für ein datenschutz- und grundrechtskonformes Verhalten ansehen können. Dies spiegelt sich auch in den Bezugnahmen der Rechtsakte wider, welche die Gemeinschaft im Regelungsbereich der Art. 61-64 EG (gemeinschaftsrechtlichen Asyl- und Flüchtlingsrecht) erlassen hat.[99]

Legt man dementsprechend Art. 8 EuGrC als Substrat eines unionsspezifischen „Grundrechts auf Datenschutz“ zugrunde, müssten folgende Prinzipien zu beachten sein:

---

91 Zur Funktion der Datenschutzrichtlinie als Konkretisierung des Art. 8 EMRK vgl. Art. 1 Abs. 1 und Erwägung 10 der Datenschutzrichtlinie; mit unterschiedlicher Terminologie aber im Ergebnis ähnlich: *Dammann/Simitis*, EG-Datenschutzrichtlinie 1997, Art. 1 Anm. 3: grundrechtliche Ausgestaltungsfunktion der Richtlinie; *Petri*, Europol 2001, S. 130 ff.: Richtlinie als unionsspezifische Ausgestaltung des Art. 8 EMRK; *Gola/Schomerus*, BDSG Art. 1 Rn. 3: Schutz der Persönlichkeitsrechte der Betroffenen durch die Richtlinie.

92 Vertrag zur Gründung der Europäischen Gemeinschaft vom 25. März 1957 in der Fassung des Amsterdamer Vertrags (BGBl. 1998 II S. 387). Art. 286 hat allerdings nur für die Gemeinschaftsorgane, nicht für mitgliedstaatliche Institutionen Bedeutung; vgl. dazu im Einzelnen *Kingreen* in *Calliess/Ruffert* (Hrsg.), EUV / EGV, Kommentierung zu Art. 286 EGV.

93 Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 L 281/31).

94 Vgl. insbesondere die ausdrückliche Bezugnahme auf die Datenschutzrichtlinie bei der bereits erwähnten EURODAC-Verordnung Nr. EG/2725/2000 vom 11.12.2000 (ABl. 2000, L 316/1), Erwägung 15; abgeschwächt in Erwägung 17 der Richtlinie 2001/55/EG über die Mindestnormen für die Gewährung vorübergehenden Schutzes im Falle eines Massenzustroms von Vertriebenen ... (ABL. 2001 L 212/12).

95 Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Konvention des Europarates Nr. 108) vom 28.1.1981.

96 Vgl. Erläuterungen des Präsidiums der Grundrechtekommission zu Art. 8 EuGrC.

97 Vgl. beispielsweise Generalanwalt *Tizzano* vom 14.11.2002 in der Rs. C-465/00 – Rechnungshof vs. Österreichischer Rundfunk, Rn. 2 ff.; Generalanwalt *Alber* vom 24.10.2002 in der Rs. C-63/01 (Evans vs. Secr. of State for the Environment, Transport and the Regions et al.); Generalanwalt *Jacobs* am 14.6.2001 (Rs. C-377/98 – Niederlandevs.Parlament u. Rat); Generalanwalt *Colomer* am 3.12.2001 (Rs. C-208/00 – Überseering).

98 Vgl. Beschluss vom 18.10.2002, Rs. C-232/02 P(R) (Kommission vs. Technische Glaswerke Ilmenau GmbH) – Rn. 85; Urteil vom 30.1.2002, Rs. T-54/99 (max.mobil TK Service/ Kommission) – Rn. 48.

99 Ausdrücklich Bezugnahme auf den Grundrechtsschutz der EuGrC finden sich insbesondere auch in Rechtsakten der Europäischen Gemeinschaft zum Asylrecht, z.B. in Erwägung 15 der VO Nr. EG/343/2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Antrags zuständig ist (ABl. 2003 L 50/1); Erwägung 5 der Richtlinie 2003/9/EG zur Festlegung von Mindestnormen für die Aufnahme von Asylbewerbern in den Mitgliedstaaten (ABl. 2003. L 31/18).

1. Die Verarbeitung von personenbezogenen Daten hat nach Treu und Glauben zu erfolgen.

2. Die verarbeitenden Stellen sind an festgelegte, legitime Zwecke gebunden.

3. Verarbeitungsvoraussetzung muss die Einwilligung des Betroffenen oder eine gesetzliche Legitimationsgrundlage sein.

4. Jede betroffene Person hat das Recht auf Auskunft über die sie betreffenden erhobenen Daten.

5. Jede betroffene Person hat das Recht, sie betreffende personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

6. Die Einhaltung des Datenschutzes ist von einer unabhängigen Stelle zu beobachten.

Damit entspricht die europäische Grundrechtslage weitgehend den oben beschriebenen Vorgaben des deutschen Verfassungsrechts.

2.2.2.2 Bindung an Art. 8 EMRK: Schutz des Privatlebens[100]

Die oben genannten Grundsätze erlangen dann unmittelbare Geltung, wenn sie in sekundäre EG-Rechtsakte inkorporiert werden.

Beispielsweise ist nach Erwägung 12 der EURODAC Verordnung[101] zumindest die Verfolgung einer einheitlichen Asylpolitik auch als *Gemeinschaftsangelegenheit* zu betrachten.[102] Dementsprechend findet nach Erwägung 15 der EURODAC-Verordnung die EG-Datenschutzrichtlinie auf die Verarbeitung personenbezogener Daten im Rahmen des EURODAC-Systems Anwendung. Ein Bekenntnis zur EuGrC findet sich in den Rechtsakten, die

[100] Authentische Übersetzung der Originaltexte der EMRK (englisch: Respect for private live / französisch: Respect de la vie privée).
[101] VO EG/2725/2000, ABL. 2000 L 316/1.
[102] Zu dem damit verbundenen Problem der Subsidiarität vgl. jüngst *Koenig/ Lorz*, JZ 2003, 167 (167 ff.).

für Verfahren gelten, die im Rahmen einer gemeinschaftsweit einheitlichen Prüfung von Asylanträgen durchgeführt werden.[103]

Diese gemeinschaftsrechtlichen grundrechtlich geprägten Vorgaben gelten allerdings für solche rein innerstaatlichen Regelungen des Terrorismusbekämpfungsgesetzes nicht, die keine Bezüge zum Gemeinschaftsrecht aufweisen. Dementsprechend dürfen diese Vorschriften auch nicht unter dem Gesichtspunkt der Verletzung der EMRK *als Bestandteil des EU-Rechts* beurteilt werden.[104]

Soweit wegen eines fehlenden Gemeinschaftsbezugs oder wegen der Zuordnung zu den Titeln V und VI EUV die Europäische Datenschutzrichtlinie keine Anwendung findet,[105] muss die Bundesrepublik Deutschland allerdings gleichwohl die Anwendung des Art. 8 EMRK im Rahmen ihrer völkerrechtlichen Bindung als innerstaatliches Recht berücksichtigen.

Nach Art. 1 gilt die EMRK für alle Menschen, die der Hoheitsgewalt der EMRK-Mitgliedstaaten unterstehen. Garantiert wird ein unmittelbarer Schutz, der nicht an einen Bürgerstatus anknüpft.[106]

Nach der Rechtsprechung des Bundesverfassungsgerichts[107] gilt die EMRK kraft gesetzlicher Übernahme im Rang eines Bundesgesetzes, nicht als allgemeine Regel des Völkerrechts im Sinne des Art. 25 GG. Allerdings dürfen die aus der EMRK resultierenden völkerrechtlichen und menschenrechtlichen Verpflichtungen nicht durch eine Auslegung von Bundesrecht in Frage gestellt werden.[108] Im Verhältnis zu anderen bundesgesetzlichen Regelungen kommt der EMRK damit eine besondere Bedeutung zu; insbesondere findet auf Grund der völkerrechtlichen Menschenrechtsbindung der Bundesrepublik für sie die so genannte lex posterior-Regelung[109] keine Anwendung.

---

[103] Vgl. ausdrücklich Erwägung 15 der VO EG/343/2003 des Rates vom 18.2.2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist: „Die VO steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden."

[104] Grundlegend zur Problematik die *ERT-Entscheidung* des EuGH, EuGHE 1991 I 2925, 2964 (Rs. C 260/89), Rn. 42 m.w.N.. In Bezug auf Art. 8 EMRK vgl. insbesondere die Schlussanträge des Generalanwalts *Tizzano* vom 14.11.2002 in der Rs. C-465/00 – Rechnungshof vs. Österreichischer Rundfunk, Rn. 25 ff.

[105] Grundlegend dazu die *ERT-Entscheidung* des EuGH, EuGHE 1991 I 2925, 2964 (Rs. C 260/89), Rn. 42 m.w.N.

[106] Ebenso *Meyer-Ladewig*, Hk EMRK Art. 1 Rn. 10, 11; *Frowein/Peukert*, EMRK, Art. 1 Rn. 2, 3.

[107] BVerfGE 74, 358, 370.

[108] BVerfGE a.a.O.

[109] Gemeint ist die Regel, dass ein jüngeres Gesetz ältere Gesetze verdrängt.

Letztlich noch ungeklärt ist die Frage, inwiefern die Bundesrepublik über etwaige Einzelfälle[110] hinaus an die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) gebunden ist. Insoweit dürfte auch die innerstaatliche Rechtsprechung zu berücksichtigen haben, dass der EGMR zur *authentischen Interpretation* der EMRK berufen ist.[111] Insbesondere ist zu beachten, dass der EGMR auch Legislativakte der Mitgliedsstaaten in seinen Kontrollbereich einbeziehen kann.[112]

Das Menschenrecht auf *Schutz des Privatlebens* ist unstreitig betroffen, wenn ein Hoheitsträger personenbezogene Daten erfasst, speichert oder weitergibt, die das Privatleben eines Menschen betreffen.[113] Der Begriff des Privatlebens wird umfassend verstanden;[114] soweit sich aus der Verarbeitung Informationen über die körperliche Integrität und geistige Gesundheit ergeben, sind wesentliche Elemente des Privatlebens betroffen.[115]

Einschränkungen des Schutzes des Privatlebens müssen *gesetzlich vorgesehen* sein. Das den Eingriff legitimierende Gesetz muss *deutlich* und *genau* sein („ „in accordance with the law" implies conditions which go beyond the existence of a legal basis in domestic law and requires that the legal basis be „accessible" and „foreseeable"[116]"). Vorhersehbar ist eine gesetzliche Regelung nach der Rechtsprechung des EGMR, wenn sie mit einer hinreichenden Präzision formuliert ist, so dass jedes Individuum – nötigenfalls unter entsprechender Anleitung – die Folgen der Regelung absehen kann.

Verfolgt eine gesetzliche Regelung wie bei dem Terrorismusbekämpfungsgesetz Zwecke der nationalen oder öffentlichen Sicherheit, müssen die vorgesehenen Maßnahmen „*in einer demokratischen Gesellschaft notwendig*" sein, Art. 8 Abs. 2 EMRK. Danach müssen bei der Errichtung eines Datenbestandes (mindestens) die Umstände, das Verfahren, die Art der Informationen, ihre Aufbewahrungsfristen und die Vernichtung geregelt sein. Immer wenn eine

---

[110] Nach Art. 46 Abs. 1 EMRK sind nur die Parteien eines Rechtsstreits an die Entscheidung des Gerichtes *unmittelbar* gebunden.
[111] *Petri*, Europol 2001, S. 120.
[112] Vgl. z.B. Urteil vom 18.2.1999 Beschwerde Nr. 24833 (Matthews vs. UK), EuGRZ 1999, 200 ff.
[113] Ständige Rechtsprechung des EGMR seit EGMR, U.v. 26.3.1987 (Leander vs. Sweden); z.B. EGMR U.v. 30.7.1998, ENr. 58/1997 (Contreras vs. Spanien).
[114] *Meyer-Ladewig*, Hk EMRK 2003, Art. 8 Rn. 3 m.w.N..
[115] EGMR v. 25.2.1997, Entscheidungssammlung 1997 I, S. 347 ff., Rn. 95 ff. (Z. vs. Suomi). Zustimmend: *Meyer-Ladewig*, Hk EMRK 2003, Art. 8 Rn. 11.
[116] U.v. 16.2.2000, E-Nr. 27798/95 (Amann vs. CH), Rn. 55.

Offenbarung sensibler Daten droht, muss das innerstaatliche Recht überdies ausreichende Garantien gegen einen etwaigen Datenmissbrauch geben.[117]

2.2.2.3 Europarechtliche Vorgaben zu biometrischen Verfahren

Es ist fraglich, ob auf europäischer Ebene konkrete Vorgaben für die Ausgestaltung biometrischer Systeme auf nationaler Ebene bestehen. Es existieren verschiedene Vorschriften, die im weitesten Sinne relevant für die Aufnahme biometrischer Merkmale in Ausweispapiere sind.

So betreffen die EURODAC-Verordnungen[118] im Wesentlichen die Übermittlung von Fingerabdruckdaten an das zentrale System EURODAC und ihre dortige Speicherung. Sie regeln nicht die Anforderungen an die Ausgestaltung von Ausweispapieren jedweder Art. Hieraus Maßgaben für die Ausweispapiergestaltung ableiten zu wollen, würde bedeuten, dass die Rechtmäßigkeit der Aufnahme von biometrischen Daten in Ausweispapieren bereits wegen der besagten Verordnungen in Frage gestellt wäre. Dieses Ergebnis ist jedoch nicht zugrunde zu legen, da die Aufnahme von Fingerabdrücken in Flüchtlingspapieren bereits in der Genfer Flüchtlingskonvention zugelassen wurde und seitdem gängige Praxis ist.

Die Verordnungen zur einheitlichen Visagestaltung[119] sehen die Integration eines „gemäß Hochsicherheitsnormen hergestellten Lichtbildes“ in Visadokumenten vor. Bindend für den innerstaatlichen Gesetz- und Verordnungsgeber sind vor allem die Maßstäbe der Fälschungssicherheit. Die Aufnahme von (weiteren) biometrischen Merkmalen ist (soweit ersichtlich) nicht verbindlich vorgegeben.

Das Schengen-Akquis, insbesondere das Schengener Durchführungsübereinkommen (SDÜ)[120], sieht gemeinsame Regelungen für die sichtvermerksfähigen Reisedokumente sowie Form, Inhalt und Gültigkeitsdauer der Sichtvermerke insbesondere für kurzfristige Aufenthalte vor (vgl. Art. 17 Abs. 3 SDÜ). Die erforderlichen Entscheidungen werden durch einen Exekutivausschuss[121] getroffen. Insoweit dürfte der deutsche Gesetz- und Verordnungsgeber

---

[117] U.v. 16.2.2000, E-Nr 27798/95 (Amann vs. CH), Rn. 56 ff., 76 ff. mit weiteren Nachweisen aus der EGMR-Rechtsprechung.
[118] VO EG/2725/2000 (ABl. 2000 L 316/1); VO EG/407/2002 (ABl. 2002 L 62/1).
[119] Vgl. insbesondere VO EG/1683/95, Art. 1, 6 zzgl. Anhang (ABl. L 1995, 1); geändert durch VO EG/334/2002 (ABl. C 313/167).
[120] Vom 19.06.1990, BGBl. II 1993, S. 1010.
[121] Gemäß Artikel 131 Abs. 1 SDÜ richten die Vertragsparteien im Hinblick auf die Anwendung des Übereinkommens einen Exekutivausschuss ein. Gemäß Artikel 132 Abs. 1 SDÜ hat jede Vertragspartei einen Sitz in

an die Vorgaben des Ausschusses gebunden sein. Sichtvermerke für längere Aufenthalte (länger als drei Monate) werden nach Maßgabe des nationalen Rechts erstellt, Art. 18 SDÜ. Soweit ersichtlich, sind dabei keine verbindlichen Mindeststandards hinsichtlich der Aufnahme biometrischer Merkmale vorgesehen, die die Bundesrepublik zu Maßnahmen im Sinne des Terrorismusbekämpfungsgesetzes anhalten.[122]

Im Ergebnis nichts wesentlich Anderes ergibt sich auch aus der Verordnung EG/1030/2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatenangehörige.[123] Diese Verordnung ersetzt[124] die Gemeinsame Maßnahme vom 16.12.1996 des Rates (97/11/JI) zur einheitlichen Gestaltung der Aufenthaltstitel,[125] deren Verbindlichkeitswirkung im Hinblick auf Artikel K.3 des EUV (Maastrichter Vertrag[126]) äußerst fragwürdig war.[127] Aus der besagten Maßnahme ergaben sich *keine* besonderen Anforderungen an biometrische Merkmale.

Diese Rechtslage ist durch die Verordnung EG/1030/2002 abgeändert worden; sie gilt gemäß Art. 249 Abs. 2 EGV in der zurzeit geltenden Amsterdamer Fassung *unmittelbar* in jedem Mitgliedsstaat. Soweit man von der Möglichkeit geheimer Ausweisspezifikationen absieht,[128] verlangt die Verordnung als biometrisches Mindestmerkmal bislang allerdings nur die Anbringung eines *Lichtbildes*.[129] Die Aufnahme *weiterer biometrischer Merkmale ist nicht vorgesehen*. Vielmehr weist Erwägung 6 der genannten Verordnung darauf hin, dass die Mitgliedsstaaten und die Kommission in regelmäßigen Abständen *prüfen*, ob biometrische Merkmale entsprechend dem technischen Fortschritt künftig an den Sicherheitsmerkmalen des Titels vorzunehmen sind. Die Präambel der Verordnung als verbindlicher *Auslegungsmaßstab* konstituiert dabei keine Verpflichtung zur *Aufnahme* von zusätzlichen biometrischen Merkmalen, eine solche Anordnung wäre ausdrücklich in den Artikelteil der Verordnung aufgenommen worden.

---

dem Exekutivausschuss. Die Vertragsparteien sind in dem Exekutivausschuss durch einen für die Durchführung des Übereinkommens zuständigen Minister vertreten.

[122] Vgl. dazu auch Gemeinsames Handbuch EG 2002/C 313/02, insbes. S. 151ff.

[123] Vom 13. Juni 2002, vgl. ABl. 2002 L 157/1.

[124] Vgl. Art. 9 Abs. 2 der VO.

[125] ABl. EG 1997 L 7/01.

[126] Vom 07.02.1992, vgl. BGBl. II 1992, S. 1251.

[127] Art. K.3 Abs. 2 EUV sieht für die Gemeinsame Maßnahme keine Rechtswirkungen vor, anders der die Gemeinsame Maßnahme substituierende Rahmenbeschluss (vgl. Art. 34 Abs. 2b EUV in der Fassung des Amsterdamer Vertrages).

[128] Vgl. Erwägung 7 der VO. Nach dieser Erwägung enthält die Verordnung nur diejenigen Spezifikationen, die nicht geheim sind. Diese sollten durch weitere Spezifikationen ergänzt werden, die geheim bleiben müssen, um Fälschungen und Verfälschungen zu verhindern und die keine personenbezogenen Daten oder Hinweise auf personenbezogene Daten umfassen dürfen.

[129] Art. 9 Abs. 3 der VO.

Der nationale Gesetzgeber hat in der Begründung zur Änderung des AuslG durch das Terrorismusbekämpfungsgesetz angeführt, mit der Regelung werde die o.g. Gemeinsame Maßnahme umgesetzt. Es ist allerdings bereits an dieser Stelle kritisch anzumerken, dass der Gesetzgeber mit der Änderung von § 5 AuslG und insbesondere der Regelung zur Aufnahme biometrischer Merkmale weit über die Vorgaben der Gemeinsamen Maßnahme hinausgeht.[130]

Darüber hinaus hat sich die Bundesrepublik verpflichtet, Reisedokumente nach den Standards[131]der Internationalen Organisation für die zivile Luftfahrt (International Civil Aviation Organization, ICAO) auszugeben. Ob diese Verpflichtung unmittelbar gegenüber der ICAO im Rahmen der Umsetzung des Abkommens über die Internationale Zivilluftfahrt[132] gilt, kann mangels Zugänglichkeit der Anlagen zum Abkommen nicht ermittelt werden. In einer Entschließung[133] des Rates der EU, die keine unmittelbar rechtsbindende Wirkung hat, wurde die Übereinkunft festgelegt, Reisepässe mit maschinenlesbaren Lesezonen gemäß dem ICAO-Dokument 9003 Teil 1 und 2 auszustatten. Der Gesetzgeber hat die Vorgaben dieser Entschließung bzw. seiner Vorläufer über die Gestaltung von Reisepässen 1986 mit § 4 Abs. 4 PassG direkt in das PassG[134] übernommen, den Verweis aber im Jahr 2000 gestrichen.[135]

Eine rechtlich bindende Verpflichtung zur Umsetzung des ICAO-Standards ist im Rahmen der Entschließung der EU zur Sicherung von Pässen und Reisedokumenten[136] nur mittelbar gegeben. Derzeit untersucht eine Arbeitsgruppe der ICAO[137] die Ergänzung von maschinenlesbaren Ausweisen um biometrische Merkmale.[138] Ob diese Ergänzungen Eingang in die ICAO-Dokumente 9303 finden, ist derzeit nicht abzusehen.

---

[130] Vgl. *Weichert*, DuD 2002, 423 (425).
[131] ICAO-Standard ICAO-DOC 9303, zugleich ISO 7501.
[132] IntZLuftAbk, Ratifizierung mit Gesetz vom 7.4.1956, BGBL II 1956, S. 412, letzte ratifizierte Änderung vom 10. Mai 1984 geändert durch BGBl. 1996 II S. 210, 1999 II S. 307.
[133] EU-Entschließung 2000/C310/01, Anhang II.
[134] Passgesetz vom 19. April 1986 (BGBl. I, S. 537).
[135] Artikel 1 Abs. 3 des Gesetzes zur Änderung des Pass- und Personalausweisrechts, BGBl. I 2000 vom 10.05.2000, S. 626.
[136] EU-Entschließung 2000/C310/01, Anhang II.
[137] Technical Advisory Group on Machine Readable Travel Documents (TAG-MRTD).
[138] Exekutive Summary of the Technical Report on ICAO Work on Selection and Testing of a Biometric Technology for Identity Confirmation with Machine Readable Travel Documents (MRTDS), (abrufbar unter http://www.icao.int/icao/en/atb/fal/mrtd/biometric_tech.htm).

2.2.2.4 Folgerungen

Das Recht der Europäischen Union und das Völkerrecht begründen Vorgaben, die weitgehend den deutschen verfassungsrechtlichen Rahmenbedingungen für die Verarbeitung personenbezogener Daten entsprechen. Einschränkungen des gemäß Art. 8 EMRK garantierten Menschenrechts auf Schutz des Privatlebens müssen insbesondere durch eine gesetzliche Grundlage legitimiert sein.
Für den Einsatz biometrischer Verfahren existieren konkrete europarechtliche Vorgaben. Jedoch lassen sich den Regelungen keine spezifischen Anforderungen für den nationalen Gesetzgeber entnehmen, die bei der Ausgestaltung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie „Ausländerausweise" zu erfüllen wären. Europarechtliche Vorschriften verpflichten den nationalen Gesetzgeber insbesondere nicht zur Aufnahme biometrischer Merkmale in entsprechende Dokumente, noch regeln sie die dabei gegebenenfalls zu beachtenden Einzelheiten.

3 Regelungen zum Einsatz biometrischer Verfahren im Terrorismusbekämpfungsgesetz

Mit dem Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002[139] wurden insgesamt Vorschriften in 21 Gesetzen und Rechtsverordnungen geändert bzw. neu geschaffen. Nach den Terroranschlägen vom 11. September 2001 sah sich der Gesetzgeber veranlasst, zahlreiche Vorschriften zu erlassen, mit deren Hilfe u.a. die Kompetenzen der Sicherheitsbehörden erweitert, der Datenaustausch zwischen den Behörden erleichtert sowie die Aufnahme biometrischer Merkmale in Pässe und Personalausweise sowie in „Ausländerausweise" geregelt wurden. Die letzt genannten Regelungen zur Aufnahme biometrischer Merkmale in Pässe und Personalausweise von Bundesbürgern sowie in Ausländerpapiere bilden den zentralen Gegenstand der nachfolgenden Ausführungen.

Nach der Begründung zum Gesetzentwurf der Bundesregierung liegt der Schwerpunkt des Entwurfs bei der Schaffung der notwendigen gesetzlichen Voraussetzungen für eine Verbesserung des Informationsaustausches, bei der Verhinderung der Einreise terroristischer Straftäter nach Deutschland und den notwendigen identitätssichernden Maßnahmen.[140] Ohne an dieser Stelle eine Bewertung der Inhalte der gesamten mit dem Terrorismusbekämpfungsgesetz neu geschaffenen und geänderten Vorschriften vornehmen zu können, so lässt sich doch

[139] BGBl. I 2002, S. 361.

sagen, dass es Anhaltspunkte gibt, dass das Terrorismusbekämpfungsgesetz über das Ziel einer angemessenen und zielorientierten Reaktion auf die Terroranschläge vom 11. September 2001 hinausgeht. So führt die Verschärfung der Sicherheitsgesetze dazu, dass Polizei und Geheimdiensten neue Befugnisse eingeräumt werden, die sensible Bereiche des Rechtsstaates wie die föderale Struktur der Polizei, die Trennung von Polizei und Geheimdiensten sowie die Unterscheidung von Strafverfolgung und Gefahrenabwehr berühren. Auch die Frage, welchen Sicherheitsgewinn die vielen Antiterrorgesetze der vergangenen 20 Jahre gebracht haben, wurde nicht beantwortet, ebenso wenig wurden Vollzugsdefizite bei den deutschen Sicherheitsbehörden analysiert.[141]

Gegenstand der vorliegenden Darstellung sind in erster Linie die mit dem Terrorismusbekämpfungsgesetz geschaffenen Regelungen, die die Aufnahme biometrischer Merkmale in Identifikationspapiere von Bundesbürgern und von Ausländern vorsehen.

Nach dem Willen des Gesetzgebers sollen im Pass- und Personalausweisrecht die Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente verbessert werden, u.a. um zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Aus diesem Grunde sieht der Gesetzentwurf im Wesentlichen vor, dass neben dem Lichtbild und der Unterschrift weitere Merkmale in den Pass und Personalausweis – auch in verschlüsselter Form – aufgenommen werden dürften.[142]

Der Gesetzgeber hat sich nicht darauf beschränkt, die Aufnahme biometrischer Merkmale in Pässe und Personalausweise für Bundesbürger vorzusehen, sondern er hat gleichzeitig auch neue Vorschriften im AuslG und AsylVfG geschaffen, die die Aufnahme derartiger Merkmale auch in die Identifikationspapiere von Ausländern und Asylbewerbern ermöglichen.

Nachfolgend werden die die Aufnahme biometrischer Merkmale regelnden Vorschriften zunächst in ihrem Inhalt dargestellt und bewertet. In diesem Zusammenhang werden auch die Unterschiede der Regelungen zu biometrischen Merkmalen von Bundesbürgern sowie von Ausländern und Asylbewerbern aufgezeigt. In einem nächsten Schritt sollen die datenschutzrechtlichen Anforderungen an die für die Aufnahme biometrischer Merkmale noch erforderlichen Ausführungsvorschriften dargestellt werden.

---

[140] BR-Drucks. 920/01, S. 82.

[141] *Lamprecht*, SZ 19./20. Januar 2002, S. III; *Nolte,* DVBl. 2002, 573ff.; zum Bereich des Ausländerrechts *Huber*, NVwZ 2002, 787ff.

3.1 Inhalt und Zweck der Aufnahme biometrischer Merkmale in Identifikationspapiere für Bundesbürger

Zurzeit enthalten Pässe und Personalausweise für Bundesbürger neben persönlichen Angaben wie Namen, Geburtsdatum und Unterschrift auch biometrische Angaben, deren automatisierte Auswertung nicht vorgesehen ist. Es handelt sich hierbei um Angaben zur Größe und Augenfarbe sowie um ein Bild des Inhabers. Diese Daten liegen als Kopie dezentral bei der ausstellenden Behörde in einem Register vor. Auskunft über die in dem Register gespeicherten Daten sind nur in dem gesetzlich definierten Umfang möglich.

Die Passbehörden führen Passregister (§ 21 Abs. 1 PassG), in denen die in § 21 Abs. 2 PassG aufgeführten Daten enthalten sind (u.a. Familienname und ggf. Geburtsname; Vornamen; Doktorgrad; Ordensname/Künstlername; Tag und Ort der Geburt; Geschlecht; Größe, Farbe der Augen; gegenwärtige Anschrift; Staatsangehörigkeit; Seriennummer; Gültigkeitsdatum). Die Passbehörden dürfen Daten aus dem Passregister anderen Behörden auf deren Ersuchen unter bestimmten in § 22 Abs. 2 Nr. 1 bis 3 PassG genannten Voraussetzungen übermitteln. Eine Datenübermittlung ist danach z.B. zulässig, wenn ein gesondertes Gesetz oder eine Rechtsverordnung die Übermittlung erlaubt.

Für Personalausweise werden von den Personalausweisbehörden Personalausweisregister geführt (§ 2a Abs. 1 PAuswG). Gemäß § 2b PAuswG dürfen Personalausweisbehörden personenbezogene Daten aus dem Personalausweisregister an andere Behörden übermitteln. Diese Datenübermittlungen sind jedoch lediglich unter den in § 2b Abs. 2 Satz 2 genannten Voraussetzungen zulässig. Diese entsprechen den im PassG geregelten Voraussetzungen.

Es ist darauf hinzuweisen, dass weder das Pass- noch das Personalausweisregister als Auskunftsregister ausgestaltet ist und Auskünfte lediglich in einem sehr begrenzten Umfang unter restriktiven Voraussetzungen zulässig sind. Im Gegensatz zu diesen Registern sind Auskünfte aus den Melderegistern in einem höheren Umfang möglich. Das Melderechtsrahmengesetz (MRRG) enthält einen eigenen Abschnitt 4 (§§ 17ff.), der Datenübermittlungen an andere Stellen sowie Auskunftsrechte von Bürgerinnen und Bürgern regelt.

Mit Erlass des Terrorismusbekämpfungsgesetzes wurden im Pass- und Personalausweisgesetz Regelungen geschaffen, die neben dem Lichtbild und der Unterschrift die Aufnahme weiterer

---

[142] BR-Drucks. 920/01, S. 84.

biometrischer Merkmale von Fingern oder Händen oder Gesicht in Pässe und Personalausweise erlauben. Ein noch zu erlassendes Ausführungsgesetz muss u.a. die Arten der biometrischen Merkmale, ihre Einzelheiten, die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung noch gesondert regeln (vgl. § 4 Abs. 4 PassG bzw. § 1 Abs. 5 PAuswG).

3.1.1 Artikel 7 Terrorismusbekämpfungsgesetz (Änderung des Passgesetzes)

Durch Artikel 7 des Terrorismusbekämpfungsgesetzes wurden u.a. § 4 PassG zwei neue Absätze hinzugefügt. § 4 Abs. 3 PassG lautet nunmehr: *„Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Auch die in Absatz 1 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden."* Bei letzteren Angaben über die Person handelt es sich um Familienname und ggf. Geburtsname (Nr. 1), Vornamen (Nr. 2), Doktorgrad (Nr. 3), Ordensname/Künstlername (Nr. 4), Tag und Ort der Geburt (Nr. 5), Geschlecht (Nr. 6), Größe (Nr. 7), Farbe der Augen (Nr. 8), Wohnort (Nr. 9), Staatsangehörigkeit (Nr. 10).

Der ebenfalls neu formulierte § 4 Abs. 4 PassG lautet: *„Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen sowie Angaben in verschlüsselter Form nach Absatz 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet."*

Nach der Begründung zum Gesetzentwurf kann künftig eines von drei bereits alternativ festgelegten Biometriemerkmalen eingeführt und dessen Verschlüsselung sowie die Verschlüsselung des Lichtbildes, der Unterschrift und anderer Personalangaben durch besonderes Bundesgesetz eingeführt werden. Zukünftig könne damit zweifelsfrei überprüft werden, ob die Identität der betreffenden Person mit den im Dokument abgespeicherten Originaldaten übereinstimme.[143] Hauptziel der Änderungen im PassG und im PAuswG ist es , die zweifelsfreie Identifizierung der Inhaber dieser Ausweisdokumente zu verbessern.

[143] BR-Drucks. 920/01, S. 84.

In der Gesetzesbegründung wird ausgeführt, die Zuverlässigkeit der Identifizierung einer Person allein durch den visuellen Abgleich zwischen Lichtbild und Person sei von der subjektiven Wahrnehmungsfähigkeit abhängig und werde auch durch zahlreiche andere Faktoren, wie z.B. die Qualität des Lichtbildes, den natürlichen Alterungsprozess, Veränderung von Haar- und Barttracht usw. beeinträchtigt. Die Aufnahme weiterer biometrischer Merkmale sei daher Voraussetzung für eine Verbesserung der Identifizierungsmöglichkeiten einer Person anhand des vorgelegten Ausweisdokumentes.[144]

Gemäß § 16 Abs. 1 Satz 1 PassG a.F. durfte der Pass bislang weder Fingerabdrücke noch verschlüsselte Angaben über die Person des Inhabers enthalten. So lautete die Vorschrift: *„Der Pass darf weder Fingerabdrücke noch verschlüsselte Angaben über die Person des Inhabers enthalten.“* Hintergrund dieser Vorschrift, deren Entsprechung für Personalausweise bislang in § 3 Abs. 1 Satz 1 PAuswG enthalten war, war die Forderung, dass weder Pässe noch Personalausweise Informationen enthalten dürfen, die nicht für jeden Inhaber lesbar und verständlich sind.[145] Mit der Schaffung der Möglichkeit zur Aufnahme biometrischer Merkmale und deren verschlüsselter Einbringung in den Pass durch das Terrorismusbekämpfungsgesetz war es notwendig, diese Vorschrift zu ändern.

Um datenschutzrechtlichen Belangen gerecht zu werden, hat der Gesetzgeber eine weitere Vorschrift in § 16 Abs. 6 PassG aufgenommen, die regelt, dass die im Pass enthaltenen verschlüsselten Angaben nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden dürfen. Außerdem wird ein Recht des Passinhabers auf Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben gegenüber der Passbehörde normiert.

3.1.2 Artikel 8 Terrorismusbekämpfungsgesetz (Änderung des Gesetzes über Personalausweise)

Inhaltlich entsprechen die in § 1 Abs. 4 und 5 PAuswG neu aufgenommenen Regelungen § 4 Abs. 3 und 4 PassG. In der Gesetzesbegründung wird hierzu ausgeführt, der beabsichtigte umfassende Schutz vor Identitätsmanipulationen mit Reisedokumenten werde nur erreicht, wenn nicht nur der Pass, sondern auch der Personalausweis, der von vielen europäischen

[144] BR-Drucks. 920/01, S. 110.
[145] Siehe Beschlussempfehlung und Bericht des Innenausschusses zum Entwurf eines Gesetzes zur Änderung des Gesetzes über Personalausweise, BT-Drucks. 8/3498, S. 9.

Staaten als Reisedokument anerkannt werde, die gleiche Absicherung habe wie der Pass.[146] Der Inhalt der Gesetzesbegründung entspricht inhaltlich der Begründung zu den geänderten Vorschriften im PassG, auf die an dieser Stelle verwiesen werden kann.

Die datenschutzrechtlichen Bestimmungen finden sich in § 3 PAuswG. Eine dem oben erwähnten § 16 Abs. 6 gleich lautende Regelung über die Verwendungszwecke verschlüsselter Merkmale und der Auskunftsrechte der Betroffenen enthält § 3 Abs. 5 PAuswG. Inhaltlich kann ebenfalls auf die obigen Ausführungen zum PassG verwiesen werden.

3.2 Biometrische Merkmale in „Ausländerausweisen“

Während das Ausländer- und Asylverfahrensrecht bislang keine Vorschriften darüber enthielt, in welcher Form Aufenthaltstitel auszugestalten sind, wurden nunmehr mit dem Terrorismusbekämpfungsgesetz Regelungen geschaffen, die konkrete Vorgaben enthalten. In die für Ausländer auszustellenden Dokumente können wie in die Identifikationspapiere für Bundesbürger ebenfalls biometrische Merkmale aufgenommen werden.

3.2.1 Artikel 11 Terrorismusbekämpfungsgesetz (Änderung des Ausländergesetzes)

Das Ausländerrecht sieht verschiedene Arten von Aufenthaltstiteln vor. Eine wichtige Bedeutung kommt § 5 AuslG zu. In dieser Vorschrift werden die Formen, in denen eine Aufenthaltsgenehmigung erteilt werden kann, geregelt. Hierbei handelt es sich um insgesamt vier Arten von Aufenthaltsgenehmigungen (Aufenthaltserlaubnis [§§ 15, 17]; Aufenthaltsberechtigung [§ 27]; Aufenthaltsbewilligung [§§ 28, 29]; Aufenthaltsbefugnis [§ 30]). Die Arten der Aufenthaltsgenehmigung unterscheiden sich nach Dauer und/oder Zweck des jeweiligen Aufenthalts. Die Aufenthaltsgenehmigung stellt die Entscheidung der Ausländerbehörde, durch die einem Ausländer mit konstitutiver Wirkung der Aufenthalt im Geltungsbereich des Ausländergesetzes erlaubt wird, dar. Die Aufenthaltsgenehmigung selbst zählt allerdings nicht zu den Aufenthaltstiteln, sondern bildet den zusammenfassenden Oberbegriff für die in § 5 AuslG aufgeführten Titel.[147]

Durch das Terrorismusbekämpfungsgesetz wurde die bislang aus einem Absatz bestehende Vorschrift des § 5 AuslG um sechs weitere Absätze ergänzt. Während das AuslG bisher die Gestaltung von Aufenthaltstiteln nicht regelte, wird nunmehr durch die Ergänzung der Vor

[146] BR-Drucks. 920/01, S. 112.
[147] GK-AuslR II-Komment. § 5 Rn. 3, 5.

schrift ein einheitliches Vordruckmuster für die Aufenthaltsgenehmigung vorgesehen. Auf diese Weise wird ein Dokument bzw. Vordruck über die Aufenthaltsgenehmigung eingeführt, mit dem eine Vielzahl identifizierender Merkmale aufgenommen wird. Hierbei kann die Aufenthaltsgenehmigung wie bisher als Klebeetikett in den Pass oder das Passersatzpapier des Ausländers eingeklebt werden (§ 5 Abs. 2 AuslG) oder aber als eigenständiges Dokument ausgestellt werden (§ 5 Abs. 3 AuslG). In beiden Fällen kann die Aufenthaltsgenehmigung gemäß § 5 Abs. 4 AuslG neben dem Lichtbild und der eigenhändigen Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten, wobei die Merkmale auch in mit Sicherheitsverfahren verschlüsselter Form in die Aufenthaltsgenehmigung eingebracht werden dürfen. In ihrem Inhalt entspricht die Vorschrift insoweit § 4 Abs. 3 PassG bzw. § 1 Abs. 4 PAuswG.

Die Aufnahme biometrischer Merkmale ist nicht nur für die Aufenthaltsgenehmigung vorgesehen. Vielmehr sollen diese auch in die unterschiedlichen, nach einheitlichem Muster gestalteten „Ausländerausweise“ aufgenommen werden können. Hierbei handelt es sich um den Ausweisersatz (§ 39 Abs. 1 AuslG), die Duldungsbescheinigung (§ 56a AuslG) sowie die Fiktionsbescheinigung (§ 69 Abs. 2 AuslG).

Neben der Aufnahme biometrischer Merkmale in die genannten Dokumente sieht § 5 Abs. 2 AuslG auch vor, dass die Aufenthaltsgenehmigung eine Zone für das automatische Lesen enthält. Diese Zone enthält zahlreiche identifizierende Merkmale, wie u.a. Familienname, Geburtsdatum, Geschlecht, Staatsangehörigkeit. Die in dieser Zone enthaltenen Daten können alle öffentlichen Stellen „zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen“ (§ 5 Abs. 7 AuslG). Nach der Gesetzesbegründung ist das Speichern der Daten erforderlich, um maschinelle Datenabgleiche durchführen zu können.[148] Aus datenschutzrechtlicher Sicht handelt es sich bei dieser pauschalen Datenverarbeitungsbefugnis für alle öffentlichen Stellen um eine Vorschrift, die dem verfassungsrechtlichen Bestimmtheitsgebot nicht genügt. Die einzige Einschränkung auf die Erforderlichkeit der Datenverarbeitung „zur Erfüllung der gesetzlichen Aufgaben“ ist unter datenschutzrechtlichen Gesichtspunkten als nicht ausreichend anzusehen.[149] Die Einräumung der generellen Befugnis, maschinelle Datenabgleiche durchzuführen, steht mit den verfassungsrechtlichen Vorgaben zur informationellen

[148] BR-Drucks. 920/01, S. 127.
[149] Stellungnahme der Deutschen Vereinigung für Datenschutz vom 15.11.2001: Terrorismusbekämpfungsgesetz und Ausländer.

Gewaltenteilung und zur Zweckbindung nicht in Einklang.[150] Die Vorschrift des § 5 Abs. 5 und 7 AuslG wird auch für den Ausweisersatz, die Duldungsbescheinigung und die Fiktionsbescheinigung, die ebenfalls eine Zone für das automatische Lesen enthalten sollen, für entsprechend anwendbar erklärt. Die vorstehenden Ausführungen gelten daher auch für diese Vorschriften.

Wie bereits erwähnt, besteht ein wesentlicher Unterschied zwischen den Regelungen über die Aufnahme biometrischer Merkmale in Ausweisen für Bundesbürger und in „Ausländerausweisen" darin, dass die Vorschriften im PassG und PAuswG noch durch ein Ausführungsgesetz konkretisiert werden müssen, während im AuslG und AsylVfG eine Rechtsverordnung für ausreichend erachtet wird. Diese Unterscheidung ist aus verfassungsrechtlicher Sicht durchaus kritikwürdig und wird in Abschnitt 4.1 näher problematisiert.

3.2.2 Artikel 12 Terrorismusbekämpfungsgesetz (Änderung des Asylverfahrensgesetzes)

Da § 63 Abs. 2 AsylVfG auf die Geltung des § 56a AuslG verweist, können biometrische Merkmale auch auf die Bescheinigung über die Aufenthaltsgestattung von Asylbewerbern aufgenommen werden. Die Vordruckmuster und Ausstellungsmodalitäten sind ebenfalls vom Bundesministerium des Innern durch Rechtsverordnung zu bestimmen.

4 Datenschutzrechtliche Anforderungen an die Umsetzung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Regelungen zum Einsatz biometrischer Verfahren

Um eine Bewertung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Ermächtigungsgrundlagen für die Aufnahme biometrischer Merkmale aus datenschutzrechtlicher Sicht vornehmen zu können, muss in erster Linie geprüft werden, ob die Maßnahmen zur Aufnahme biometrischer Merkmale dem Grundsatz der Verhältnismäßigkeit entsprechen, d.h. geeignet, erforderlich und angemessen sind. Zu diesem Zweck werden die vom Gesetzgeber in den einzelnen Vorschriften geregelten inhaltlichen Vorgaben für die Aufnahme biometrischer Merkmale im Folgenden dargestellt und in ihren datenschutzrechtlichen Kontext eingebettet. In diesem Zusammenhang werden auch die mit dem flächendeckenden Einsatz biometrischer Verfahren verbundenen Risiken für das Recht auf informationelle Selbstbestimmung der Betroffenen dargestellt. Dabei werden die Defizite der gesetzlichen Regelungen benannt und Lösungsmöglichkeiten aufgezeigt. Anhand verschiedener denkbarer Einsatzszenarien der

[150] *Weichert*, DuD 2002, 423 (425).

Aufnahme biometrischer Merkmale werden sodann Vorschläge für die praktische Umsetzung der vom Gesetzgeber geschaffenen Vorschriften gemacht.

4.1 Unterschiedliche Behandlung von Bundesbürgern und Ausländern bei Erlass der notwendigen Ausführungsbestimmungen

Sowohl die Ermächtigungsgrundlagen im PassG und PAuswG als auch im AuslG und AsylVfG erlauben zwar die Aufnahme biometrischer Merkmale, überlassen die nähere Ausgestaltung jedoch einem Bundesgesetz bzw. für Ausländer einer Rechtsverordnung gemäß Art. 80 Abs. 1 Satz 2 GG. Insbesondere enthält die gesetzliche Regelung keine Vorgaben über die Modalitäten der Aufnahme biometrischer Merkmale in die jeweiligen Dokumente. Im Folgenden gilt es, die aus der vom Gesetzgeber vorgenommenen Unterscheidung zwischen Bundesbürgern und Ausländern folgenden rechtlichen Konsequenzen aufzuzeigen.

Im Unterschied zu den Identifikationspapieren für deutsche Bundesbürger bedarf es zur Einführung der Ausweise für Ausländer nicht eines Ausführungsgesetzes, sondern lediglich einer Rechtsverordnung. Gemäß § 5 Abs. 6 AuslG handelt es sich um eine Rechtsverordnung des Bundesministeriums des Innern, die der Zustimmung des Bundesrates bedarf. Die verfassungsrechtlichen Anforderungen, die an das Ermächtigungsgesetz zu stellen sind, ergeben sich aus Art. 80 GG. Nach dieser Vorschrift müssen Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden (Art. 80 Abs. 1 Satz 2 GG). Das Bundesverfassungsgericht hat verschiedene Formeln entwickelt, die zur Auslegung der Vorschrift heranzuziehen sind, die sich allerdings nur schwer systematisieren lassen.[151] Bei der Auslegung sind insbesondere drei maßgebliche Gesichtspunkte festzuhalten. Die wichtigste Kategorie stellt dabei der Zweck der Ermächtigung dar, da Inhalt und Ausmaß sich gut erschließen lassen, wenn der Zweck bestimmt ist. Zu beachten ist außerdem, dass es bei der Auslegung auch auf die Eingriffsintensität ankommt. Je schwerwiegender die Auswirkungen sind, desto höhere Anforderungen sind insoweit an die Bestimmtheit der Ermächtigung zu stellen.[152] Sofern der Gesetzgeber im AuslG und im AsylVfG die Regelung der Einzelheiten der Aufnahme biometrischer Merkmale einer Rechtsverordnung überlässt, ist es im Hinblick auf die Anforderungen des Art. 80 Abs. 1 Satz 2 GG durchaus fraglich, ob die Zwecke ausreichend bestimmt sind, da eine inhaltliche Konkretisierung völlig fehlt.

---

[151] Zu den einzelnen Formeln *Jarass/Pieroth*, GG, Art. 80 Rn. 11; *Ramsauer*, in: AK-GG, Art. 80 Rn. 65, jeweils m.zahlreichen Rechtsprechungsnachweisen.

[152] *Jarass/Pieroth*, GG, Art. 80 Rn. 12 m.w. Rechtsprechungsnachweisen.

Von entscheidender Bedeutung ist allerdings ein weiterer Aspekt: Eingriffe in das Grundrecht auf informationelle Selbstbestimmung bedürfen nach der Rechtsprechung des Bundesverfassungsgerichts „einer (verfassungsgemäßen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht“.[153] Aus dieser Vorgabe des Bundesverfassungsgerichts lässt sich zwar nicht eindeutig die Forderung ableiten, dass Einschränkungen des Rechts auf informationelle Selbstbestimmung ausschließlich auf der Grundlage eines formellen Gesetzes erfolgen dürfen, dennoch müsste ein sachlicher Grund dargetan werden, der eine unterschiedliche Behandlung von Bundesbürgern und Ausländern rechtfertigt. In der Gesetzesbegründung wird ein Grund für die unterschiedliche Behandlung von Bundesbürgern und Ausländern auch an keiner Stelle angeführt. Angesichts der gleich lautenden Vorschriften zur Aufnahme biometrischer Merkmale im Pass- bzw. PersAuswG und dem AuslG bzw. AsylVfG ist es mit dem Gleichheitsgrundsatz nicht zu vereinbaren, für Bundesbürger ein formelles Gesetz zu fordern und für Ausländer eine Rechtsverordnung für ausreichend zu erachten.

Aus der sog. Wesentlichkeitsrechtsprechung des Bundesverfassungsgerichts[154] folgt, dass der Gesetzgeber verpflichtet ist, in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, alle wesentlichen Entscheidungen selbst zu treffen, soweit diese einer staatlichen Regelung zugänglich sind.[155] Alle für die Verwirklichung der Grundrechte wesentlichen Entscheidungen sind nach der Kernaussage der Wesentlichkeitstheorie dem Parlament vorbehalten. § 5 Abs. 6 AuslG überlässt die Regelung sämtlicher Modalitäten, wie z.B. die Wahl der biometrischen Merkmale, die Aufnahme und die Abspeicherung im Rahmen des Erstellungsvorgangs oder das Führen von Referenzdateien sowie die Nutzung dieser Daten der zu erlassenden Rechtsverordnung. Da mit der Aufnahme der biometrischen Merkmale sowie ihrer weiteren Speicherung, Verarbeitung und Nutzung in das auch für Ausländer geltende Recht auf informationelle Selbstbestimmung eingegriffen wird, ist es mit dem vom Bundesverfassungsgericht in seiner Rechtsprechung aufgestellten Verfassungsgrundsatz, nach dem alle wesentlichen Entscheidungen vom Parlament selbst zu regeln sind, nicht vereinbar,

---

[153] BVerfGE 65, 1 (44).
[154] Vgl. etwa BVerfGE 33, 1 (2ff.); 33, 303 (337ff.); 34, 52 (60); 34, 165 (192f.); 41, 251 (259ff.); 45, 400 (417); 47, 46 (78f.); 49, 89 (126f.); 57, 295 (320f.); 58, 257 (268).
[155] BVerfGE 49, 89 (126); 61, 260 (275); 77, 170 (230f.); vgl. auch *Jarass/Pieroth*, GG, Art. 20 Rn. 46 m. zahlr. w. Nachw.

die Ausgestaltung der Modalitäten der Aufnahme biometrischer Merkmale ohne nähere Präzisierung und Eingrenzung einer Rechtsverordnung zu überlassen.[156]

4.2 Anforderungen des Terrorismusbekämpfungsgesetzes an den Inhalt der Ausführungsbestimmungen

4.2.1 Gesetzliche Vorgaben des Terrorismusbekämpfungsgesetzes zu den Modalitäten der Aufnahme biometrischer Merkmale

Die mit dem Terrorismusbekämpfungsgesetz geschaffenen Vorschriften enthalten zwar inhaltliche Vorgaben, die jedoch der Konkretisierung bedürfen. Die Vorschriften im PassG, PAuswG sowie AuslG und AsylVfG unterscheiden sich in vielen Punkten nicht wesentlich. Vielmehr sind die mit dem Terrorismusbekämpfungsgesetz für das Ausführungsgesetz bzw. die Ausführungsverordnung geschaffenen Vorgaben zu den Arten der biometrischen Merkmale, der Einbringung dieser Daten in verschlüsselter Form sowie zur Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung inhaltlich gleich lautend. Insofern werden auch zwischen den Identifikationspapieren für Bundesbürger und den Ausweisen für Ausländer keine inhaltlichen Unterschiede gemacht. Im Folgenden gilt es, die vom Gesetzgeber nicht näher geregelten Vorgaben zu präzisieren und die an die Ausgestaltung zu stellenden datenschutzrechtlichen Anforderungen zu definieren. Hierbei wird die Rechtslage jeweils zunächst für Bundesbürger bewertet. Ergänzungen bzw. Abweichungen für Ausländer werden gegebenenfalls jeweils am Ende der Ausführungen dargestellt.

Es stellt sich in diesem Zusammenhang die grundsätzliche Frage, ob die Vorgaben des Terrorismusbekämpfungsgesetzes für den Gesetz- und Verordnungsgeber der Ausführungsbestimmungen bindend sind. Relevant ist diese Frage insbesondere bei der Beurteilung der Aufzählung der für die biometrischen Merkmale in Betracht kommenden Körperbereiche in den neu erlassenen Vorschriften des PassG und PAuswG bzw. AuslG und AsylVfG. Es ist in diesem Zusammenhang zwischen den Vorschriften für Bundesbürger und denen für Ausländer zu differenzieren. Grundsätzlich gilt hinsichtlich des Verhältnisses von Gesetzen die sog. lex posterior-Regelung, d.h. auf Grund der Gleichrangigkeit formeller Gesetze geht das später erlassene Gesetz dem älteren Gesetz vor (lex posterior derogat legi priori). Während das für den Bereich des Pass- und Personalausweiswesens erforderliche Ausführungsgesetz als Parlamentsgesetz auch über den bisherigen Regelungsinhalt der Vorschriften des Pass- und

[156] Siehe hierzu Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 22.

PAuswG hinausgehen kann, gilt dies für den Bereich des Ausländerwesens lediglich eingeschränkt. So darf der Inhalt der Rechtsverordnung über die Vorgaben des AuslG und des AsylVfG lediglich in den Grenzen der Wesentlichkeitstheorie hinausgehen, nach der wesentliche Entscheidungen vom Parlament zu treffen sind. Im Übrigen bedürfte es für diesen Bereich einer Novellierung der zugrunde liegenden Vorschriften im Rahmen eines förmlichen Gesetzgebungsverfahrens.

Im Rahmen der vorliegenden Darstellung erfolgt eine Beurteilung der mit dem Terrorismusbekämpfungsgesetz geschaffenen Vorschriften anhand der bestehenden Vorgaben des Gesetzgebers. In diesem Zusammenhang werden allerdings Defizite der gesetzlichen Vorgaben aufgezeigt.

4.2.1.1 Arten der biometrischen Merkmale und ihre Einzelheiten

4.2.1.1.1 Regelungen für Bundesbürger

Die Arten der biometrischen Merkmale und ihre Einzelheiten sind nach § 4 Abs. 4 Satz 1 PassG und § 1 Abs. 5 Satz 1 PAuswG durch ein Bundesgesetz zu regeln. Welche biometrischen Merkmale im Einzelnen gemeint sind, lässt sich den Vorschriften nicht entnehmen. Allerdings geben § 4 Abs. 3 Satz 1 PassG bzw. § 1 Abs. 4 Satz 1 PAuswG die Körperbereiche vor, auf die sich die biometrischen Merkmale beziehen können. So sollen „biometrische Merkmale von Fingern oder Händen oder Gesicht“ zulässig sein. Es erscheint bedenklich, dass der Gesetzgeber nicht geregelt hat, um welche Merkmale es sich im Einzelnen handeln soll.[157] Es stellt sich die Frage, ob die Auswahl des Gesetzgebers die genannten Merkmale alternativ oder kumulativ zulässt. Aus dem Wortlaut des Gesetzes ergibt sich eine Antwort nicht unmittelbar. Allerdings lässt sich der Gesetzesbegründung entnehmen, dass die drei genannten Körperbereiche nach dem Willen des Gesetzgebers alternativ zu verstehen sind.[158]

Die Nennung von Fingern, Händen und Gesicht ist abschließend. Biometrische Verfahren, die sich auf andere Körpermerkmale beziehen, scheiden von vornherein aus. Als in Betracht kommende biometrische Merkmale sind exemplarisch die Folgenden zu nennen: Finger- oder Handflächenabdruck, Handvenenmuster, Geometrie der Hand oder die Gesichtsgeometrie. Daneben können biometrische Systeme auf weiteren Merkmalen wie dem Irismuster (Muster der Regenbogenhaut) oder dem Retinamuster (Muster des Augenhintergrundes) als passiven

[157] *Nolte*, DVBl. 2002, 573 (576); *Roggan*, Handbuch der Inneren Sicherheit, S. 172.

biometrischen Merkmalen sowie der Stimme, Lippenbewegungen, der (Unter) Schrift sowie dem Tippverhalten auf einer Tastatur als aktiven biometrischen Merkmalen beruhen. Die durch das Terrorismusbekämpfungsgesetz geschaffenen Vorschriften führen die in Betracht kommenden Körperbereiche präzise auf, so dass hinsichtlich der davon umfassten Merkmale eine eher restriktive Auslegung vorzunehmen ist. So ist angesichts der ausdrücklichen Benennung sowohl der Hände als auch der Finger davon auszugehen, dass z.B. die Iriserkennung oder die Erkennung anhand des Retinamusters vom Körperbereich „Gesicht" wohl nicht mehr umfasst werden. Vielmehr ist davon auszugehen, dass der Gesetzgeber nicht lediglich die Bezeichnung „Gesicht" in das Gesetz aufgenommen hätte, wenn er auch diese biometrischen Merkmale hätte zulassen wollen.

Geht man davon aus, dass sich der Wille des Gesetzgebers darauf gerichtet hat, biometrische Merkmale lediglich der ausdrücklich genannten Körperbereiche und nur in alternativer Form zuzulassen, so stellt sich das Problem, dass die Beschränkung auf nur einen Körperbereich eine kombinierte Anwendung verschiedener biometrischer Systeme nicht zulässt. Dies wirft die Frage auf, ob die gesetzgeberische Beschränkung auf einzelne biometrische Merkmale überhaupt geeignet ist, den mit der Regelung erstrebten Zweck zu erreichen. Die Geeignetheit stellt einen Bestandteil des verfassungsrechtlichen Grundsatzes der Verhältnismäßigkeit dar. Das Gebot der Geeignetheit verlangt den Einsatz solcher Mittel, mit denen der gewünschte Erfolg gefördert werden kann, wobei ein Beitrag zur Zielerreichung ausreicht.[159] Zur Klärung dieser Frage ist zu prüfen, ob ein Verzicht auf eine Kombination mehrerer Merkmale unter dem Gesichtspunkt der Zuverlässigkeit biometrischer Systeme aus heutiger technischer Sicht überhaupt sinnvoll ist.

In diesem Zusammenhang ist eine Studie des National Institute of Standards and Technology (NIST)[160] des US-amerikanischen Handelsministeriums zu erwähnen. Wissenschaftler dieses Instituts empfehlen der US-Regierung nach Abschluss einer groß angelegten Studie, in der biometrische Erkennungsverfahren an sechs Grenzübergängen des Landes untersucht worden waren, für ein sicheres Verfahren zur Einreisekontrolle von Ausländern in die USA ein biometrisches System, das sowohl Merkmale des Gesichtes als auch der Fingerabdrücke erfasst. Ein derartiges System solle an allen 300 Einreisepunkten der USA eingesetzt werden. Im Auftrag des NIST wurden über mehrere Monate hinweg Papiere von Einreisenden mit

---

[158] BR-Drucks. 920/01, S. 110
[159] *Jarass/Pieroth*, GG, Art. 20 Rn. 84 mit zahlr. Hinweisen auf bundesverfassungsgerichtliche Rechtsprechung.
[160] http://www.nist.gov.

120.000 digitalisierten Lichtbilder und 600.000 Fingerabdrücken in Datenbeständen verglichen. Hierbei habe die Gesichtserkennung eine Erkennungsrate von 90 Prozent ergeben, die False-Acceptance-Rate habe bei einem Prozent gelegen. Bei den eingesetzten Fingerabdruck-Scannern habe eine Erkennungsquote von über 90 Prozent vorgelegen. Es ist nicht außer Acht zu lassen, dass bei Hochrechnung des Wertes von einem Prozent auf die Gesamtzahl der Visa trotz biometrischer Kontrolle jährlich rund 150.000 Personen von den Grenzbeamten über diese Methode nicht korrekt identifiziert werden. Der Direktor des NIST wies darauf hin, dass selbst eine Kombination aus Gesichtserkennung und Fingerabdruck-Scanning nicht zu einer hundertprozentig sicheren Kontrolle der Grenzen führen könne.[161] Dennoch empfiehlt das NIST den Einsatz eines dualen biometrischen Systems, das sowohl zwei Fingerabdrücke als auch eine Fotografie des Gesichtes umfasst.[162]

Im Ergebnis ist davon auszugehen, dass die Einschränkung des Gesetzgebers, lediglich biometrische Merkmale der genannten Körperbereiche alternativ zuzulassen, unter dem Aspekt der Falscherkennung bzw. Falschakzeptanz im Rahmen biometrischer Systeme problematisch ist. Wenn eine hohe Sicherheit nicht einmal mit einer Kombination verschiedener Merkmale zu erreichen ist, ist es zweifelhaft, ob die Beschränkung auf ein einziges biometrisches Merkmal eine Falschzurückweisungs- bzw. Falscherkennungsrate gewährleisten kann, die in den geplanten Einsatzbereichen akzeptiert werden kann. Die vom Gesetzgeber vorgesehene Alternativität der genannten Körperbereiche schränkt des Weiteren die in Betracht kommenden Systeme ein. Die Entscheidung für bestimmte Körperbereiche begrenzt ebenfalls die in Betracht kommenden Verfahren. So wird z.B. ein auf der Iris-Erkennung basierendes biometrisches Grenzkontrollsystem, wie es in den Vereinigten Arabischen Emiraten erstmals flächendeckend eingesetzt wird[163], vom Wortlaut des Gesetzes nach dem Willen des Gesetzgebers wohl nicht abgedeckt.

Der Gesetzgeber hat im Rahmen des Terrorismusbekämpfungsgesetzes keine Entscheidung darüber getroffen, welche biometrischen Merkmale im Einzelnen zum Einsatz kommen sollen. Es ist daher bei Erlass des Bundesgesetzes bzw. für den Bereich des Ausländerrechts der

---

[161] Meldung bei Heise Online vom 12.02.2003 (abrufbar unter: http://www.heise.de/newsticker/data/pmz-12.02.03-001/); Pressemitteilung des NIST vom 11.02.2003 (abrufbar unter: http://www.nist.gov/public_affairs/releases/n03-01.htm).

[162] NIST standards for biometric accuracy, tamper resistance, and interoperability. November 13, 2002; S. 21 (abrufbar unter: http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf).

[163] Meldung bei Heise Online vom 07.04.2003 (abrufbar unter: http://www.heise.de/newsticker/data/pmz-07.04.03-000/).

Rechtsverordnung ein besonderes Augenmerk darauf zu richten, die mit der Auswahl bestimmter biometrischer Merkmale verbundenen Folgen zu berücksichtigen.

So stellt sich bei der Aufnahme biometrischer Merkmale z.B. ein Problem im Hinblick auf die Gültigkeitsdauer von Pässen und Ausweisen. Die Gültigkeitsdauer dieser Dokumente ist gesetzlich bestimmt. Die Gültigkeitsdauer von Pässen beträgt gemäß § 5 Abs. 1 PassG zehn Jahre. Für Personen, die das 26. Lebensjahr noch nicht vollendet haben, beträgt die Gültigkeitsdauer fünf Jahre. Gesetzgeberisches Motiv dieser Entscheidung für eine kürzere Gültigkeitsdauer bei diesen Personengruppen war, dass die körperliche Entwicklung dieser Personen in diesem Alter noch nicht abgeschlossen ist. Dieses bedingt wiederum eine schnelle Änderung des persönlichkeitstypischen Erscheinungsbildes, was zur Folge hat, dass das im Reisepass befindliche Bild bereits nach wenigen Jahren eine zuverlässige Identifizierung des Passinhabers nicht mehr gewährleistet.[164] Gleiches gilt für Personalausweisinhaber, die das 26. Lebensjahr noch nicht vollendet haben (§ 2 Abs. 1 Satz 2 PAuswG). Auch die automatisierten Verfahren zur Gesichtserkennung weisen bei jüngeren Personen höhere Fehlerquoten als bei älteren Personen auf. [165] Bei der Aufnahme biometrischer Merkmale stellt sich ein ähnliches Problem, das sich jedoch nicht auf eine bestimmte Altersgruppe beschränken lässt. Vielmehr können biometrische Merkmale Änderungen unterworfen sein, die dazu führen können, dass eine Verifikation auf Grund dieses Merkmals lediglich in einem begrenzten Zeitraum möglich ist. Bei der Auswahl eines bestimmten biometrischen Merkmals ist darauf zu achten, dass eine Verifikation über den gesamten Gültigkeitszeitraum des entsprechenden Dokumentes sichergestellt werden kann. Biometrische Merkmale werden es daher erfordern, dass die Gültigkeitsdauer des entsprechenden Dokumentes angeglichen werden muss. Die Frage, ob und inwieweit bestimmte biometrische Merkmale eine Verifikation über einen Gültigkeitszeitraum von gegenwärtig zehn Jahren ermöglichen, bedarf einer eingehenden Untersuchung anhand der in Betracht kommenden biometrischen Systeme. Die Ergebnisse entsprechender Untersuchungen sind bei der gegebenenfalls erforderlich werdenden Neubestimmung des Gültigkeitszeitraums zu berücksichtigen. Bei der Definition der Anforderungen an ein biometrisches System bedarf es einer kritischen Bewertung, ob das System geeignet ist, die Verifikation über einen angemessenen Zeitraum hinweg zu ermöglichen. Eine Verkürzung der Gültigkeitsdauer von Pässen und Ausweisen wäre in der Praxis nämlich als sehr unpraktikabel anzusehen.

---

[164] *Medert/Süßmuth*, Paß- und Personalausweisrecht, Bd. 2, Erl. § 5 PaßG Rn. 3.

Verfassungsgemäß sind gesetzlich erlaubte Eingriffe nur, wenn weniger einschneidende Grundrechtseingriffe zur Zielerreichung nicht genügen. Insofern ist die Beschränkung auf die genannten biometrischen Merkmale verfassungsrechtlich in Frage zu stellen. Die Eingriffstiefe bestimmt sich nicht nur durch den verfolgten Zweck. Bei Eingriffen in das Recht auf informationelle Selbstbestimmung liegt u.a. eine größere Eingriffstiefe vor, wenn durch die Art der verarbeiteten Daten eine erleichterte Zweckänderungsmöglichkeit oder gar eine größere Missbrauchsgefahr besteht. Die gesetzlich vorgesehenen Merkmale Finger, Hände und Gesicht zeichnen sich dadurch aus, dass sie vom Besitzer unwillentlich hinterlassen werden können bzw. entgegen dessen Willen erhoben werden können. Dies ist bei anderen biometrischen Merkmalen wie z.B. der Erfassung der Retina oder der Iris nicht der Fall. Die Nutzung von biometrischen Merkmalen, deren Erfassung eine aktive Beteiligung des Betroffenen erfordern, reduziert auch die Möglichkeit einer zweckändernden Nutzung durch Abgleich mit an anderer Stelle ohne oder gegen den Willen des Betroffenen erfassten biometrischen Merkmalen (dazu näher unten Abschnitt 4.3.1.1.2). Gerade diese Merkmale hat der Gesetzgeber mit der expliziten Bezeichnung der in Betracht kommenden Körperbereiche aber wohl von den durch das Terrorismusbekämpfungsgesetz geschaffenen Vorschriften als nicht mitumfasst angesehen. Auch wenn die Merkmale aus oben genannten Gründen als datenschutzfreundlich erscheinen, so darf nicht außer Acht gelassen werden, dass diese Merkmale angesichts der mit ihnen enthaltenen überschießenden Zusatzinformationen ebenfalls datenschutzrechtliche Probleme aufwerfen (siehe dazu Abschnitt 4.3.1.1.2).

4.2.1.1.2 Regelungen für Ausländer

Für das AuslG und das AsylVfG kann im Wesentlichen auf die vorstehenden Ausführungen verwiesen werden. Da die entsprechenden Vorschriften inhaltlich gleich lautend sind, ergibt sich keine abweichende Beurteilung. Hinsichtlich der Problematik der Geeignetheit der biometrischen Merkmale zur Verifikation über den erforderlichen Gültigkeitszeitraum des Passes oder Personalausweises für Bundesbürger lässt sich für „Ausländerausweise“ eine Parallele ziehen. So existieren zwar Aufenthaltsgenehmigungen, die lediglich über einen kurzen Gültigkeitszeitraum verfügen (z.B. Aufenthaltsbewilligung gemäß § 28 AuslG, die in der Regel längstens für zwei Jahre erteilt wird). Andere Aufenthaltsgenehmigungen gelten jedoch auch unbefristet (z.B. Aufenthaltsberechtigung gemäß § 27 AuslG). Unter im AuslG näher geregelten Voraussetzungen kann die jeweilige Aufenthaltsgenehmigung verlängert werden. Es ist daher erforderlich, bei Schaffung der Rechtsverordnung die Geeignetheit der biometrischen

[165] FRVT 2002: Overview and Summary. Abb. 5, S. 7, Abb. 10, S. 12.

Merkmale zur dauerhaften Verifikation des Merkmalsinhabers sorgfältig zu prüfen und gegebenenfalls die Gültigkeitsdauer von „Ausländerausweisen“ anzupassen.

4.2.1.2 Einbringung von Merkmalen und Angaben in verschlüsselter Form

Gemäß § 4 Abs. 3 Satz 2 und 3 PassG sowie § 1 Abs. 4 Satz 2 und 3 PAuswG dürfen das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass oder Personalausweis eingebracht werden. Die Befugnis erstreckt sich auch auf die weiteren im Pass oder Personalausweis enthaltenen personenbezogenen Daten über den jeweiligen Inhaber. In der Begründung zum Gesetzentwurf wird ausgeführt, die Option, die biometrischen Merkmale auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass zu integrieren, ermögliche die zweifelsfreie Feststellung der Übereinstimmung der Identität des Passinhabers mit der Identität der zu kontrollierenden Person durch ein computergestütztes Verfahren.[166]

Es stellt sich die Frage, was Verschlüsselung im Sinne dieser Vorschrift bedeutet. Eine Auslegung des Begriffes anhand der Begründung zum Gesetzentwurf ist nicht möglich, da dort keinerlei Angaben und Hinweise enthalten sind.

Der Begriff Verschlüsselung könnte dahingehend interpretiert werden, dass die auf dem Pass oder Personalausweis enthaltenen Daten über den Inhaber des Dokumentes mittels des gewählten Verfahrens so unkenntlich gemacht werden, dass sie lediglich von Berechtigten, die im Besitz des Schlüssels sind, wieder gelesen werden könnten. Der Zweck der Verschlüsselung wäre also der Schutz vor unbefugter Kenntnisnahme. Um eine Verschlüsselung in diesem Sinne zu erreichen und zu gewährleisten, dass also die Daten tatsächlich nur von einem hierzu Berechtigten wieder entschlüsselt werden können, bedarf es eines Verschlüsselungsverfahrens, das wissenschaftlich anerkannt ist und nach dem Stand der Technik als sicher gilt. Bei den meisten der derzeit verwendeten Verfahren hängt die Sicherheit (u.a.) von der Länge des verwendeten Schlüssels ab. Bei der Bestimmung der ausreichenden Länge des Schlüssels ist die derzeitige und künftige Leistungsfähigkeit der Computertechnik zu beachten: Je größer die Leistungsfähigkeit, desto leichter können Verschlüsselungen mit Schlüsseln geringer Länge gebrochen werden.

---

[166] BR-Drucks. 920/01, S. 110.

Denkbar ist auch, dass mit dem Begriff „Verschlüsselung“ der Wunsch des Gesetzgebers zum Ausdruck gebracht werden sollte, biometrische Daten vor einer Verfälschung durch Unbefugte zu schützen. Dazu ist zwar eine Verschlüsselung im Sinne einer Unkenntlichmachung geeignet (denn nur die Berechtigten im Besitz des Schlüssels können beim Einbringen der biometrischen Daten in den Ausweis diese so verschlüsseln, dass nur Lese-Berechtigte sie entschlüsseln und auswerten können), vorteilhafter und moderner sind jedoch Public-Key – Signaturverfahren, wie sie im Rahmen der elektronischen Signatur nach dem deutschen Signaturgesetz zum Einsatz kommen: Diese ermöglichen einen Authentizitäts- und Integritätsnachweis, indem der Aussteller die biometrischen Daten um eine elektronische Signatur ergänzt, die nur er erzeugen kann (da nur er sich im Besitz des dazu verwendeten [Signaturerstellungs-]Schlüssels des Signaturverfahrens befindet). Die Prüfung der Signatur geschieht beim Lesen mit einem zweiten (Prüf)Schlüssel. Der Vorteil liegt darin begründet, dass mit dem Prüfschlüssel nur die Prüfung der Signatur, nicht aber deren Erstellung möglich ist. Daher kann der Prüfschlüssel öffentlich bekannt gemacht werden, ohne die Sicherheit des Verfahrens zu gefährden. Ähnlich wie bei der Verschlüsselung hängt die Sicherheit des Signaturverfahrens von der Länge der verwendeten Signaturschlüssel ab[167]. Im europäischen Bereich hat die EU bereits per Verordnung auf diesen Weg der Authentitätssicherung mithilfe der elektronischen Signatur hingewiesen.[168] Verschlüsselungs- und Signaturverfahren sind kombinierbar und können gleichzeitig Authentizität, Integrität und Vertraulichkeit der biometrischen Daten sicherstellen.

Auch an dieser Stelle stellt sich das in Abschnitt 4.2.1.1 bereits erörterte Problem des Gültigkeitszeitraums der Pässe und Personalausweise sowie der „Ausländerausweise“. Legt man den Gültigkeitszeitraum für Pässe und Personalausweise von derzeit fünf bis zehn Jahren zugrunde, so sind Verschlüsselungs- bzw. Signaturverfahren zu fordern, die mindestens für diesen Gültigkeitszeitraum als sicher gelten müssen.[169] An dieser Stelle ist auf § 14 Abs. 3 der Signaturverordnung (SigV)[170] hinzuweisen. Nach dieser Vorschrift dürfen qualifizierte Zertifikate höchstens fünf Jahre gelten. Entsprechende weitergehende Regelungen sind daher vom Gesetz- bzw. Verordnungsgeber zu schaffen. Da biometrische Merkmale dauerhaft personengebunden sind und daher die biometrischen Daten auch auf bereits nicht mehr gültigen Aus

[167] Siehe dazu die Amtlichen Veröffentlichung der Regulierungsbehörde für Telekommunikation und Post (RegTP) zu geeigneten Signaturalgorithmen gemäß Anlage 1Abschnitt 1 Nr. 2 Signaturverordnung (SigV), abrufbar unter: http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/03/index.html.
[168] EU-Entschließung 2000/C 310/01, Anhang I.
[169] Vgl. hierzu Positionspapier des AK Technik, März 2002.
[170] Verordnung zur elektronischen Signatur vom 16.11.2001, BGBl. I S. 3074.

weisen von Interesse für Unbefugte sein können, ist ein über die Gültigkeitsdauer hinausreichender Schutz durch Verschlüsselungsverfahren wünschenswert.

Im Bereich der „Ausländerausweise“ ist es problematisch, dass die einzelnen Aufenthaltstitel teilweise eine unterschiedliche Gültigkeitsdauer aufweisen. Betrachtet man die Aufenthaltsberechtigung gemäß § 27 AuslG, die unbefristet erteilt wird, so stellt sich das Problem, dass eine Prognose über eine dauerhaft als sicher geltende Schlüssellänge sehr schwierig ist. Der Gesetz- bzw. Verordnungsgeber ist daher aufzufordern, bei Erlass der Ausführungsbestimmungen ein besonderes Augenmerk darauf zu richten, den jeweiligen Gültigkeitszeitraum der in Rede stehenden Dokumente im Hinblick auf den für eine sichere Verschlüsselung erforderlichen Verschlüsselungsalgorithmus anzupassen.

Weiterhin ist fraglich, welche Stelle die Verschlüsselung/Signatur vornehmen soll. In Betracht kommen die jeweiligen örtlichen Pass- und Personalausweisbehörden oder aber die Bundesdruckerei oder eine andere öffentliche oder private zentrale Stelle. Da es für „Ausländerausweise“ in der zu erlassenden Rechtsverordnung einer Regelung der Ausstellungsmodalitäten bedarf, ist die für die Vornahme der Verschlüsselung bzw. Signatur zuständige Stelle zu benennen. In diesem Zusammenhang bedarf es des Weiteren der Regelung von Sicherheitsvorkehrungen, die eine Bekanntgabe der Entschlüsselungs- bzw. Signaturerstellungsschlüssel an Unbefugte verhindern.[171] Dies ist insbesondere zu beachten, wenn Verschlüsselungsverfahren zum Einsatz kommen, deren Ver- und Entschlüsselungsschlüssel gleich ist (sog. „symmetrische Verfahren“)[172]: Da jedes Prüf- bzw. Lesegerät für biometrische Ausweise diesen Schlüssel enthalten muss, besteht die Gefahr, dass durch den Diebstahl eines Gerätes der Schlüssel kompromittiert wird und der unrechtmäßige Besitzer in die Lage versetzt wird, selbst Verschlüsselungen vorzunehmen.

Denkbar ist schließlich auch, dass der Gesetzgeber mit der Wahl der Worte „*in verschlüsselter Form*“ lediglich zum Ausdruck bringen wollte, dass Daten in einer nicht unmittelbar mit den menschlichen Sinnen erfassbaren Form auf den Ausweispapieren aufgebracht werden können. Denkbar wären etwa Bar-Codes o. Ä., die lediglich eine andere technische Repräsentation der Daten darstellen, ohne durch Verschlüsselung oder Signatur zusätzlichen Schutz von Authentizität, Integrität oder Vertraulichkeit zu gewährleisten.

[171] Vgl. hierzu Positionspapier des AK Technik, März 2002.

Für die Betroffenen stellt sich ohne weitere Maßnahmen die Situation gleich dar: Auf ihren Ausweisen finden sich „unverständliche“ Daten, für deren Verständnis sie auf die Mithilfe der Behörde (etwa in Form eines Auskunftsverpflichtung nach § 16 Abs. 6 PassG bzw. § 3 Abs. 5 PAuswG) oder zumindest technischer Mittel angewiesen sind. Ob diese Daten signiert, verschlüsselt (im kryptographischen Sinn) oder lediglich codiert (mit einem öffentlich bekannten Code) vorliegen, kann der Betroffene im Einzelfall nicht entscheiden.

Da der Gesetzgeber mit der Formulierung „dürfen auch in mit Sicherheitsverfahren verschlüsselter Form [...] eingebracht werden“ eine Kann-Bestimmung geschaffen hat, ist es dem Gesetz- bzw. Verordnungsgeber freigestellt, die Verschlüsselung der Daten vorzusehen. Erfolgt dies nicht, so ist darauf hinzuweisen, dass es angesichts der Sensibilität biometrischer Daten in jedem Fall erforderlich ist, die bei der Aufnahme der biometrischen Merkmale gespeicherten Werte gegen Missbrauch zu sichern.

4.2.1.3 Art ihrer Speicherung und sonstigen Verarbeitung und ihrer Nutzung

Der Gesetzgeber hat die Regelung der Aufnahme biometrischer Merkmale „die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung“ für Pässe und Personalausweise einem Bundesgesetz überlassen. Eine Einschränkung wurde lediglich dahingehend aufgenommen, dass eine bundesweite Datei für Bundesbürger nicht eingerichtet wird (§ 4 Abs. 4 Satz 2 PassG, § 1 Abs. 5 Satz 2 PAuswG). Zudem enthalten § 16 Abs. 6 PassG und § 3 Abs. 5 PAuswG Vorgaben dahingehend, dass die im Pass oder Personalausweis gespeicherten Angaben nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung[173] des Pass- oder Personalausweisinhabers ausgelesen werden dürfen. Insoweit legt der Gesetzgeber im Rahmen dieser Vorschriften bereits fest, für welche Zwecke die Daten verwendet werden dürfen. Die Zulässigkeit einer über diesen Zweck hinausgehenden Verarbeitung und Nutzung der Daten wäre angesichts der bestehenden gesetzlichen Regelung nicht gegeben.

Es ist wohl davon auszugehen, dass der Gesetzgeber mit der Formulierung in § 4 Abs. 4 Satz 1 PassG bzw. § 1 Abs. 4 Satz 1 PAuswG die technischen Modalitäten der Speicherung, Verarbeitung und Nutzung gemeint hat. Welche Anforderungen an die Regelung dieser Modalitäten zu stellen sind, wird unten in Abschnitt 4.3 näher erörtert.

---

[172] Siehe z.B. *Schneier,* Angewandte Kryptographie, Kapitel 2.2.

[173] Es ist davon auszugehen, dass der Gesetzgeber den Begriff „Identitätsprüfung“ fälschlich gewählt hat und damit die Echtheits- und Authentizitätsprüfung gemeint hat; siehe hierzu *Garstka*, Neue Justiz 2002, 524 (525).

Während der Gesetzgeber für Bundesbürger eine Einschränkung der Verwendungszwecke der biometrischen Daten in die entsprechenden Regelungen aufgenommen hat, fehlen derartige Regelungen für die biometrischen Merkmale auf „Ausländerausweisen“. Welche Konsequenzen sich hieraus für Ausländer ergeben, wird ebenfalls in Abschnitt 4.3 näher erörtert.

4.2.2 Weitere Vorgaben des Gesetzgebers

4.2.2.1 Verbot der Einrichtung einer bundesweiten Datei für Bundesbürger

Das PassG und das PAuswG regeln, dass eine bundesweite Datei, in der die biometrischen Merkmale gespeichert werden, nicht eingerichtet wird.[174] Diese Regelung war in dem Gesetzentwurf zunächst nicht enthalten. Vielmehr wurde sie erst auf Grund des Änderungsantrages der Fraktionen SPD und BÜNDNIS 90/ DIE GRÜNEN vom 11.12.2001 eingefügt. Dort heißt es zur Begründung: „Die Einrichtung einer bundesweiten Datei ist nicht vorgesehen. Dies gilt in gleicher Weise für eine länderübergreifende Vernetzung der lokalen Register.“[175] Vorher hatte der Bundesbeauftragte für Datenschutz in seiner Stellungnahme vom 23.10.2001 bereits darauf hingewiesen, dass zur Klarstellung ausdrücklich normiert werden sollte, dass eine solche Datei nicht eingerichtet werden dürfe, weil ansonsten ein Tor zu einer nicht überschaubaren Dimension der Sammlung personenbezogener Daten in deutschen Personaldokumenten geöffnet werde.

Mit der Aufnahme eines Verbotes zur Einrichtung einer bundesweiten Datei hat der Gesetzgeber einer zentralen Auswertung der biometrischen Daten eine Absage erteilt. Dennoch stellt sich darüberhinausgehend die Frage, wie die Speicherung der biometrischen Daten in den Pass- und Personalausweisbehörden realisiert werden soll. Anhand verschiedener Einsatzszenarien werden Möglichkeiten der Speicherung dieser Daten unten in Abschnitt 4.3.1.1.3 aufgezeigt und sodann aus datenschutzrechtlicher Sicht bewertet.

4.2.2.2 Abweichende Regelung für Ausländer

Eine der für Bundesbürger geltenden Regelung entsprechende Vorschrift ist im AuslG oder AsylVfG nicht zu finden. Eine Pflicht zur dezentralisierten Speicherung von biometrischen Daten gilt also nicht für Ausländer.[176] Es ist daher nicht gesetzlich ausdrücklich ausgeschlos

[174] § 4 Abs. 4 Satz 2 PassG, § 1 Abs. 5 Satz 2 PAuswG.
[175] Abrufbar unter: http://www.cilip.de/terror/aenderung11122001.pdf.
[176] *Weichert*, RDV 2002, 170 (175).

sen, zentrale Referenzdateien für die biometrischen Merkmale von Ausländern und Asylbewerbern, z.B. beim Bundesverwaltungsamt, einem künftigen Bundesamt für Migration und Flüchtlinge, der Bundesdruckerei oder auch dezentrale Referenzdateien bei den die Dokumente ausstellenden Ausländerbehörden oder bei anderen Stellen einzurichten. Da in jedem Fall in den Unterlagen der jeweils zuständigen Ausländerbehörden ein Verweis auf die Ausweiserstellung vorgenommen werden müsste, wären diese Daten über das Ausländerzentralregister (AZR) zentral erschlossen.[177]

§ 3 AZRG enthält eine Regelung über den allgemeinen Inhalt des Ausländerzentralregisters. Gemäß § 3 Nr. 1 AZRG ist im Ausländerzentralregister die meldende Stelle und deren Geschäftszeichen zu speichern. Die Vorschrift enthält dagegen keine Ermächtigung zur Speicherung biometrischer Daten. Eine zentrale Speicherung der biometrischen Merkmale der Ausländer im AZR ist nach § 3 AZRG mithin nicht zulässig.

Durch eine zentrale Speicherung von derartigen Ausländerdaten würde eine zweckändernde Nutzung dieser Daten erheblich erleichtert. Für die Durchführung von Datenabgleichen bedürfte es nicht der Kenntnis der sonstigen Identifizierungsdaten sowie der zuständigen bzw. meldenden Ausländerbehörde. Vielmehr würde für eine Zuordnung der biometrischen Datensätze das Vorliegen eines entsprechenden biometrischen Referenzmusters genügen. Eine Nutzung der biometrischen Ausländerdaten für andere Zwecke ist nach der derzeitigen Rechtslage nicht eingeschränkt, sondern für öffentliche Stellen ausdrücklich auf jeden gesetzmäßigen Zweck und jede Form der Datenverarbeitung ausgeweitet (§ 5 Abs. 7 AuslG, dazu s.u. Abschnitt 4.3.2.2.2). Eine Nutzung durch Private ist nicht ausdrücklich ausgeschlossen. Mangels bereichsspezifischer Regelungen gelten die allgemeinen Übermittlungs- und Erhebungsvorschriften im allgemeinen Datenschutzrecht. Eine Nutzung der biometrischen Ausländerdaten z.B. durch die Polizei oder durch Strafverfolgungsbehörden unterliegt also keinerlei spezifischen Einschränkungen (s.u. Abschnitt 4.3.1.1.2). Durch die erleichterte Abgleichsmöglichkeit und das Fehlen von spezifischen Zweckbindungsregelungen würde bei einer zentralen Speicherung von biometrischen Merkmalen von Ausländern eine Ungleichbehandlung gegenüber deutschen Staatsangehörigen erfolgen. Für diese Ungleichbehandlung im Sinne von Art. 3 GG werden keine fachlichen Gründe vorgetragen; solche Gründe sind auch nicht erkennbar.

[177] Stellungnahme der Deutschen Vereinigung für Datenschutz vom 15.11.2001: Terrorismusbekämpfungsgesetz

Das Grundgesetz enthält zwar eine Privilegierung von Deutschen in Bezug auf bestimmte Grundrechte (Art. 8 Abs. 1, 9 Abs. 1, 11 Abs. 1, 12 Abs. 1, 16 Abs. 1 und 2 Satz 1 GG), jedoch gilt dieses nicht für das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Hierbei handelt es sich um ein sog. Jedermann-Grundrecht, das in gleicher Weise für Nicht-Deutsche gilt. Es stellt sich allerdings die Frage, ob und unter welchen Voraussetzungen eine Ungleichbehandlung von Ausländern und Deutschen im Hinblick auf das Recht auf informationelle Selbstbestimmung gerechtfertigt sein könnte. Zum Beispiel lässt sich in Bezug auf die Einrichtung des Ausländerzentralregisters (AZR) sagen, dass eine Ungleichbehandlung grundsätzlich sachlich begründbar sein kann, wenn mit dem Ausländerzentralregister ausländer- und asylrechtliche Zwecke verfolgt werden, die z.B. am aufenthaltsrechtlichen Status eines Ausländers anknüpfen oder wenn vom Aufenthaltsrecht des Ausländers Entscheidungen anderer öffentlicher Stellen abhängen (z.B. Erwerbstätigkeit, Arbeitsaufnahme, Sozialleistungen). Dieses gilt jedoch dann nicht, wenn Daten des AZR für Entscheidungen herangezogen werden, bei denen es nicht ausdrücklich auf den Aufenthaltsstatus ankommt. So lässt sich eine sachlich nicht gerechtfertigte Ungleichbehandlung durch das Ausländerzentralregistergesetz (AZRG) z.B. darin sehen, dass mit der AZR-Nummer ein gegenüber Deutschen nicht vorhandenes Instrument zur Zusammenführung von Daten im AZR besteht, soweit sie zu anderen als ausländer- und asylrechtlichen Zwecken genutzt wird.[178]

Zu den aufenthaltsrechtlichen Zwecken gehören gerade nicht die Zwecke der Gefahrenabwehr und Strafverfolgung. Die Vorschrift des § 5 Abs. 7 AuslG erlaubt, dass „öffentliche Stellen die in der Zone für das automatische Lesen enthaltenen Daten zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen“ können. Insoweit erlaubt die Vorschrift die Datenverarbeitung auch über die ausschließlich aufenthaltsrechtlichen Zwecke hinaus. Diese weite Zweckänderung kann eine Ungleichbehandlung von Deutschen und Ausländern jedoch nicht rechtfertigen.

Eine zentrale Speicherung biometrischer Daten von Ausländern stellte aus den gleichen Gründen eine sachlich nicht gerechtfertigte Ungleichbehandlung dar, da die biometrischen Merkmale gerade nicht für aufenthaltsrechtliche Maßnahmen erforderlich sind. Hierfür reichen vielmehr die bereits im AZR gespeicherten Daten aus. Eine zentrale Speicherung bio

---

und Ausländer.

[178] Weichert, AZRG, Einführung Rn. 44-46.

metrischer Merkmale kann daher nicht durch die bestehenden Unterschiede im Status von Deutschen und Ausländern gerechtfertigt werden.

Die sich aus diesen unterschiedlichen Regelungen für Bundesbürger und Ausländer ergebenden Konsequenzen werden nachfolgend in Abschnitt 4.3.1 näher erörtert.

4.3 Datenschutzrechtliche Anforderungen an die praktische Ausgestaltung biometrischer Verfahren

4.3.1 Realisierung biometrischer Verfahren in Identifikationspapieren für Bundesbürger und in „Ausländerausweisen“

Es gibt verschiedene Möglichkeiten, die Aufnahme biometrischer Merkmale in Pässe und Ausweise zu realisieren. Je nachdem, welche Realisierungsmöglichkeit gewählt wird, ergeben sich unterschiedliche Konsequenzen für die von der Datenverarbeitung Betroffenen. Im Folgenden gilt es, die in Betracht kommenden Einsatzszenarien zu skizzieren, um diese dann aus datenschutzrechtlicher Sicht zu bewerten.

4.3.1.1 Denkbare Einsatzszenarien der Realisierung in Identifikationspapieren

4.3.1.1.1 Nutzung bereits vorhandener biometrischer Merkmale

Bevor auf die möglichen Einsatzszenarien der Aufnahme biometrischer Merkmale eingegangen wird, ist zu klären, ob nicht die Nutzung der im bisherigen Ausweis bereits vorhandenen biometrischen Merkmale wie das Lichtbild oder die Unterschrift des Pass- oder Personalausweisinhabers ausreichen könnten, um den in der Gesetzesbegründung als Grund für die Aufnahme biometrischer Merkmale genannten Zweck der zweifelsfreien Überprüfung, „ob die Identität der betreffenden Person mit den im Dokument abgespeicherten Originaldaten übereinstimmt“[179], zu erreichen.

Das Lichtbild des Dokumenteninhabers stellt ein biometrisches Merkmal dar. Grundsätzlich ist es technisch möglich, das Foto mit dem Gesicht derjenigen Person zu vergleichen, die bei einer Grenzkontrolle das Dokument vorlegt. Allerdings werden die bisherigen Lichtbilder wohl nicht die Qualitätsanforderungen erfüllen, die für einen effektiven automatisierten Abgleich erforderlich sind. Die Auswertung von Lichtbildern ist insbesondere stark von den

[179] BR-Drucks. 920/01, S. 84.

Lichtverhältnissen abhängig. Mit dem oben bereits erwähnten[180] von der Bundesdruckerei entwickelten sog. Verifier ist es aber wohl angeblich möglich, ein im Unterschied zum bisher im Halbprofil aufgenommenen Lichtbild in Frontalsicht aufgenommenes Foto als digitales Bild in den Deckel des Passes einzubauen und dieses in weniger als einer Sekunde mit dem sog. Verifier auszulesen.[181] Unabhängig von der tatsächlichen Zuverlässigkeit dieser Technik lässt sich sagen, dass auch dieser Einsatz die Aufnahme bestimmter den technischen Anforderungen genügender Lichtbilder voraussetzt. Im Ergebnis ist die Verwendung der bereits vorhandenen Passbilder für eine biometrische Erkennung nicht geeignet. Denkbar ist aber wohl, dass durch eine Änderung der aktuellen Anforderungen an Ausweis-Lichtbilder den neu eingeführten gesetzlichen Identifizierungszwecken genügt werden kann.

Bei der auf bisherigen Ausweisen vorhandenen Wiedergabe der Unterschrift handelt es sich um ein biometrisches Merkmal. Dieses ist aber wegen der leichten Fälschbarkeit als wenig zuverlässig zu bewerten. Für eine zuverlässige Identifizierung wird in der Regel eine dynamische Unterschriftserkennung eingesetzt. Die Dynamik bei der Erzeugung der Unterschrift wird als einzigartig angesehen. So werden z.B. die Schreibgeschwindigkeit, Beschleunigung, Schreibdruck, Neigungswinkel des Stiftes, die Richtungen der Handbewegung oder Anzahl und Zeitpunkt einzelner Federstriche erfasst.[182] Da diese erforderlichen dynamischen Daten der Unterschrift in herkömmlichen Ausweisen nicht gespeichert sind, wäre ein automatisierter Abgleich mit dieser Unterschrift nicht möglich, so dass auch die Verwendung der vorhandenen Unterschrift nicht in Betracht kommt.[183]

4.3.1.1.2 Aufnahme biometrischer Merkmale von „Fingern oder Händen oder Gesicht“

Wie oben bereits dargestellt, hat der Gesetzgeber die Körperbereiche festgelegt, die für die Auswahl der biometrischen Merkmale in Betracht kommen. Es ist nicht vorrangiger Gegenstand der vorliegenden Darstellung, die einzelnen biometrischen Merkmale im Hinblick auf ihre technische Eignung und Zuverlässigkeit zu bewerten; vielmehr soll an dieser Stelle aufgezeigt werden, welche datenschutzrechtlichen Anforderungen allgemein an die Geeignetheit und Verhältnismäßigkeit der in Betracht kommenden biometrischen Merkmale zu stellen sind. In erster Linie erfassen die biometrischen Merkmale der genannten Körperbereiche die Ge

[180] Siehe Abschnitt 2.1.3.
[181] Siehe hierzu *Filser*, in: SZ vom 11.03.2003, V2/9.
[182] *Breitenstein*, Überblick über biometrische Verfahren, in: *Nolde/Leger* (Hrsg.), Biometrische Verfahren, S. 35 (55).
[183] Vgl. hierzu Positionspapier des AK Technik, März 2002.

sichtsgeometrie, Fingerabdrücke sowie die Handgeometrie. Im Folgenden soll das Augenmerk daher im Wesentlichen auf diese Merkmale gerichtet werden. Es werden allerdings auch allgemeine datenschutzrechtliche Anforderungen definiert, die bei der Auswahl der zum Einsatz kommenden biometrischen Merkmale zu beachten sind.

Gesichtsgeometrie

Der Gesetzgeber hat das biometrische Merkmal „Gesicht" ausdrücklich benannt. Die biometrische Gesichtserkennung anhand der Gesichtsgeometrie hat als biometrisches Merkmal eine gewisse Verbreitung erfahren. Allerdings stellt sich das Problem, dass eine für Grenzkontrollen ausreichende Wiedererkennungsrate hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme stellt. Diese werden in der Praxis nur mit beträchtlichem Aufwand zu realisieren sein. So scheiterte kürzlich ein Pilotprojekt zur biometrischen Gesichtserkennung am Nürnberger Flughafen, weil diese Qualität gerade nicht erreicht wurde.[184] Zur Erzielung guter Ergebnisse bedarf es insbesondere idealer Lichtbedingungen und gut ausgeleuchteter Frontalaufnahmen von Gesichtern. Diese Voraussetzungen sind allerdings in der Praxis nicht ohne weiteres zu gewährleisten.

Fingerabdrücke

Der Einsatz der Papillarmuster der Finger stellt ein weiteres in Betracht kommendes biometrisches Merkmal dar. Diese Methode wirft Probleme auf, wenn der Finger Verletzungen aufweist oder anderweitig stark beansprucht wurde, wie z.B. durch Gartenarbeit oder bei Bauarbeitern. Eine Erfassung der Daten mehrerer Finger und gegebenenfalls alternative Vergleiche bei Kontrollen sind sehr aufwändig. Des Weiteren stellt sich auch das Problem, dass es Personen gibt, bei denen der Fingerabdruck auf Grund schlechter Merkmalsausprägung und somit aus physiologischen Gründen für ein biometrisches Verfahren nicht geeignet ist.

Handgeometrie

Als biometrisches Merkmal der „Hände" kommt die Handgeometrie in Betracht. Auch hier ergeben sich ähnliche Probleme wie bei der Verwendung von Fingerabdrücken, wenn die Hand Verletzungen aufweist. Unklar ist auch, ob die Wiedererkennungsqualität durch Arbeits- und Alterungsprozesse eingeschränkt wird.[185]

Der Gesetzgeber hat sich entschieden, lediglich biometrische Merkmale der genannten Körperbereiche zuzulassen, so dass weitere in Betracht kommende Merkmale, wie z.B. die Iris-

[184] Siehe Abschnitt 2.1.4.

Erkennung oder auch die dynamische Unterschrifterkennung wohl ausscheiden. Fraglich ist, ob der Gesetzgeber mit der Beschränkung der in Betracht kommenden Körperbereiche andere, aus datenschutzrechtlicher Sicht vorzugswürdige Merkmale ausgeschlossen hat. Allgemein lässt sich sagen, dass ein biometrisches Merkmal aus datenschutzrechtlicher Sicht dann geeignet ist, wenn es mehreren Anforderungen genügt:

Der im Datenschutzrecht geltende Grundsatz der sog. Direkterhebung verlangt, dass personenbezogene Daten grundsätzlich bei der betroffenen Person selbst zu erheben sind und zwar mit ihrer Kenntnis und gegebenenfalls Mitwirkung (§ 4 Abs. 2 Satz 1 BDSG). Die Erfordernisse der Kenntnis und Mitwirkung des Betroffenen ergeben sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung. Danach soll der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen.[186] An dieser Mitwirkung fehlt es dann, wenn Daten heimlich bei der betroffenen Person erhoben werden.[187] Biometrische Verfahren, die für den Masseneinsatz geeignet sein sollen, müssen so konstruiert sein, dass die Daten gerade nicht unbemerkt erfasst werden, sondern vielmehr der Betroffene Kenntnis von der Anwendung hat. Mit dem Grundsatz der Direkterhebung und dem bei der Datenverarbeitung allgemein geltenden Transparenzgebot wäre es also unvereinbar, eine verdeckte Sprech- oder Gesichtserkennung sowie eine verdeckte Auswertung anderer Daten, wie z.B. Unterschriften, einzusetzen. Es sind dementsprechend biometrische Verfahren vorzuziehen, die eine aktive Mitwirkung des Betroffenen verlangen und deshalb eine verdeckte Erfassung biometrischer Merkmale nicht oder lediglich unter erschwerten Bedingungen zulassen. Nach dem aktuellen technischen Kenntnisstand kommen hierfür Verfahren in Betracht, die einen Körperkontakt oder eine bestimmte „Aufnahmeposition“ erfordern. Hierbei handelt es sich z.B. um Hand- und Fingerabdruckverfahren, Handgeometrie, Handvenenmuster, Iris- und Retinaerkennung sowie verhaltensbasierte Merkmale wie die Unterschriftsdynamik.[188] Bei diesen Merkmalen bestehen jedoch Unterschiede bezüglich ihrer Missbrauchsmöglichkeiten sowie eine Einschränkung hinsichtlich ihrer technischen Eignung, die an dieser Stelle nicht abschließend bewertet werden soll.

Auch ist aus datenschutzrechtlicher Sicht unter dem Gesichtspunkt der Verhältnismäßigkeit zu beachten, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen

---

[185] Zu den einzelnen biometrischen Merkmalen siehe Positionspapier des AK Technik, März 2002.
[186] BVerfGE 65, 1, 43ff.
[187] *Sokol*, in: *Simitis* u.a., BDSG, § 4 Rn. 20ff.
[188] Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 10.

können. Biometrische Rohdaten, z.B. Aufnahmen von Gesicht, Sprache, Iris, Augenhintergrund und Fingerabdruck, können nämlich durchaus weitere Informationen über den Merkmalsträger aufzeigen. Neben Rückschlüssen auf Geschlecht, Alter und ethnische Herkunft, die anhand des Gesichtes und der Sprache zu ziehen sind, lassen Aufnahmen des Augenhintergrundes u.U. Diagnosen auf Krankheiten wie Arteriosklerose, Diabetes und Bluthochdruck zu.[189] Bei der Verwendung von Fingerabdrücken scheint es statistische Korrelationen von Fingerabdruckmustern und Krankheiten wie chronischen Magen-Darm-Beschwerden (CIP), Leukämie und Brustkrebs zu geben.[190] Da es nicht auszuschließen ist, dass mit derartigen, wissenschaftlich nicht unbedingt gesicherten Erkenntnissen Diskriminierungen verbunden sein können, ist sicherzustellen, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.[191] Bei der Auswahl und Ausgestaltung der Verfahren ist darauf zu achten, die mit der Aufnahme biometrischer Merkmale verbundenen Nebenwirkungen zu minimieren. Die Aufnahme biometrischer Merkmale, die überschießende Informationen über den Betroffenen preisgeben, würde den Einzelnen in unverhältnismäßiger Weise in seinem Grundrecht auf informationelle Selbstbestimmung beeinträchtigen. Es bedarf daher einer Abwägung zwischen dem staatlichen Interesse an einer zweifelsfreien Identifizierung anhand biometrischer Merkmale und den Beeinträchtigungen des Einzelnen in seinem Grundrecht auf informationelle Selbstbestimmung. Als angemessene und datenschutzgerechte Möglichkeit kommt der Verzicht auf die Speicherung entsprechender Rohdaten in Betracht.

Hinsichtlich der Aufnahme biometrischer Merkmale in „Ausländerausweise“ sind bei der Auswahl dieser Merkmale im Vergleich zu Bundesbürgern weitere Einschränkungen zu fordern. Während das PassG und das PAuswG eine Beschränkung des Auslesens der Daten auf die Überprüfung der Echtheit des Dokumentes und die Identitätsprüfung des Inhabers vorsehen, fehlt eine derartige Regelung im AuslG. Vielmehr dürfen sämtliche öffentlichen Stellen gemäß § 5 Abs. 7 AuslG die Daten zur Erfüllung ihrer gesetzlichen Aufgaben nutzen. Die Nutzungserlaubnis wird mit der Absicht eröffnet, maschinelle Datenabgleiche durchführen zu

[189] *Probst*, Biometrie aus datenschutzrechtlicher Sicht, in: *Nolde/Leger* (Hrsg.), Biometrische Verfahren, S. 115 (118f.) unter Hinweis auf *Woodward*, Biometric Scanning, Law & Policy: Identifying the concerns – drafting the Biometrics Blueprint, Fußnoten 70-72.

[190] *Probst*, Biometrie aus datenschutzrechtlicher Sicht, in: *Nolde/Leger* (Hrsg.), Biometrische Verfahren, S. 115 (118f.) unter Hinweis auf *Woodward*, Identifying Law & Policy Concerns, in: *Jain/Bolle/Pankati*, Biometrics: Personal Identification in Networked Society, S. 393.

[191] Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Biometrischen Merkmalen in Personalausweisen und Pässen.

können.[192] Von den in Betracht kommenden biometrischen Merkmalen fallen die Merkmale der Finger und des Gesichtes unwillkürlich bei alltäglichen Gelegenheiten an. Da sich die Daten auch für andere als ausländerrechtliche Identifizierungszwecke eignen und die Nutzung für polizeiliche Zwecke über die generellen gesetzlichen Übermittlungsbefugnisse der Ausländerbehörden und der Erhebungsbefugnisse durch Polizeibehörden eröffnet ist, ist davon auszugehen, dass eine Verwendung dieser Daten für polizeiliche Spurenabgleiche auch erfolgen wird. So ist es möglich, Spurenabgleiche z.B. mit an Gläsern hinterlassenen Fingerabdrücken vorzunehmen. Mit Zunahme der Videoüberwachung im öffentlichen Raum wird auch die Vornahme von Musterabgleichen mit anderweitig erfassten Videobildern ermöglicht.[193] Angesichts dieser Szenarien ist es daher erforderlich, bei Ausländern aus Gründen der Verhältnismäßigkeit zur Verhinderung einer zweckwidrigen Nutzung darauf zu achten, dass ein Merkmal verwendet wird, das keine derartigen Zusatzinformationen enthält. Wie bereits oben dargestellt, kann dieses durch den Verzicht auf die Speicherung von Rohdaten erreicht werden.

4.3.1.1.3 Möglichkeiten der Speicherung biometrischer Merkmale

4.3.1.1.3.1 Speicherung auf dem Pass- oder Personalausweis

Die Aufnahme biometrischer Merkmale in Ausweispapiere kommt in unterschiedlichen Konstellationen in Betracht. Es ist denkbar, die biometrischen Merkmale ausschließlich in dem jeweiligen Pass oder Personalausweis zu speichern. Sofern anhand der biometrischen Merkmale festgestellt werden soll, ob derjenige, der das Dokument vorlegt, auch tatsächlich der Inhaber des Dokumentes ist, handelt es sich um eine biometrische Verifikation, d.h. um einen Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Pass oder Personalausweis gespeicherten Daten. Zur Erfüllung dieses Zweckes ist eine Speicherung außerhalb des jeweiligen Dokumentes nicht erforderlich. Vielmehr hätten die Betroffenen die alleinige Verfügungsgewalt über ihre biometrischen Daten.

4.3.1.1.3.2 Dezentrale Speicherung in Registern

Eine weitere Möglichkeit bestünde darin, die biometrischen Merkmale zusätzlich zu der Speicherung im Pass- bzw. Personalausweis selbst in dezentralen (elektronischen) Registern zu

[192] *Weichert*, DuD 2002, 423 (425); vgl. BR-Drucks. 920/01, S. 127.
[193] Stellungnahme der Deutschen Vereinigung für Datenschutz: Terrorismusbekämpfungsgesetz und Ausländer vom 15.11.2001; *Weichert*, DuD 2002, 423 (425).

speichern. Gegenwärtig werden die in Pässen und Personalausweisen gespeicherten Daten über die Person des Pass- bzw. Personalausweisinhabers im Pass- bzw. Personalausweisregister gespeichert. § 16 Abs. 2 PassG bzw. § 3 Abs. 2 PAuswG regeln derzeit ausdrücklich, dass die Beantragung, Ausstellung und Ausgabe von Pässen bzw. Personalausweisen nicht zum Anlass genommen werden darf, die dazu erforderlichen Angaben außer bei den zuständigen Pass- bzw. Personalausweisbehörden zu speichern. Mit dieser Regelung sollte nach der Gesetzesbegründung zum PassG „verhindert werden, dass über die ausdrücklich zugelassenen Dateien hinaus zentrale Register eingerichtet werden".[194] Auf diese Weise wurde die Unzulässigkeit der Schaffung von bundes- oder landesweiten Pass- oder Personalausweisregistern festgestellt.

Für die Bundesdruckerei, die Pässe und Personalausweise personengebunden herstellt und an die zu diesem Zwecke von den Pass- und Personalausweisbehörden die zur Erstellung des Ausweises erforderlichen Daten einschließlich des Lichtbildes übertragen werden, gilt ein explizites Löschungsgebot. Die Bundesdruckerei erhält nämlich Kenntnis *aller* auf Pässen und Personalausweisen enthaltenen Daten sämtlicher Bundesbürger. Sie darf lediglich eine zentrale Speicherung der Seriennummern der Pässe zum Nachweis des Verbleibs der Pässe vornehmen (§ 16 Abs. 3 Satz 1 PassG, § 3 Abs. 3 Satz 1 PAuswG). Die Speicherung der übrigen im Pass oder Personalausweis enthaltenen Angaben ist unzulässig, soweit sie nicht ausschließlich und vorübergehend der Herstellung des Passes bzw. Personalausweises dient. Die Angaben sind anschließend zu löschen (§ 16 Abs. 3 Satz 2 PassG, § 3 Abs. 3 Satz 2 PAuswG).

In diesem Zusammenhang ist zu betonen, dass auch die Zusammenfassung von Melde-, Personalausweis- und Passregistern unzulässig wäre. Auch wenn diese einzelnen Register organisatorisch bei den Einwohnermeldeämtern ein Register darstellen, so muss die funktionelle Trennung strikt gewährleistet sein. Außerdem darf eine Datenspeicherung ausschließlich im Pass- bzw. Personalausweisregister erfolgen, eine zentrale Speicherung in Dateien anderer Behörden wäre dagegen unzulässig.[195]

Gegenwärtig wird die Speicherung biometrischer Merkmale nicht von den im Pass- und Personalausweisregister zu speichernden Angaben umfasst. In Bezug auf die Speicherung der

[194] BT-Drucks. 10/3303, S. 15.
[195] *Medert/Süßmuth*, Paß- und Personalausweisrecht, Bd. 2, Erl. § 16 Rn. 5/6.

biometrischen Merkmale bedarf es vielmehr noch einer Regelung in dem zu erlassenden Ausführungsgesetz.

4.3.1.1.3.3 Zentrale Datenspeicherung in einem eigenen Register

Es wäre denkbar, die biometrischen Merkmale im Ausweis zu speichern und zusätzlich eine zentrale Speicherung der Daten in einem eigens für diesen Zweck eingerichteten Register vorzunehmen. Aus datenschutzrechtlicher Sicht stellt die Speicherung in einem zentralen Register diejenige Lösung dar, die unter verschiedenen rechtlichen Gesichtspunkten, u.a. im Hinblick auf die Grundsätze der Erforderlichkeit sowie der Datenvermeidung und Datensparsamkeit, am problematischsten wäre. Da die Einrichtung einer bundesweiten Datei für biometrische Merkmale von Bundesbürgern nach gegenwärtiger Rechtslage ausgeschlossen ist, soll eine nähere Betrachtung dieser Möglichkeit an dieser Stelle unterbleiben.

Ein zentraler Datenbestand ist allerdings für die in den „Ausländerausweisen" gespeicherten biometrischen Daten nicht gesetzlich ausgeschlossen. Eine solche zentrale Datenspeicherung wäre jedoch aus Gründen der Ungleichbehandlung und der Verhältnismäßigkeit unzulässig (s.o. Abschnitt 4.2.2.2). Mit dem Fingerabdruckidentifikationssystem (AFIS) befindet sich ein solches Verfahren im Asylbereich bereits im Einsatz.

Gegen das derzeit bestehende AFIS-Verfahren werden erhebliche verfassungsrechtliche Bedenken erhoben.[196]

Ungeklärt ist bisher, in welchem Verhältnis AFIS, das vorrangig dem Zweck der Identifizierung von Ausländern dient, und der Einsatz von Biometrie auf „Ausländerausweisen" mit genau dem selben Zweck stehen. Aus Gründen der Datensparsamkeit wie auch aus Gründen der Verhältnismäßigkeit ist eine redundante biometrische Datenspeicherung zu gleichen Zwecken zu vermeiden.

Einer zentralen Speicherung der biometrischen Ausweisdaten beim Bundeskriminalamt (BKA) steht entgegen, dass eine solche Datenverarbeitung nicht zu den Aufgaben dieser Behörde gehört.[197]

---

[196] *Weichert*, in: Huber, Handbuch des Ausländerrechts, Stand Februar 2002, § 16 AsylVfG, Rn. 7, 9; *derselbe* DuD 1999, 167 (167).

Eine zentrale Speicherung der biometrischen Daten beim AZR ist wegen der eindeutigen und abschließenden spezielleren Regelung des § 3 AZRG unzulässig.

4.3.1.1.4 Datenschutzrechtliche Bewertung der verschiedenen Möglichkeiten

Die aufgezeigten Möglichkeiten der Speicherung biometrischer Daten auf den Ausweisen selbst, in einem dezentralen Datenbestand oder einem zentralen Datenbestand sind aus datenschutzrechtlicher Sicht unter dem Gesichtspunkt der Verhältnismäßigkeit unterschiedlich zu bewerten.

Der in der Begründung zum Terrorismusbekämpfungsgesetz angeführte Zweck der Verbesserung der „Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente“ und der Verhinderung, dass „Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen“, kann sowohl durch eine Speicherung allein auf dem Ausweis als auch durch eine Speicherung in einem dezentralen oder zentralen Register erreicht werden.

Fraglich ist deshalb, ob die Speicherung der Daten außerhalb der Ausweise unter dem Gesichtspunkt der Zweckbindung sowie der Datenvermeidung und Datensparsamkeit überhaupt als verhältnismäßig angesehen werden kann. Der oben genannte Zweck der Echtheits- und Authentizitätsprüfung kann auch erreicht werden, wenn die Daten lediglich auf den Dokumenten selbst gespeichert werden. Zur Verhinderung einer unbefugten Nutzung von Ausweisdokumenten ist lediglich eine Verifikation erforderlich, d.h. der Abgleich der biometrischen Daten einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Hierfür reicht eine Speicherung auf dem Dokument selbst aus.

Der Zweck der Verhinderung von „Doppelidentitäten“ durch den Abgleich biometrischer Daten einer unbekannten Person mit denjenigen anderer Personen im Sinne einer Identifikation würde dahingegen eine Speicherung personenbezogener Daten in zentralen Referenzdateien voraussetzen.[198] Angesichts der mit der Speicherung biometrischer Daten verbundenen Risiken dürfen Referenzdaten allerdings keinesfalls zentral abgelegt werden. Zwar könnte der

---

[197] Vgl. zu den historisch erklärlichen, inzwischen aber überholten Regelungen der § 78 Abs. 1 AuslG, § 16 Abs. 3 Satz 1 AsylVfG: *Weichert*, in: *Huber*, Handbuch des Ausländerrechts, Stand Februar 2002, § 78 AuslG, Rn. 4, § 16 AsylVfG Rn. 9.

[198] Positionspapier des AK Technik, März 2002.

Zweck, Ausweis-Doppelausstellungen zu verhindern, lediglich mit einem zentralen Datenbestand wirksam unterbunden werden, dessen Aufbau der Gesetzgeber angesichts der Gefahren für das Recht auf informationelle Selbstbestimmung aber zu Recht abgelehnt hat. Mit den zunehmenden Möglichkeiten einer Erfassung und Speicherung biometrischer Merkmale in umfassenden Datenbeständen stiege nämlich das Missbrauchs- und Schadenspotenzial. Es wäre damit zu rechnen, dass nicht nur Strafverfolgungsbehörden, sondern ebenfalls Unbefugte durch unbefugten Zugriff auf die Datenbanken (Hacking) in den Besitz der Daten gelangen. Aus datenschutzrechtlicher Sicht ist eine zentrale Datei, die die Referenzdaten aller Bundesbürger umfasst, auch aus Verhältnismäßigkeitsgründen als unzulässig anzusehen.

Neben der zentralen Speicherung kommt eine Speicherung in dezentralen Registern in Betracht. Eine derartige Speicherung wird gegenwärtig hinsichtlich der übrigen in den Dokumenten gespeicherten Daten vorgenommen. Auch eine solche Speicherung ist weder für Zwecke der Authentizitätsprüfung noch zur Erkennung von Doppelidentitäten erforderlich. Stattdessen ist zu bedenken, dass die Speicherung in dezentralen Registern durchaus die Verwendung auch zu anderen, etwa strafrechtlichen Zwecken bis hin zur „Rasterfahndung“ ermöglichen würde. In diesem Zusammenhang ist zu bedenken, dass eine Speicherung in dezentralen Registern die Möglichkeit eröffnete, die Daten zu Ermittlungs- und Fahndungszwecken sowie zur Vorbeugung der Gefahrenabwehr oder sogar der Gefahrenermittlung an die Polizei und andere Strafverfolgungsbehörden zu übermitteln. Eine derartige Nutzung verstieße gegen den Verhältnismäßigkeitsgrundsatz und wäre daher aus verfassungsrechtlicher Sicht als unzulässig anzusehen. Auch eine Speicherung der biometrischen Daten in dezentralen Registern würde mit dem Recht auf informationelle Selbstbestimmung nicht in Einklang stehen, weil sie eine zweckfremde Nutzung der Daten ohne Einwilligungsmöglichkeit der Betroffenen zuließe.

Weiterhin käme eine Speicherung der biometrischen Daten durch die Ausstellungsbehörde „für die Akten“ in Betracht. Die Daten würden nicht zum Abruf bereitgestellt werden. Der einzige Zweck der Speicherung bestünde darin, im Einzelfall bei Manipulationsverdacht die Ordnungsmäßigkeit des Verwaltungshandelns überprüfen zu können, indem (manuell) Einblick in die aufbewahrten Unterlagen genommen würde. Zu unterscheiden wäre hier, ob die biometrischen Rohdaten, die Templates oder beide gespeichert werden. Im Hinblick auf das Gebot der Datensparsamkeit ist eine Speicherung allein der Templates zu bevorzugen. Sollten die biometrischen Daten durch Aufdruck auf den Ausweisen gespeichert werden, würde ein

Ausdruck „für die Akten“ genügen. Im Falle einer elektronischen Speicherung auf den Ausweisen würde dieser Datenbestand der biometrischen Merkmale vermutlich auch elektronisch gespeichert werden. In diesem Fall wäre zu gewährleisten, dass der Datenbestand von den übrigen Datenbeständen abgeschottet ist und im Hinblick auf die enge Zweckbindung (Überprüfbarkeit der Ordnungsmäßigkeit des Verwaltungshandelns) einer unbedingt wirksamen Zugriffsregelung unterliegt.

Allerdings ist zu bedenken, dass die entsprechenden biometrischen Merkmale in jedem Falle in einem Datenbestand gespeichert würden, der nicht der Verfügungsgewalt des Betroffenen unterläge. Es bedürfte lediglich einer gesetzgeberischen Entscheidung, um eine Zusammenführung und damit Nutzbarkeit dieser Daten für andere Zwecke zu ermöglichen. Im Hinblick auf das informationelle Selbstbestimmungsrecht ist es deshalb geboten, die biometrischen Merkmale des Pass- oder Personalausweisinhabers lediglich auf dem Dokument und damit im Verfügungsbereich des Betroffenen selbst zu speichern und bei einer Kontrolle über ein Lesegerät mit den Merkmalen des Inhabers zu vergleichen. Auf eine dauerhafte Speicherung biometrischer Daten außerhalb des Verfügungsbereichs des Betroffenen müsste gänzlich verzichtet werden.[199]

Bezüglich der Frage nach einer zentralen Datenspeicherung von biometrischen Ausländerdaten ist auf § 5 Abs. 7 AuslG hinzuweisen. Diese Regelung sieht zwar keine zwingende Datenspeicherung der biometrischen Daten vor. Wohl aber erlaubt sie deren automatisierte Speicherung, Übermittlung und Nutzung nicht nur bei der Ausländerbehörde, sondern bei allen einbezogenen öffentlichen Stellen „zur Erfüllung ihrer gesetzlichen Aufgaben“. Dies bedeutete, dass die Daten zumindest in Templateform als Personenkennzeichen verwendet werden dürften (s.o. Abschnitt 2.2.2.7). Diese Regelung enthält systemwidrig im Ausländerrecht eine Befugnisnorm für sämtliche öffentliche Stellen und steht im inhaltlichen Widerspruch zu bereichsspezifischen Regelungen (z.B. § 3 AZRG). Sie dürfte im Hinblick auf die überwiegende Meinung in Literatur und Rechtsprechung verfassungswidrig sein (s.u. Abschnitt 4.3.2.2.2). Faktisch läuft diese Regelung darauf hinaus, dass alle kommunalen, Landes- oder Bundesbehörden die Befugnis zur Erstellung von (u.U. bundesweiten) biometrischen Ausländerverzeichnissen erhalten, soweit dies für die Aufgabenerfüllung als erforderlich angesehen wird.

[199] Vgl. Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 11.

Im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung wäre eine Speicherung der biometrischen Merkmale außerhalb des Ausweisdokumentes allenfalls bei einer dezentralen oder zentralen Ausländerbehörde vorstellbar, wobei jedoch eine ausschließliche Bindung auf Zwecke der Datensicherung gesetzlich vorgesehen werden müsste (vgl. § 14 Abs. 4 BDSG).

4.3.1.2 Sonstige denkbare Nutzungen der biometrischen Merkmale

Neben der Nutzung biometrischer Daten auf Pässen und Ausweisen zum Zwecke der Identifizierung und Datensicherung sind darüber hinaus weitere Nutzungsmöglichkeiten biometrischer Daten denkbar:

In Betracht kommt die Überprüfung auf Doppelausstellungen von Ausweispapieren durch Datenabgleich mit gespeicherten biometrischen Daten: Denkbar wäre es, die biometrischen Daten aller ausgestellten Dokumente zu speichern und bei einer Neubeantragung die biometrischen Daten des Antragstellers mit dem gespeicherten Datenbestand zu vergleichen, um auf diese Weise eine eventuelle Beantragung unter falscher Identität aufzudecken. Dieses Verfahren wird im Rahmen der EURODAC-Verordnung bei Asylbewerbern angewandt. Als biometrisches Merkmal werden dabei Fingerabdrücke verwendet, die in einer europaweiten Datenbank gespeichert werden. (siehe zu EURODAC Abschnitt 2.1.1) Im Bereich der Pässe und Personalausweise für Bundesbürger wäre ein zentraler Bestand der biometrischen Daten (oder ein Zugriff auf alle dezentral gespeicherten Bestände) notwendig. Ein solches Verfahren könnte allenfalls unter Wahrung strenger Zweckbindung und unter Verwendung von Templates zugelassen werden. Eine zentrale Speicherung von biometrischen Original-Daten ausschließlich zum Zweck der Verhinderung der doppelten Ausstellung eines zweiten Ausweises bzw. Passes an eine Person wäre angesichts der bislang äußerst geringen Missbrauchsquote nicht verhältnismäßig.

Ein weiteres Szenario liegt in der Nutzung zu kriminalistischen bzw. polizeilichen Zwecken. Die Übermittlung biometrischer Daten von Einzelpersonen aus zentralen oder dezentralen Registern oder Archiven könnte Strafverfolgungsbehörden z.B. für erkennungsdienstliche Maßnahmen, Ermittlungen gegen Verdächtige durch Vergleiche von Tatortspuren (z.B. Finger- oder Handabdrücke, Gesichtsaufnahmen aus Videoüberwachungen) mit den biometrischen Daten der Verdächtigen, Übermittlungen zu Fahndungszwecken, Observierungen oder

gar zur Durchführung von Ordnungswidrigkeitenverfahren dienen[200] (in erster Linie Lichtbilder). Derartige Übermittlungen könnten je nach technischer Ausgestaltung manuell oder automatisiert durch ein Abrufverfahren erfolgen. Voraussetzung wäre, dass der Name und ggf. der Wohnort zum Abruf bekannt sein müssen. In der Erprobung beim BKA befinden sich bereits Verfahren, die Gesichtsaufnahmen aus Videoüberwachungkameras biometrisch auswerten sollen. Denkbar ist der Einsatz sog. „Watchlists", die Fahndungslisten vergleichbar Aufnahmen von gesuchten oder zu überprüfenden Personen enthalten.

Denkbar wäre sogar die Einspeicherung von für Ausweiserstellungszwecke erhobenen Gesichtsdaten zum generalpräventiven Abgleich in Videoüberwachungssysteme. Schließlich ist auch ein massenhafter (namenloser) Abruf biometrischer Daten aus Registern (ggf. im Hinblick auf Personeneigenschaften wie Alter, Geschlecht, etc. sortiert) in Kombination mit einem automatisierten Datenabgleich zur Personenermittlung (Identifikation) vorstellbar. Dies stellt im Prinzip eine Rasterfahndung mit biometrischen Daten dar. Ob die biometrischen Daten aus einzelnen Registern (etwa bei Meldebehörden) abgerufen und anschließend in einer zentralen Datei zusammengeführt werden oder ob sie aus einer bestehenden zentralen Datei abgerufen werden oder die Vergleichsalgorithmen auf den Datenbanken der Registerdateien implementiert werden, ist keine Frage grundsätzlicher Machbarkeit, sondern eine Frage der Aufwandes, der sich hinsichtlich technischer Ausgestaltung sowie Art und Anzahl der verwendeten Verfahren unterscheidet.

Derartige Systeme sind teilweise schon auf Grund des Verbotes einer zentralen Datenhaltung unzulässig. In jedem Fall verstießen sie gegen die verfassungsrechtlichen Prinzipien der Zweckbindung und des Verbots der Vorratsdatenverarbeitung.

Zu bedenken ist in diesem Zusammenhang, dass sich aus den seit den 70-er Jahren im Bereich der Terrorismusfahndung gewonnenen Erfahrungen die Erwartung ableiten lässt, dass ein einmal eingerichteter öffentlicher oder überregionaler Datenbestand trotz zunächst enger Zweckbestimmung auf Dauer auch für andere Zwecke genutzt wird. Sowohl Druck der Medi

[200] Im Rahmen der Täterermittlung bei Verkehrsdelikten (Geschwindigkeitsübertretung/Rotlichtverstößen) werden durch einige Ordnungsämter digitalisierte Lichtbilder von den Meldebehörden angefordert, um Vergleiche mit den Meßfotos der Überwachungsanlage durchzuführen. Die Rechtmäßigkeit dieses Vorgehens ist unklar (OLG Stuttgart, Az: 1 Ss 230/02, Beschluss vom 26.08.2002, http://www.ra-kotz.de/passfoto1.htm; dagegen AG Stuttgart, DANA 2/2002, S. 41f.).

en als auch außenpolitischer Druck kann dazu führen, dass derzeit kaum vorstellbare und in der Öffentlichkeit nicht konsensfähige Verwendungen in Betracht kommen.[201]

4.3.2 Datenschutzrechtliche Vorgaben für die Realisierung

Neben den bereits im Rahmen der einzelnen Einsatzszenarien abgehandelten datenschutzrechtlichen Anforderungen an die den Einsatz biometrischer Verfahren regelnden Ausführungsbestimmungen sind allgemeine datenschutzrechtliche Grundsätze zu beachten.

4.3.2.1 Geeignetheit biometrischer Systeme für den Masseneinsatz

Bei der Planung des Einsatzes biometrischer Verfahren ist es wichtig, die Rechtsfolgen für die Betroffenen zu beachten. Nach dem gegenwärtigen technischen Entwicklungsstand können biometrische Verfahren Sicherheit lediglich in einem begrenzten Umfang bieten. Die Entscheidungen biometrischer Verfahren können nur im Rahmen einer gewissen Schwankungsbreite korrekt sein. Die Genauigkeit biometrischer Systeme hängt wiederum von vielen Faktoren ab. So kommt es entscheidend auf das gewählte biometrische Merkmal an, wobei zu beachten ist, dass die mit den einzelnen Merkmalen zu erreichende Genauigkeit schwankend ist. Entscheidend sind auch die Parametereinstellungen. Da biometrische Rohdaten mit Messfehlern behaftet sind oder sich im Laufe der Zeit durch verschiedene Faktoren, wie z.B. Stimmbruch, Änderung der Frisur, Verletzungen am Finger etc., ändern können, stimmen nämlich auch die Templates nicht mehr vollständig überein, was beim Vergleich (Matching) berücksichtigt werden muss. Die Wahl des Parameters, mit dem eingestellt werden kann, ab welchem Übereinstimmungsgrad eine positive Identifikation gemeldet werden soll, bestimmt den Prozentsatz der Falschentscheidungen.[202]

Bereits oben in Abschnitt 2.1.4 wurde aufgezeigt, dass biometrische Merkmale auf Grund praktischer Erfahrungen nicht von vornherein als geeignet für den Masseneinsatz angesehen werden können. Vielmehr gilt es zu bedenken, dass sich die Pilotprojekte immer nur auf eine im Verhältnis zum flächendeckenden Einsatz sehr geringe Anzahl von Personen beziehen. Bei einem Masseneinsatz biometrischer Systeme ist es von grundsätzlicher Bedeutung, strenge Anforderungen an die Leistungsfähigkeit des gewählten Systems zu stellen. Zur Erreichung

[201] Vgl. Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 19.
[202] Vgl. Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, S. 16.

des vom Gesetzgeber verfolgten Zweckes der zweifelsfreien Überprüfung der Identität der das Dokument vorlegenden Person mit dem Inhaber des Dokumentes bedarf es eines Systems, das in der Lage ist, die Zahl der Personen, die die Grenzkontrollen trotz falscher Identität passieren können (FAR False Acception Rate), möglichst gering zu halten. Auch die trotz ständiger Verbesserung der Technik nicht zu vermeidenden fälschlichen Zurückweisungen berechtigter Personen müssen sich in einem für die Betroffenen zumutbaren Rahmen bewegen. Die Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) muss daher möglichst gering sein. In diesem Zusammenhang ist auch zu fordern, dass eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten vor der Ausgabe der Ausweise und Pässe bereits durch die örtlichen Pass- und Personalausweisbehörden ausgeschlossen werden muss. Zu diesem Zweck bedarf es flankierender technischer und organisatorischer Maßnahmen, wie z.B. eine vor der Aushändigung des Dokumentes erfolgende Prüfung mithilfe eines Referenz-Kontrollsystems.[203]

4.3.2.2 Verwendungszwecke der Daten

4.3.2.2.1 Regelung für Bundesbürger

Wie oben in Abschnitt 2.2.2.2 dargestellt, gilt im gesamten Datenschutzrecht der Grundsatz der Zweckbindung, so dass bei jeder Datenverarbeitung feststehen muss, für welche Zwecke die Daten verarbeitet und genutzt werden sollen. Der Gesetzgeber hat im Rahmen des Terrorismusbekämpfungsgesetzes in § 16 Abs. 6 PassG und § 3 Abs. 5 PAuswG geregelt, dass die im Pass oder Personalausweis enthaltenen verschlüsselten Merkmale und Angaben, zu denen nicht lediglich die biometrischen Merkmale, sondern auch die weiteren im Pass oder Personalausweis gespeicherten Angaben gehören, nur zur Überprüfung der Echtheit des Dokumentes und zur „Identitätsprüfung“, d.h. zur Echtheits- und Authentizitätsprüfung des Personalausweisinhabers ausgelesen und verwendet werden dürfen. Eine Verwendung zur direkten Identifizierung, z.B. durch die automatische Erkennung gesuchter Personen im Rahmen einer Videoüberwachung, wird durch die Vorschriften ausgeschlossen.[204] Es stellt sich in diesem Zusammenhang die Frage, ob der in der Vorschrift genannte Verwendungszweck der Überprüfung der Echtheit des Dokumentes bzw. der Identitätsprüfung den Anforderungen genügt, die nach dem strengen Zweckbindungsgrundsatz zu stellen sind. Im Hinblick auf Pässe und Personalausweise von Bundesbürgern wird dies wohl zu bejahen sein.

---

[203] Positionspapier des AK Technik, März 2002.
[204] *Garstka*, Neue Justiz 2002, 524 (525).

4.3.2.2.2 Regelung für Ausländer

Eine andere Beurteilung ergibt sich allerdings für Ausländer in Bezug auf die „Ausländerausweise“. Den für die Bundesbürger geltenden Vorschriften entsprechende Regelungen wurden in das AuslG gerade nicht aufgenommen. Stattdessen enthält § 5 Abs. 7 AuslG eine pauschale Verarbeitungsbefugnis sämtlicher automatisch lesbaren Daten für sämtliche öffentlichen Stellen, die die Daten zur Erfüllung ihrer gesetzlichen Aufgaben speichern, übermitteln und nutzen können. Nach der Gesetzesbegründung ist die Speicherung der Daten „erforderlich, um maschinelle Datenabgleiche durchführen zu können.“[205] Zwar sieht die Vorschrift eine Beschränkung auf die Erforderlichkeit „zur Erfüllung ihrer gesetzlichen Aufgaben“ vor, dennoch fehlt es ihr an der verfassungsrechtlich gebotenen Bestimmtheit. Die Vorschrift enthält nicht einmal eine Beschränkung der Zwecke im polizeilichen Bereich (Gefahrenabwehr, Strafverfolgung) und ist mit den verfassungsgerichtlichen Vorgaben zur Zweckbindung nicht in Einklang zu bringen. Insbesondere eröffnet diese Einschränkung eine immer noch zu weitgehende Verarbeitungsbefugnis, da die Vorschrift für *alle* öffentlichen Stellen gilt und der Betroffene nicht erkennen kann, für welche Zwecke seine Daten verarbeitet und genutzt werden sollen.

Es muss jedoch darauf hingewiesen werden, dass mit AFIS bzgl. einer großen Gruppe der Ausländerbevölkerung (Asylsuchende und Bürgerkriegsflüchtlinge gem. § 41a AuslG, § 16 AsylVfG) eine polizeiliche Nutzung von Fingerabdruckdaten bei völlig unverdächtigen Personen zugelassen wird (§ 78 Abs. 3 AuslG, § 16 Abs. 5 AsylVfG). Diese Regelungen werden als verfassungswidrig kritisiert.[206] Diese Kritik muss erst recht für § 5 Abs. 7 AuslG gelten.

Die Verwendung von Personalausweis und Pass im nichtöffentlichen Bereich ist in § 4 PAuswG bzw. § 18 PassG eingeschränkt. Die Dokumente dürfen danach auch hier als Ausweis- und Legitimationspapier benutzt werden. Die Seriennummer darf aber nicht zum Abruf von Dateien oder zu deren Zusammenführung verwendet werden. Auch ein automatisierter Abruf oder eine automatisierte Speicherung mithilfe der Karte ist ausdrücklich verboten. Dies schließt eine entsprechende Nutzung und dadurch auch faktisch die Weiterverarbeitung der biometrischen Daten durch Private mit aus.

---

[205] BR-Drucks. 920/01, S. 127.
[206] *Weichert*, in: Huber, Handbuch des Ausländerrechts, § 78 AuslG, Rn. 9, § 16 AsylVfG Rn. 13 m.w.N.

Eine Verwendungsregelung für andere als öffentliche Stellen (d.h. private Stellen) ist im Ausländerbereich bisher nicht vorgesehen. Diese ist aber, da die „Ausländerausweise“ voraussichtlich auch im privaten Bereich genutzt werden dürften, im Interesse der Gleichbehandlung und dem Schutz vor Datenmissbrauch durch Private dringend erforderlich.[207]

4.3.2.3 Rechte der Betroffenen

Wie in Abschnitt 2.2.2.5 dargestellt, muss dem von der Datenverarbeitung Betroffenen eine größtmögliche Information über die ihn betreffende staatliche Datenverarbeitung geboten werden. Im Hinblick auf dieses vom Bundesverfassungsgericht betonte Transparenzgebot ist es fraglich, ob die Zulassung der Verschlüsselung der Daten des Betroffenen auf dem Pass oder Personalausweis diesem Gebot nicht entgegensteht, da der Betroffene im Falle der Verschlüsselung gerade nicht sehen kann, welche Daten über ihn gespeichert sind. Da der Gesetzgeber den Betroffenen in § 16 Abs. 6 PassG und § 3 Abs. 5 PAuswG jedoch ausdrücklich ein Auskunftsrecht eingeräumt hat, ist dem Transparenzgebot Genüge getan.
Anders stellt sich die Rechtslage für Ausländer dar. Ausländern wurde ein gesetzlicher Auskunftsanspruch über den Inhalt der verschlüsselten Merkmale und Angaben gerade nicht eingeräumt.[208] Auch im Ausländerrecht ist kein ausdrücklicher allgemeiner Auskunftsanspruch vorgesehen. Dies ändert aber nichts an dem Umstand, dass auch Ausländern ein verfassungsrechtlich begründeter und über das allgemeine Datenschutzrecht normativ zugesicherter Auskunftsanspruch zusteht[209] (vgl. § 19 BDSG). Gesetzmäßige Gründe zum Ausschluss des Auskunftsanspruchs können bzgl. der auf den Ausweisdokumenten gespeicherten verschlüsselten Daten nicht zum Tragen kommen (vgl. § 19 Abs. 4 BDSG). Die Auskunftserteilung bedingt nicht eine Offenlegung des (geheimen) Schlüssels an den Betroffenen. Auch sonstige Gründe, z.B. der öffentlichen Sicherheit, begründen keine Notwendigkeit der Geheimhaltung.

Subsidiär anwendbar ist bei mobilen personenbezogenen Speicher- und Verarbeitungsmedien (Chipkarten) § 6c BDSG bzw. die entsprechende Landesregelung. Darin ist vorgesehen, dass die Betroffenen von Chipkarten u.a. über die verantwortliche Stelle, die Funktionsweise, die Wahrnehmung ihrer Betroffenenrechte sowie über die Maßnahmen bei Verlust oder Zerstörung der Karte informieren müssen.

---

[207] *Weichert* DuD 2002, 423 (425); ders. RDV 2002, 170 (175).
[208] *Garstka*, Neue Justiz 2002, 524 (525).
[209] Vgl. § 19 BDSG; dazu *Weichert*, in: *Huber*, Handbuch des Ausländerrechts, Vorbemerkung zu den §§ 75-80 AuslG, Rn. 18.

4.3.3 Technische und organisatorische Vorgaben

Angesichts der Risiken, die mit dem flächendeckenden Einsatz biometrischer Verfahren für das Recht auf informationelle Selbstbestimmung des Einzelnen verbunden sind, bedarf es hierfür besonderer technischer und organisatorischer Maßnahmen, die geeignet sind, den mit dem Masseneinsatz verbundenen Gefahren wirksam zu begegnen.

4.3.3.1 Realisierung der Speicherung des biometrischen Merkmals auf dem Identifikationspapier

Es bedarf einer detaillierten Regelung über die Modalitäten der Speicherung des biometrischen Merkmals auf dem Identifikationspapier. Es sind mehrere Szenarien denkbar, wie diese Speicherung realisiert werden könnte.

Aufdruck

Denkbar ist es, ähnlich wie das Lichtbild, biometrische Rohdaten (z.B. Fingerabdrücke, ein Lichtbild des Gesichts oder eine verkleinerte Abbildung der Handgeometrie) durch Aufdruck auf dem Ausweis zu erfassen. Möglich dürfte auch der Aufdruck eines sog. Bar-Codes sein, der digitalisiert biometrische Rohdaten oder Templates enthält. Auch der Aufdruck dieser Daten in Buchstaben (vergleichbar der Zone für das automatisierte Lesen) ist denkbar. Dies gilt auch für ggf. verschlüsselte und/oder signierte Daten; zu beachten ist jedoch, dass je nach verwendetem biometrischen Merkmal und Verfahren der Datensatz und damit der Platzbedarf für den Aufdruck unterschiedlich groß sein kann.

Chipkarten

Die Speicherung könnte elektronisch auf einer sog. Chipkarte oder einem in den Ausweis eingebrachten Chip erfolgen. Diese könnte als reine Speicherkarte (ohne Verarbeitungsfunktion) ausgelegt sein. Zu unterscheiden sind „Nur-Lese-Karten“ sowie schreibfähige Speicherkarten. Während bei „Nur-Lese-Karten“ der Datensatz bei der Produktion endgültig festgelegt wird, erlauben schreibfähige Speicherkarten auch eine nachträgliche Änderung der gespeicherten Daten (etwa Änderung von Name, Adresse oder biometrischem Merkmal), ohne dass eine Neuproduktion der Chipkarte erforderlich wird. Dies macht aber nur bei solchen Daten Sinn, die nicht zusätzlich auf der Karte bzw. dem Ausweis aufgedruckt sind, da es andernfalls zu Inkonsistenzen zwischen aufgedrucktem und gespeichertem Datenbestand kommt. Schreibfähige Speicherkarten müssen vor unbefugter Änderung sicher geschützt werden (etwa der Name), da es andernfalls zu Inkonsistenzen zwischen aufgedruckten und gespeicherten

Datenbestand kommt. Denkbar ist beispielsweise die Aktualisierung allein der biometrischer Daten innerhalb der Gültigkeitsdauer des Ausweises, etwa bei Kontrollen und Grenzübertritten, bei denen die biometrischen Daten auf den Ausweisen durch die aktuell erhobenen Daten ersetzt oder ergänzt werden. Im Hinblick auf eine revisionsfeste Datenspeicherung müsste aber genau protokolliert werden, welche Stelle wann welche Daten auf den Ausweis geschrieben hat. Schreibfähige Speicherkarten müssen vor unbefugter Änderung sicher geschützt werden, um eine Verfälschung der biometrischen Daten oder eine mutwillige Unkenntlichmachung auszuschließen.

Möglich sind aber auch Chipkarten oder aufgebrachte Chips, die Daten nicht nur speichern, sondern auch verarbeiten können (eingesetzt werden solche Karten bei der Erstellung elektronischer Signaturen). Durch geeignete Implementation könnte beispielsweise eine gegenseitige Authentisierung von Ausweis und Ausweislesegerät sichergestellt werden[210].

Zu beachten ist, dass bei einer Speicherung durch codierten Aufdruck (z.B. Barcode) oder mithilfe von Chipkarten der Betroffene nicht unmittelbar wahrnehmen kann, welche Daten auf dem Ausweis aufgebracht sind. Diesem Umstand wurde durch die Einfügung von § 3 Abs. 5 PAuswG bzw. § 16 Abs. 6 Rechnung getragen, indem den Betroffenen ein Auskunftsrecht eingeräumt wurde.

4.3.3.2 Signatur

Sollen biometrische Merkmale in verschlüsselter oder signierter Form in die Ausweise eingebracht werden (siehe Abschnitt 4.2.1.2), so stellt sich die Frage, an welcher Stelle die Verschlüsselung bzw. Signatur der Daten vorzunehmen ist. Unabhängig von der konkreten Ausgestaltung und den verwendeten Algorithmen ist die Erstellung der Verschlüsselung bzw. Signatur an einer zentralen Stelle zu bevorzugen, da die Sicherheit der Verschlüsselung bzw. Signatur in den meisten Fällen von der Geheimhaltung der verwendeten Schlüssel abhängt. Daher ist eine zentrale Erstellung der Ausweise in einer Sicherheitsumgebung, z.B. bei der Bundesdruckerei, vorzuziehen. Eine Übermittlung der Daten von den Ausgabestellen zur

[210] Damit könnte auch das Auslesen der Ausweisdaten durch Unberechtigte unterbunden werden: Nur im Fall einer erfolgreichen Authentisierung von Karte und Lesegerät übermittelt die Karte Daten an das Lesegerät, nicht aber an Replikate von Lesegeräten, die nicht im Besitz der geheim zu haltenden Authentifizierungscodes sind. Ein solcher kryptographischer Schutz dürfte qualitativ besser sein als der Schutz, der in der Geheimhaltung oder eingeschränkten Verfügbarkeit der Lesegeräte besteht.

Bundesdruckerei muss - wie gegenwärtig auch - gegen unbefugte Kenntnisnahme und Manipulation gesichert sein.

4.3.3.3 Template-Berechnung

Biometrische Rohdaten bergen einen höheren Gehalt an Informationen als die aus ihnen zu erstellenden Templates, aus denen sich in vielen Fällen ohne ein bestimmtes System, das das Auslesen dieser Templates ermöglicht, kein Informationsgehalt mehr gewinnen lässt. Es ist daher aus Datenschutzsicht empfehlenswert, die für die Erstellung des Templates erforderlichen Rohdaten zu löschen und auf ihre Aufbewahrung zu verzichten. Das Gebot zur Löschung dieser Daten folgt bereits aus dem oben unter Abschnitt 2.2.2.4 dargestellten Grundsatz der Datenvermeidung und Datensparsamkeit.[211] Datenschutzrechtlichen Problemen wird so bereits im Vorfeld begegnet, weil eine Speicherung unnötiger Daten von vornherein vermieden wird.

4.3.3.4 Zwischenspeicherung der Ergebnisse einer Verifikation an den Kontrollstellen?

Denkbar wäre es, bei automatisierten Ausweiskontrollen (etwa an Grenzübergängen etc.) die Tatsache der Kontrolle selbst oder die sogar aktuell erhobenen biometrischen Merkmale zu speichern.

Schon der erste Fall würde von der derzeitigen Praxis der Grenzkontrollen abweichen. Aktuell wird ggf. bei einem Grenzübertritt mithilfe der Zone für das automatisierte Lesen in Pässen bzw. Personalausweisen ein Abgleich mit dem aktuellen Fahndungsdatenbestand vorgenommen; bei einer Negativauskunft (d.h. Ergebnis der Abfrage ist, dass die Person nicht im Fahndungsdatenbestand enthalten ist) wird jedoch die Tatsache des Abrufes nicht gespeichert. Die Speicherung der anlässlich von Kontrollen erhobenen biometrischen Daten in Dateien der Polizei oder der Grenzkontrollbehörden wäre technisch durchaus möglich, würde aber hinsichtlich der Eingriffsintensität eine Speicherung der Tatsache des Grenzübertritts noch übersteigen und wäre als Vorratsdatenspeicherung unzulässig. Eine Rechtsgrundlage für eine solche Speicherung besteht im Übrigen außer im Falle von § 163 d StPO nicht.

---

[211] *Probst*, Biometrie aus datenschutzrechtlicher Sicht, in: *Nolde/Leger* (Hrsg.), Biometrische Verfahren, S. 115 (S. 119).

Es wäre technisch möglich, die erneute Erhebung biometrischer Daten z.B. bei der Grenzkontrolle zu nutzen, um den Datenbestand auf den Ausweisen zu aktualisieren. Dies wäre nur machbar, wenn eine Speicherung der biometrischen Daten auf dem Ausweis durch die Grenzkontrollbehörden möglich wäre (etwa bei Speichermedien in Form von Chipkarten o.ä., siehe Abschnitt 4.3.3.1); dies würde aber mannigfaltige Sicherheitsprobleme aufwerfen:

Zum einen bestünde eine erhöhte Manipulationsgefahr, wenn die Lesegeräte auch eine Schreibmöglichkeit besäßen, da eine große Anzahl von Lesegeräten im Einsatz ist und Diebstahl bzw. Manipulation einzelner Geräte nicht auszuschließen sind. Eine einzige, zentrale Stelle mit Schreibbefugnis ist leichter vor Manipulation zu schützen.

Zum anderen ist im Hinblick auf eine revisionsfeste Datenspeicherung genau zu protokollieren, welche Stelle wann welche Daten auf dem Ausweis geändert hat. Die Koordination wäre angesichts der unterschiedlichen Zuständigkeiten (Grenzpolizei und Zoll unter Bundesaufsicht, Länderpolizei und kommunale Zuständigkeiten bei der Ausweiserstellung) äußerst schwierig.

4.3.4 Folgerungen

Der Gesetzgeber hat eine Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ vorgenommen und damit von vornherein die Kombination mehrerer Merkmale ausgeschlossen. Diese Einschränkung ist nach heutigem technischen Kenntnisstand unter dem Aspekt der Falscherkennung bzw. Falschakzeptanz biometrischer Systeme nicht unproblematisch. Bei der Planung des Einsatzes biometrischer Verfahren ist auch zu berücksichtigen, dass diese für den Masseneinsatz nach heutigem technischen Stand lediglich begrenzt geeignet sind. An die Leistungsfähigkeit biometrischer Systeme sind hohe Anforderungen zu stellen. Hinsichtlich der Auswahl der einzelnen in Betracht kommenden biometrischen Merkmale ist zu berücksichtigen, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können. Rohdaten können durchaus weitere Informationen über Merkmalsträger aufzeigen. Unter dem Gesichtspunkt der Verhältnismäßigkeit ist es notwendig, die mit der Aufnahme der biometrischen Merkmale verbundenen Nebenwirkungen zu minimieren. In Betracht kommt ein Verzicht auf die Speicherung von Rohdaten. Angesichts der im AuslG eingeräumten weitergehenden Nutzungserlaubnis für die biometrischen Daten von Ausländern ist zur Verhinderung einer zweckwidrigen Nutzung

dieser Daten bei der Auswahl des biometrischen Merkmals darauf zu achten, dass das Merkmal keine Zusatzinformationen enthält.

Die vom Gesetzgeber - ohne nähere Vorgaben - geschaffene Befugnis, die Merkmale und Angaben auch in verschlüsselter Form in das jeweilige Dokument zu integrieren, wirft die Frage auf, in welcher Weise eine Verschlüsselung vorzunehmen ist bzw. die biometrischen Daten mit einer elektronischen Signatur zu signieren sind. Außerdem ist zu bestimmen, welche Stelle(n) die Verschlüsselung vornehmen bzw. die Signatur erzeugen sollen. Angesichts der hierfür erforderlichen Sicherheitsumgebung erscheint eine zentrale Erstellung der Dokumente vorzugswürdig zu sein.

Im Datenschutzrecht gilt ein aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteter strenger Zweckbindungsgrundsatz. Hinsichtlich der Bundesbürger hat der Gesetzgeber geregelt, dass die biometrischen Merkmale nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwendet werden dürfen, so dass dem Zweckbindungsgrundsatz Rechnung getragen ist. Anders ist der Bereich der „Ausländerausweise“ zu beurteilen. Die pauschale Verarbeitungsbefugnis in § 5 Abs. 7 AuslG ist mit den verfassungsrechtlichen Vorgaben zur Zweckbindung nicht in Einklang zu bringen.
Es kommen unterschiedliche Möglichkeiten der Speicherung der biometrischen Merkmale in Betracht. Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger bereits gesetzlich ausgeschlossen. Die Einrichtung zentraler Referenzdateien ist für Ausländer nicht gesetzlich ausgeschlossen. Eine solche zentrale Datenspeicherung wäre jedoch aus Gründen der Ungleichbehandlung im Sinne des Art. 3 GG und der Verhältnismäßigkeit unzulässig. Eine dezentrale Speicherung der Daten in einem Register würde die Verwendung zu strafrechtlichen Ermittlungszwecken oder zur „Rasterfahndung“ ermöglichen. Da die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, die Gefahr einer Zweckentfremdung birgt, ist auch auf die Speicherung in dezentralen Registern zu verzichten.

Für die Speicherung der biometrischen Merkmale von Ausländern wäre im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung eine Speicherung außerhalb des Ausweisdokumentes lediglich bei einer dezentralen oder zentralen Ausländerbehörde vorstellbar, wobei eine ausschließliche Bindung auf Zwecke der Datensicherung gesetzlich vorgesehen werden müsste (vgl. § 14 Abs. 4 BDSG)

5 Schlussfolgerungen

Zusammenfassend lassen sich zu den datenschutzrechtlichen Anforderungen an die Aufnahme biometrischer Merkmale in Pässe und Personalausweise von Bundesbürgern sowie „Ausländerpapieren“ folgende Thesen aufstellen:

- Biometrische Daten sind personenbezogene Daten, die den datenschutzrechtlichen Vorschriften unterliegen.

- Die Erhebung, Verarbeitung und Speicherung biometrischer Daten bedarf der Legitimierung durch eine verfassungsgemäße rechtliche Grundlage, die insbesondere dem Zweckbindungsgrundsatz genügt.

- Biometrische Merkmale dürfen nicht als sog. „Biometrische Personenkennzeichen“ verwendet werden, um Persönlichkeitsprofile über die Betroffenen zu bilden.

- Das Recht der Europäischen Union und die völkerrechtlichen Vorgaben entsprechen im Wesentlichen den deutschen verfassungsrechtlichen Rahmenbedingungen für die Verarbeitung personenbezogener Daten.

- Die europäischen Vorgaben enthalten keine konkreten, vom nationalen Gesetzgeber bei der Aufnahme biometrischer Merkmale in die jeweiligen Dokumente zu beachtenden Anforderungen. Insbesondere verpflichten europarechtliche Vorschriften den Gesetzgeber nicht zur Aufnahme biometrischer Merkmale.

- Die vom Gesetzgeber vorgenommene Einschränkung der in Betracht kommenden Merkmale auf solche von „Fingern oder Händen oder Gesicht“ lässt eine Kombination verschiedener Merkmale nicht zu.

- Nach heutigem technischen Kenntnisstand ist diese Einschränkung unter dem Aspekt der Falscherkennung bzw. Falschakzeptanz biometrischer Systeme nicht unproblematisch.

- An die Leistungsfähigkeit biometrischer Systeme sind hohe Anforderungen zu stellen. Diese müssen insbesondere für den Masseneinsatz geeignet sein. Für Menschen, die das verwendete biometrische Merkmal nicht nutzen können, bedarf es praktikabler, diskriminierungsfreier Ersatzlösungen.

- Angesichts der bei der Verwendung biometrischer Merkmale anfallenden Zusatzinformationen ist die Speicherung von Templates gegenüber der Speicherung von Rohdaten vorzuziehen.

- Solange die biometrischen Merkmale von Bundesbürgern nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwertet werden dürfen, ist insoweit dem aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteten strengen Zweckbindungsgrundsatz Rechnung getragen.

- Die pauschale Verarbeitungsbefugnis in § 5 Abs. 7 AuslG ist mit den verfassungsrechtlichen Vorgaben zur Zweckbindung nicht in Einklang zu bringen.

- Eine zentrale Speicherung der biometrischen Merkmale ist für Bundesbürger gesetzlich ausgeschlossen. Die Einrichtung zentraler Referenzdateien für Ausländer verstieße gegen Art. 3 GG sowie den Grundsatz der Verhältnismäßigkeit.

- Die Speicherung der biometrischen Merkmale von Ausländern wäre außerhalb des Ausweisdokumentes lediglich bei einer dezentralen oder zentralen Ausländerbehörde vorstellbar, wobei eine ausschließliche Bindung auf Zwecke der Datensicherung gesetzlich geregelt werden müsste.

- Eine Speicherung der biometrischen Daten ausschließlich in der Verfügungsgewalt der Betroffenen und damit allein auf dem Pass oder Personalausweis ist ausreichend zur Zweckerreichung. Sie ist damit unter dem Gesichtspunkt der Erforderlichkeit sowie der Datenvermeidung und Datensparsamkeit geboten.

Literaturverzeichnis

Albrecht, Astrid	Biometrische Verfahren im Spannungsfeld zwischen Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Reihe Frankfurter Studien zum Datenschutz, Baden Baden, 2003 (i.E)
Bäumler, Helmut/ *Breinlinger*, Astrid/ *Schrader*, Hans-Hermann (Hrsg.)	Datenschutz von A-Z, Loseblatt, Neuwied, Kriftel, Stand: Juli 2002
Bäumler, Helmut/ *Gundermann*, Lukas/ *Probst*, Thomas	Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Gutachten für den Deutschen Bundestag, vorgelegt dem Büro für Technikfolgenabschätzung beim Deutschen Bundestag, 2001
Breitenstein, Marco	Überblick über biometrische Verfahren, in: *Nolde*, Veronika/ *Leger*, Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 35 bis S. 82
Busch, Christoph/ *Daun*, Henning	Frei von Zweifel?, Biometrische Erkennung: Grundlagen, Verfahren, Sicherheit, in: c't 5/2002, S. 156 bis S. 161
Calliess, Christian / *Ruffert*, Matthias (Hrsg.)	Kommentar zu EU-Vertrag und EG-Vertrag. 2. Auflage, Neuwied 2002
Dammann, Ulrich / *Simitis*, Spiros	EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997
Denninger, Erhard/ *Hoffmann-Riem*, Wolfgang/ *Schneider*, Hans-Peter/ *Stein*, Ekkehart (Hrsg.)	Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, 3. Auflage, Neuwied/Kriftel, Loseblatt, Stand: 2001
Deutsche Vereinigung für Datenschutz (DVD)	Stellungnahme „Terrorismusbekämpfungsgesetz und Ausländer" vom 15.11.2001 (abrufbar unter http://www.aktiv.org/DVD/Themen/teaus.html)

Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Biometrische Merkmale in Personalausweisen und Pässen, vom 07.03./08.03.2002, abrufbar unter http://www.datenschutz-berlin.de/doc/de/konf/63/bio.htm
Filser, Hubert	Kontrollen im Grenzbereich - Ein neues elektronisches System soll Reisende an Flughäfen automatisch überprüfen -, in: SZ vom 11.03.2003, V2, S. 9
Fingerprint Verification Competion 2002	Ergebnisse abrufbar unter http://bias.csr.unibo.it/fvc2002
Frowein, Jochen Abr. / Peukert, Wolfgang	Europäische Menschenrechtskonvention, 2. Auflage, Kehl, Straßburg, Arlington 1996
Garstka, Hansjürgen	Terrorismusbekämpfung und Datenschutz – Zwei Themen im Konflikt, in: Neue Justiz 2002, S. 524 bis S. 525
Gemeinschaftskommentar zum Ausländerrecht	Loseblatt, Neuwied, Kriftel, Stand: 67. Aktualisierungslieferung, Juli 2002
Gola, Peter / *Schomerus*, Rudolf	BDSG Kommentar, 7. Auflage, München 2002.
Gundermann, Lukas / *Probst*, Thomas	Stichwort *Biometrie*, in: *Roßnagel*, Alexander *(Hrsg.),* Handbuch Datenschutzrecht, München 2003.
Huber, Bertold	Die Änderungen des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz, in: NVwZ 2002, S. 787 bis S. 794
Huber, Bertold (Hrsg.)	Handbuch des Ausländer- und Asylrechts, Loseblatt, München, Stand: 02/2002
Jarass, Hans D./ *Pieroth*, Bodo	Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 6. Auflage, München 2002
Kilian, Wolfgang/ *Heussen*, Benno (Hrsg.)	Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, München, Loseblatt, Stand: 15. September 2002

Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Auswirkungen des Volkszählungsurteils, in: DÖV 1984, S. 504 bis S. 510
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen (Positionspapier –AK-Technik), abrufbar unter http://www.datenschutz.mvnet.de/beschlue/63biomet.html
*Koenig,*Christian/ *Lorz*, Ralph Alexander/ *Lamprecht*, Rolf	Die Freiheit stirbt an ihrer Verteidigung, in: SZ vom 19./20. Januar 2002, Seite III
Medert, Klaus M./ *Süßmuth*, Werner	Paß- und Personalausweisrecht, Band 1: Personalausweisrecht, Band 2: Paßrecht, 2. Auflage, Köln 1992
Meyer-Ladewig, Jens	EMRK-Handkommentar, Baden-Baden 2003.
NIST (National Institute of Standards and Technology)	NIST standards for biometric accuracy, tamper resistance, and interoperability. November 13, 2002; S. 21, abrufbar unter: http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf
Nolte, Martin	Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, in: DVBl. 2002, S. 573 bis S. 578
Ohne Verfasser	Biometrik scannt Asylbewerber, in: Computerwoche 4/2003, S. 33
Ohne Verfasser	Eurodac, Aktuelles Lexikon, SZ vom 16.01.2003, S. 2
Ohne Verfasser	EU, Eurodac in Betrieb, in: DANA (Datenschutz Nachrichten), 1/2003, S. 23 bis S. 24
Ohne Verfasser	Bayern, Gesichtskontrolle per Computer, in: DANA (Datenschutz Nachrichten), 4/2002, S. 21
Ohne Verfasser	Rechtsprechung, AG Stuttgart, Beweisverwertungsverbot wegen unzulässigem automatisierten Lichtbildabruf, in: DANA (Datenschutz Nachrichten), 2/2002, S. 41 bis S. 42

Petermann, Thomas/ *Sauter*, Arnold	Biometrische Identifikationssysteme, Sachstandsbericht, TAB Arbeitsbericht Nr. 76, Februar 2002
Petri, Thomas Bernhard	Europol – transnationale polizeiliche Zusammenarbeit in Europa, Baden- Baden 2001; zugleich Dissertation Frankfurt am Main 2000/2001
Phillips, P.J./ *Grothe*r, P./ *Micheals*, R.J./ *Blackburn*, D.M./ *Tabassi*, E./*Bone*, J.M	FRVT 2002: Overview and Summary, by P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone, März 2003
	Face Recognition Vendor Test 2002 http://www.frvt.org/FRVT2002/
Probst, Thomas	Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren, in: *Bäumler*, Helmut/ *von Mutius*, Albert (Hrsg.), Anonymität im Internet, Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Braunschweig/Wiesbaden 2003
Ders.	Biometrie aus datenschutzrechtlicher Sicht, in: *Nolde*, Veronika/ *Leger*, Lothar (Hrsg.), Biometrische Verfahren, Körpermerkmale als Passwort, Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, S. 115 bis S. 128
Roggan, Frederik	Handbuch zum Recht der Inneren Sicherheit, Bonn 2003
Roßnagel, Alexander/ *Pfitzmann*, Andreas/*Garstka*, Hansjürgen	Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001
Schneier, Bruce	Angewandte Kryptographie, Bonn 1996
Schulte, Martin (Hrsg.)	Handbuch des Technikrechts, Berlin, Heidelberg, New York 2003
Sietmann, Richard	Im Fadenkreuz, Auf dem Weg in eine andere Gesellschaft, in: c't 5/2002, S. 146 bis S. 155
Simitis, Spiros	Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, in: NJW 1984, S. 398 bis S. 405

Simitis, Spiros (Hrsg.)	Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden, 2003
Tinnefeld, Marie Theres/ *Ehmann*, Eugen	Einführung in das Datenschutzrecht, 3. Auflage, München, Wien 1998
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Positionspapier zum Antiterrorgesetz der Bundesregierung vom 7. Dezember 2001, abrufbar unter: http://www.datenschutzzentrum.de/material/themen/divers/antiterr.htm
United States General Accounting Office	Technology Assessment : Using Biometrics for Border Security Report GAO-03-174, November 2002 http://www.gao.gov/new.items/d03546t.pdf
Vogelgesang, Klaus	Grundrecht auf informationelle Selbstbestimmung?, 1. Auflage, Baden-Baden 1987
Weichert, Thilo	AZRG, Kommentar zum Ausländerregistergesetz, 1. Auflage, Neuwied, Kriftel 1998
Ders.	Datenschutz für Ausländer ... nach dem 11. September, in: DuD 2002, S. 423 bis S. 428
Ders.	Automatisches Fingerabdruck-Identifizierungssystem – AFIS, in: DuD 1999, S. 167 bis S. 167
Ders.	Die Wiederbelebung des Personenkennzeichens – insbesondere am Beispiel der Einführung einer einheitlichen Wirtschaftsnummer, in: RDV 2002, S. 170 bis S. 177
Ders.	Biometrie – Freund oder Feind des Datenschutzes?, in: CR 1997, S. 369 bis S. 375
Woodward, John D.	Biometric Scanning, Law & Policy, Identifying the concerns – drafting the Biometrics Blueprint, University of Pittsburgh Law Review, 1997
Woodward, John D.	Identifying Law & Policy Concerns, in: Jain, Anil/Bolle, Ruud/Pankati, Sharath, Biometrics, Personal Identification in Networked Society, Norvell 1999, S. 385 bis 405
Ziegler, Peter-Michael	Adlerauge, Europas größte Gesichtserkennungsanlage im Zoo Hannover, in: c't 2003, S. 26 bis S. 28