DuD
Datenschutz und Datensicherheit

Biometrische Daten in Ausweisen

Alexander Roßnagel, Gerrit Hornung

Biometrische Daten im Pass und Personalausweis gefährden die informationelle Selbstbestimmung der Betroffenen. Ihre Einführung und der Umgang mit ihnen sind daher an verfassungs- und datenschutzrechtlichen Anforderungen zu messen. Der Beitrag untersucht die verfassungs- und datenschutzrechtliche Zulässigkeit der biometrischen Daten und prüft, durch welche Anforderungen an ihre Ausgestaltung die Grundrechtsrisiken auf ein vertretbares Maß reduziert werden können. [*]*

[FOTO]

Prof. Dr. Alexander Roßnagel

Vizepräsident der Universität Kassel, Univ.-Prof. für Öffentliches Recht, Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung - (provet)“ und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken
E-Mail: a.rossnagel@uni-kassel.de

Gerrit Hornung, LL.M. in European Law

Rechtsreferendar und Mitglied der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

1 Digitale Ausweise

Seit den Terroranschlägen des 11. September 2001 betreibt die Bundesregierung die Aufnahme von biometrischen Daten in den Reisepass und den Personalausweis. Dies soll die Verifikation des jeweiligen Ausweisinhabers verbessern.

Der Digitale Reisepass wird wegen der Notwendigkeit, Visa-Sticker und Stempel anbringen zu müssen, in absehbarer Zukunft im bisherigen Format erhalten bleiben und durch einen RF-Chip ergänzt werden. Der Digitale Personalausweis sollte – zur Aufnahme einer Signaturfunktion – ein Chipkartenformat erhalten. Wenn dabei ein Dual-Interface-Chip verwendet würde, könnte die RF-Schnittstelle technisch identisch mit der des Reisepasses sein. Dadurch könnten beide in gleicher Weise biometrische Daten speichern und verarbeiten. Unter biometrischen Daten sollen hier automatisiert verarbeitbare Daten über biometrische Merkmale verstanden werden. [1]

Bei der Gestaltung der Ausweissysteme sind verfassungs- und datenschutzrechtliche Rahmenbedingungen zu berücksichtigen. Sie werden im Folgenden am Beispiel des Personalausweises erörtert,[2] sind aber nahezu vollständig auch auf den künftigen Digitalen Reisepass übertragbar.

2 Datenschutzrechtliche Zulässigkeit

Die Aufnahme biometrischer Daten in einen Ausweis ist zulässig, wenn der Eingriff in das Grundrecht auf informationelle Selbstbestimmung auf einer gesetzlichen Grundlage beruht und bezogen auf den Zweck der Datenverwendung verhältnismäßig ist.

2.1 Spezifische gesetzliche Grundlage

Die Regelungen in § 1 Abs. 4 und § 3 Abs. 4 PersAuswG reichen für die Einführung biometrischer Daten nicht aus. Davon ging ausweislich § 1 Abs. 5 PersAuswG auch der Gesetzgeber aus. Bei einem derart weitreichenden Grundrechtseingriff müssen an formelle rechtsstaatliche Voraussetzungen hohe Anforderungen gestellt werden.[3] Eine Formulierung, die ausdrücklich die Wahl zwischen drei verschiedenen biometrischen Merkmalen lässt und keine Regelung über die Art der Speicherung auf dem Ausweis und in staatlichen Dateien trifft, ist nicht bestimmt genug. Vielmehr sind die genaue Art der Daten, ihre Speicherungsform (Volldatensatz oder Templates), ihr Speicherort (auf der Karte; ob und wenn ja wo und in welcher Form in staatlichen Dateien), die weitere Verwendung im Rahmen von Kontrollen und eventuelle Zugriffsrechte in einem Parlamentsgesetz zu regeln.

Auch wenn § 1 Abs. 4 PersAuswG für die Einführung biometrischer Daten unzureichend ist, trifft er doch spezifische Festlegungen, die unter Umständen Änderungen des Gesetzestextes erforderlich machen. Sollte sich der Iris-Scan als das zu bevorzugende biometrische Verfahren erweisen, müsste dieses in den Text aufgenommen werden, weil die Iriserkennung nicht unter das Merkmal „Gesicht“ subsumiert werden kann.[4] Das Gleiche wäre erforderlich, sollte sich eine kombinierte Anwendung verschiedener biometrischer Daten als die geeignetste Lösung erweisen. Nach der Gesetzesbegründung sind die drei Körperbereiche „alternativ“ zu verstehen.[5]

[*] Die folgenden Überlegungen gehen u.a. auf Arbeiten zurück, die im Rahmen der „Machbarkeitsstudie Digitaler Personalausweis“ im Auftrag des Bundesministeriums für Wirtschaft und Arbeit 2003/04 erstellt wurden.

[1] S. zum Personenbezug biometrischer Daten Hornung, DuD 2004, 429 ff.

[2] S. näher Reichl/Roßnagel/Müller, Machbarkeitsstudie Digitaler Personalausweis, 2005.

[3] S. allgemein z.B. v. Mangoldt/Klein/Starck-Starck, GG, 4. Aufl. 1999, Art. 2 Rn. 109.

[4] Es sind unterschiedliche Erkennungssysteme mit unterschiedlichen datenschutzrechtlichen Problemen. Der Gesetzgeber sah den Finger nicht als Teil des Merkmals „Hand“. Gleiches muss auch für Gesicht und Iris gelten.

[5] BT-Drs. 14/7386, 47.

2.1 Verhältnismäßigkeit

In materieller Hinsicht muss der Eingriff dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit genügen. Zweck der Einführung biometrischer Daten in einen Ausweis ist der Schutz vor Identitätsmanipulationen. Damit soll „die zweifelsfreie Feststellung der Übereinstimmung der Identität" des Ausweisinhabers mit der „Identität der zu kontrollierenden Person durch ein computergestütztes Verfahren ermöglicht" werden.[6] Der verfolgte Zweck besteht also nur in der Verifikation einer Identität (1:1-Vergleich), nicht in der Identifizierung einer Person (1:n-Vergleich). Dieser Zweck ist grundsätzlich legitim und verfassungsrechtlich akzeptabel.

2.2.1 Eignung

Um den beschriebenen Zweck zu erreichen, müssen biometrische Systeme eine hinreichend geringe Fehlerrate aufweisen. Für den Zweck des Manipulationsschutzes sind diese nur geeignet, wenn sie eine niedrigere Falschakzeptanzrate (FAR) aufweisen als Sichtkontrollen. Zugleich muss aber auch die Falschzurückweisungsrate (FRR) niedrig sein, weil ansonsten intensive Nachkontrollen erforderlich sind.

> Im Ergebnis sind für die Eignung automatischer Kontrollen Fehlerraten (FAR und FRR) von unter 1 % zu fordern. Diese Anforderung dürfte derzeit nur die Iriserkennung erfüllen.

Die Leistungsfähigkeit der verschiedenen Verfahren wird derzeit in mehreren Pilotverfahren getestet[7] und wird bislang durchaus skeptisch beurteilt.[8] Jedenfalls gibt es bislang keine wirklichen Erkenntnisse über die Verwendbarkeit in einem Verfahren mit 62 Mio. Teilnehmern (Deutsche über 16 Jahren) – noch dazu, wenn diese Gruppe auch technisch nicht versierte, skeptische oder behinderte Menschen umfasst. Mit Ausnahme des Gesichts, bei dem praktisch alle Betroffenen erfasst werden können, gibt es bei jedem biometrischen Verfahren eine gewisse Zahl von Bürgern, die das Merkmal entweder nicht oder nicht in hinreichender Ausprägung besitzen.[9] Auch die Langzeitstabilität der Merkmale ist bislang wenig erforscht. Um die Eignung eines Systems für die Gesamtbevölkerung seriös feststellen zu können, ist zumindest ein groß angelegter Feldversuch erforderlich.

Die Eignung könnte durch die Kombination zweier Verfahren erhöht werden, wie sie Ende 2004 für den Reisepass der EU normiert wurde (Gesicht und Fingerabdruck). Verlangt man allerdings für eine Akzeptanz ein positives Abgleichergebnis in beiden Verfahren, so wird zwar die FAR reduziert, gleichzeitig steigt jedoch die FRR. Wenn jedoch eine positive Prüfung ausreicht, so besteht die Möglichkeit, auch Personen zu identifizieren, bei denen eines von zwei Merkmalen dauerhaft oder temporär nicht zur Authentisierung geeignet ist. Auch in diesem Fall muss allerdings ein effektives Rückfallsystem eingerichtet werden, um im Fall der Nichteignung des Betroffenen oder der (unmerklichen) Zerstörung des Ausweischips eine Identifizierung zu ermöglichen. Ohne ein solches Rückfallsystem ist die Einführung biometrischer Daten nicht geeignet.

2.2.2 Erforderlichkeit

Unterstellt man hinreichend geringe Fehlerraten der biometrischen Verifikation auch bei einer Anwendung auf die Gesamtbevölkerung, so gibt es kein weniger belastendes, gleich geeignetes Mittel zur Erreichung einer sicheren Verbindung zwischen Person und Ausweis. Unter gleich geeigneten biometrischen Verfahren ist das zu wählen, das den geringsten Eingriff in Grundrechte verursacht. Dabei lassen sich drei Hauptkriterien ausmachen.

Zunächst ist wichtig, inwieweit ein Merkmal überschießende Informationen enthält.[10] Es dürfen nämlich nur so viele Daten über die betroffene Person erhoben werden, wie unabdingbar benötigt werden. Aus Gesichtsinformationen kann man auf die ethnische Herkunft und das Geschlecht schließen. Der Zusammenhang mit Gesundheitsinformationen ist umstritten. Genannt werden etwa die Möglichkeit, vom Augenhintergrund auf Arteriosklerose, Diabetes und Bluthochdruck zurück zu schließen.[11] Aus dem Fingerabdruck sollen sich Informationen über chronische Magen-Darm-Beschwerden, Leukämie und Brustkrebs ergeben.[12] In jedem Fall sind dies immer nur bestimmte Korrelationen, es ist nicht möglich, definitive Aussagen zu treffen. Auch wissenschaftlich strittige Risiken sind jedoch bei der Merkmalsauswahl zu berücksichtigen, da auch potentielle zukünftige überschießende Informationen bereits jetzt in die Entscheidung einzubeziehen sind.

Das zweite Kriterium ist das der Flüchtigkeit. Hinterlassen biometrische Merkmale dauerhafte Spuren, so besteht ein erheblich größeres Risiko, dass diese Spuren erhoben und die so gewonnenen Daten mit den für den Ausweis erhobenen Daten verglichen werden.[13] Hier schneidet die Iris am besten ab, weil sie nirgendwo Spuren hinterlässt. Dies gilt auch für das Gesicht. Dagegen wird der Fingerabdruck unwillentlich in der Umgebung hinterlassen. Insofern besteht zum Beispiel das Risiko einer Datenerhebung von Alltagsgegenständen.

Schließlich ist die Mitwirkungsgebundenheit relevant. Eine unbemerkte Datenerhebung ist bei der Gesichtserkennung am einfachsten, weil diese ohne Mitwirkung und Wissen der betroffenen Person erfolgen kann.[14] Die damit verbundenen Risiken werden verstärkt, wenn mit kontaktlosen Chips auf dem Ausweis gearbeitet wird, weil dann der komplette Abgleichvorgang ohne jede Kenntnis des Ausweisinhabers vonstatten gehen kann. Dies ist bei der Iriserkennung erheblich schwieriger.[15] Gleiches gilt auch für den Fingerabdruck, wenn auch – durch umständliche Verfahren – ein geeigneter Fingerabdruck auf einem Gegenstand genutzt werden könnte.

---

[6] Amtl. Begründung, BT-Drs. 14/7386, 48.

[7] In Deutschland v.a. in den Projekten BioFace, BioFinger, BioP I und BioP II.

[8] Nach Büro für Technikfolgenabschätzung (TAB), Biometrische Identifikationssysteme, BT-Drs. 14/10005, 4, 9, 49; 63. Konferenz der DSB 2002, DuD 2002, 247, unter 3.2 war die Zuverlässigkeit biometrischer Systeme 2002 nicht seriös abschätzbar und keines der Verfahren erfüllte alle Praxisanforderungen. Es fehlt überdies an allgemeingültigen Evaluierungskriterien, s. Gundermann/Probst, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 9.6, Rn. 27.

[9] Gundermann/Probst (Fn. 8), Rn. 10 (2 %); TAB (Fn. 8), 23 (5 %); s. auch Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003, 36.

[10] Gundermann/Probst (Fn. 8), Rn. 26f.; Golembiewski/Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren, 2003, http://www.datenschutzzerum.de/download/Biometrie_Gutachten_Print.pdf, 64f.; Albrecht (Fn. 9), 172.

[11] Gundermann/Probst (Fn. 8), Rn. 26.

[12] Johns Hopkins Physician Update: Gastoenterology: Fingerprinting GI Disease, p. 5, zit. nach Gundermann/Probst (Fn. 8), Fn. 38.

[13] Golembiewski/Probst (Fn. 10), 53.

[14] 63. Konferenz der DSB, DuD 2002, 247; Weichert, CR 1997, 369, 374.

[15] Auch wenn es Verfahren gibt, die eine Merkmalserhebung aus einem Meter Entfernung zulassen, s. Behrens/Roth, Biometrische Identifikationssysteme, 2001, 14; TAB (Fn. 8), 15. Dennoch ist in der Regel eine Kooperation des Ausweisinhabers erforderlich.

2.2.3 Zumutbarkeit

> Eine maßvolle Verwendung biometrischer Daten, die tatsächlich eine deutliche Verbesserung der Zuverlässigkeit von Ausweiskontrollen bewirkt und durch ausreichende technische, organisatorische und rechtliche Sicherungen (s. 3.) die Grundrechtsbeeinträchtigung auf das geringst mögliche Maß reduziert, wäre in der Abwägung zwischen den Vorteilen für die Allgemeinheit und den Beeinträchtigungen des Einzelnen für diesen objektiv zumutbar.

Dies gilt letztlich auch für eine Kombination zweier biometrischer Verfahren, wenn dies das einzig mögliche Mittel ist, um das legitime Ziel einer höheren Zuverlässigkeit von Ausweisprüfungen zu erreichen. Verfassungsrechtlich erforderlich ist allerdings die Vermeidung ungerechtfertigter Belästigungen oder Diskriminierungen durch die Verwendung biometrischer Merkmale.

Außerdem ist zu berücksichtigen, dass die Merkmale für bestimmte biometrische Verfahren bei einem bestimmten Anteil der Bevölkerung permanent oder zeitweilig unzureichend ausgeprägt sind oder aus anderen Gründen nicht genutzt werden können. Für diese Gruppe müssen andere, nicht diskriminierende Kontrollverfahren gefunden werden. Um Belästigungen und Belastungen von vornherein auszuschließen, müsste auf und in den Ausweis ein Hinweis angebracht werden, dass dieses oder jenes Verfahren nicht angewandt werden kann.

Auch ist zu berücksichtigen, dass die biometrischen Verfahren – in einer unter Hinblick auf Art. 3 GG bedenklichen Weise – unterschiedlich wirksam sind. So sollen zum Beispiel Verfahren der Gesichtserkennung Männer mit bis zu 9% besser erkennen als Frauen.[16] Menschen mit bestimmtem rassischem Hintergrund (Fernost) können außerdem Probleme mit dem Iris-Scan haben. Beim Fingerabdruck können sich Diskriminierungen bestimmter Berufsgruppen ergeben, die durch starke körperliche Arbeit Veränderungen am Fingermuster erfahren.

3 Anforderungen an den Datenumgang

Aus dem Verfassungs- und Datenschutzrecht ergibt sich eine Reihe von Anforderungen, die bei der Gestaltung von Ausweissystemen und für den Umgang mit biometrischen Daten zu beachten sind und als Rahmenbedingungen die Machbarkeit des Gesamtsystems beeinflussen.

3.1 Form der Daten

Fraglich ist, in welcher Form biometrische Daten gespeichert werden dürfen. In Frage kommen Volldatensätze oder Templates. Erstere sind insbesondere deshalb problematisch, weil sie erheblich mehr Informationen über den Merkmalsträger beinhalten, die Klassifizierung der Betroffenen nach unzulässigen Kriterien erleichtern und die Gefahr von Profilbildungen erhöhen. Nach dem Kriterium der Verhältnismäßigkeit und dem Grundsatz der Datensparsamkeit in § 3a BDSG sind Templates daher vorzuziehen.[17] Das gilt umso mehr, als diese Betriebsart geringere Fehlerraten aufweist.[18]

Mangels Standardisierung von Templates für die meisten biometrischen Verfahren, insbesondere für das Gesicht, hat sich die ICAO für die Verwendung von Volldatensätzen ausgesprochen.[19] Für diese unverbindlichen Empfehlungen besteht zwar keine Verpflichtung, sie in nationales Recht umzusetzen. Wenn jedoch Ausweise als Reisedokumente europa- oder weltweit einsetzbar sein sollen, müssen ihre Daten für alle Grenzkontrollstellen prüfbar sein. Hierfür sind Templates mangels Kompatibilität in den meisten Fällen ungeeignet.

> Im Ergebnis sind deshalb immer dann Templates zu verwenden, wenn für das jeweilige Merkmal internationale Standards zur Verfügung stehen. Ist das nicht der Fall, dürfen – die Eignung zur Verifikation vorausgesetzt – Volldaten verwendet werden.

Die Bundesrepublik Deutschland muss jedoch im Interesse des Grundrechtsschutzes ihrer Bürger auf eine internationale Standardisierung hinwirken.

3.2 Sicherungsmaßnahmen

Biometrische Daten sind zur Identitätsprüfung nur dann geeignet, wenn ihre Integrität gesichert ist. Hierzu sollten bei der Herstellung des Ausweises elektronische Signaturen verwendet werden. Die ICAO hat einen Vorschlag für den Aufbau einer weltweit interoperablen Prüfinfrastruktur vorgelegt, in dem sie für den Austausch der Prüfschlüssel sorgen und so als „de facto"-Zertifizierungsinstanz agieren soll.[20]

Der Zugriffsschutz der biometrischen Daten erfordert zum einen die gegenseitige Authentifizierung von Kontrollgerät und Ausweischip.[21] Hierdurch ließe sich der Zugriff auf zertifizierte Kontrollgeräte beschränken. Daneben könnte dem Ausweisinhaber die Möglichkeit gegeben werden, die biometrischen Daten selbst für Identifizierungszwecke (zum Beispiel im privaten Bereich) frei zu schalten.

Zum anderen ist ein Zugriffsschutz nach § 1 Abs. 4 Satz 2 und 3 PersAuswG durch Verschlüsselung sicher zu stellen.[22] Die Ausweisdaten müssen danach in einer „mit Sicherheitsverfahren verschlüsselten Form in den Personalausweis eingebracht" werden.[23] Faktisch ergibt sich jedoch das Problem, dass bei einer Verwendung symmetrischer Schlüssel diese europa- oder weltweit an die Kontrollstellen verteilt werden müssten und so kaum dauerhaft geheim zu halten sind. Aus staatlicher Sicht bedeutet die Verschlüsselung damit keine wirkliche Sicherung, da mit entsprechender krimineller Energie (Diebstahl eines Entschlüsselungsgeräts, Erpressung oder Bestechung von Beamten) eine Entschlüsselung möglich ist. Dennoch sichert eine Verschlüsselung das Grundrecht auf informationelle Selbstbestimmung. Es ist nämlich nicht davon auszugehen, dass der Entschlüsselungsschlüssel in der Öffentlichkeit allgemein bekannt wird. Damit besteht zumindest eine Sicherung gegen ein weit verbreitetes missbräuchliches Auslesen und Verwenden der biometrischen Daten, insbesondere im privaten Umfeld. Dies gilt umso mehr beim

[16] S. Reichl/Roßnagel/Müller (Fn. 2), Teil II, 2.4.1.2.

[17] Albrecht (Fn. 9), 2003, 158.

[18] BioP 1, http://www.bsi.de/literat/studien/biop/index.htm, 10, 49.

[19] ICAO, Biometrics Deployment of Machine Readable Travel Documents, Version 1.9, 2003, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm, 17, 14.

[20] ICAO, PKI Digital Signatures for Machine Readable Travel Documents. Version 4.0, 19. 2003, http://www.icao.int/mrtd/Home/Index.cfm.

[21] S. Reichl/Roßnagel/Müller (Fn. 2), Teil II, 2.3.

[22] S. 63. Konferenz der DSB, DuD 2002, 247, 3.1 und 5.

[23] Wie sich aus § 1 Abs. 4 Satz 3 PersAuswG ergibt, eröffnet der missverständliche Wortlaut keine Wahlmöglichkeit hinsichtlich der Verschlüsselung. Auch die Zweckbeschränkung des § 3 Abs. 5 Satz 1 PersAuswG muss für alle elektronisch gespeicherten Daten gelten. Sie auf verschlüsselte Daten zu beschränken, ungeschützte Daten aber von der Zweckbindung auszunehmen, wäre mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar.

Einsatz von kontaktlosen Übertragungssystemen. Selbst wenn das Entschlüsselungsgeheimnis allgemein bekannt werden sollte, wäre seine missbräuchliche Verwendung eine Straftat nach § 202a StGB.[24] Der dadurch bewirkte Abschreckungseffekt stellt eine zusätzliche Sicherung dar. Aufgrund dessen ist eine Verschlüsselung trotz der genannten Kompromittierungsgefahren zum Schutz der Daten geboten.

Sofern der Ausweis weitere Funktionen erfüllen soll, wie etwa Verschlüsselungs-, Authentifizierungs- und Signaturfunktionen für seinen Inhaber,[25] müssen diese strikt von den hoheitlichen Identifikationsdaten getrennt werden.[26] Letztere dienen vor allem staatlichen Zwecken und müssen gegenüber jedermann gegen Manipulation geschützt werden. Sie sind außerdem vor dem Zugriff Dritter zu schützen, dem Ausweisinhaber aber zur Verwendung zur Verfügung zu stellen. Die Daten eines elektronischen Ausweises[27] und der Funktionalitäten der Signatur, Authentifizierung und Verschlüsselung sind gegen den Zugriff anderer zu schützen, wobei dies auch den Schutz vor staatlichen Stellen einschließt. Die Datentrennung kann durch die Verwendung getrennter Chips erreicht werden. Sofern die Funktionsweise des verwendeten Mikroprozessors allerdings eine saubere Datentrennung garantiert, spricht nichts dagegen, verschiedene Funktionalitäten innerhalb ein und desselben Chips anzusiedeln.

3.3 Ort der Speicherung

§ 1 Abs. 5 Satz 2 PersAuswG stellt für biometrische Daten kategorisch fest: „Eine bundesweite Datei wird nicht eingerichtet." Diese Regelung ist verfassungsrechtlich geboten. Denn eine zentrale Speicherung solcher Daten begründet wegen der Problematik des – legalen oder illegalen – Zugriffs, der Weiterverwendung der Daten und ihrer Übermittlung für andere Zwecke hohe datenschutzrechtliche Risiken[28] und ist gleichzeitig für die Funktionsfähigkeit (Verifikation) des Digitalen Personalausweises nicht erforderlich. In manchen Staaten[29] wird eine zentrale Datenbank zwar verwendet, um die Mehrfachbeantragung unter falschem Namen zu verhindern. In Deutschland besteht hierfür jedoch aufgrund des hochentwickelten Meldewesens keine Notwendigkeit. Im Vergleich zu den beschriebenen grundrechtlichen Risiken der zentralen Datenspeicherung wären mögliche Verbesserungen überdies so geringfügig, dass eine zentrale Speicherung auch objektiv unzumutbar wäre.

> Eine bundesweite Datenbank für biometrische Daten aller Deutschen – ob zentral oder dezentral-vernetzt – ist daher verfassungswidrig.

Dies muss letztlich auch für – theoretisch mögliche – abgeschottete Speicherungen bei den Personalausweisbehörden gelten. Das geltende PersAuswG hält eine solche Speicherung für Ausweiszwecke nicht für erforderlich, indem es in § 2a Abs. 1 Satz 2 die Registerdaten abschließend bestimmt und in § 3 Abs. 2 andere Register untersagt. Für den gesetzlichen Zweck, die Echtheit des Dokuments und die Identität des Ausweisinhabers zu überprüfen, reicht es aus, die Vergleichsdaten im Ausweis selbst zu speichern und Authentizität und Integrität durch elektronische Signaturen sicherzustellen. Eine dezentrale Speicherung ist auch nicht erforderlich, um bei der Neubeantragung auf bereits vorhandene Daten zurückgreifen zu können. Hierzu bietet sich als milderes Mittel die Neuerhebung an. Diese ist schon wegen der Veränderung biometrischer Merkmale über die Zeit und wegen der zu erwartenden technischen Veränderung der Verfahren erforderlich.

> Eine weitergehende Verwendung biometrischer Daten, etwa für die Strafverfolgung, bedürfte einer eigenständigen Rechtsgrundlage. Ob eine solche Speicherung verfassungsrechtlich zulässig ist, erscheint äußerst zweifelhaft, weil die Erhebung von Daten über biometrische Merkmale ausnahmslos aller Deutscher für den Fall, dass bei einer seltenen anderweitig nicht aufklärbaren – sehr schweren[30] – Straftat auf diese Daten zurückgegriffen werden kann, eine unzulässige Vorratsdatenspeicherung und einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt.[31]

Außerdem wird zu Recht auf das Risiko hingewiesen, dass ein einmal eingerichteter öffentlicher Datenbestand trotz zunächst enger Zweckbestimmung auf Dauer auch für andere Zwecke genutzt wird. Bei einer Verwendung der biometrischen Daten zu anderen Zwecken als zur Identitätsprüfung entsteht leicht das Risiko der schleichenden Einführung eines verfassungswidrigen allgemeinen Personenkennzeichens.[32]

3.4 Datenübermittlung

Nach § 2a Abs. 2 PersAuswG dürfen die Ausweisdaten aus dem Personalausweisregister der jeweiligen Personalausweisbehörden an andere Behörden übermittelt werden. Da die Personalausweisregister keine Daten über biometrische Merkmale enthalten dürfen, spielt diese Übermittlungserlaubnis für diese Daten keine Rolle.

Nach § 3a Abs. 1 Satz 2 PersAuswG darf der Ausweis von Polizei- und Zollbehörden für Zwecke der Grenzkontrolle sowie der Fahndung oder Aufenthaltsfeststellung aus Gründen der Strafverfolgung, Strafvollstreckung und der Abwehr von Gefahren für die öffentliche Sicherheit zum automatischen Abruf personenbezogener Daten verwendet werden, die im polizeilichen Fahndungsbestand geführt werden. Die Regelung würde auch den Abgleich mit biometrischen Datenbanken dieser Behörden erfassen. Dies wird jedoch durch die abschließende Zweckbestimmung in § 3 Abs. 5 PersAuswG ausgeschlossen. Eine Änderung dieser Gesetzeslage wäre nur unter erheblichen Einschränkungen verfassungsgemäß. Die Datenübermittlung müsste auf die Fahndung wegen des dringenden Verdachts einer schwerwiegenden Straftat beschränkt werden. Außerdem müsste gefordert werden, dass weniger belastende Fahndungsmethoden erfolglos versucht worden sind oder aussichtslos erscheinen.

3.5 Datenabgleich

> Ein Grundproblem des Abgleichs biometrischer Daten ist, dass (auch bei der Verwendung von Templates) dabei stets

[24] Bei Handeln gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht kommt auch § 44 Abs. 1 BDSG in Betracht.

[25] S. hierzu Roßnagel und Gitter/Strasser in diesem Heft.

[26] S. z.B. Weichert, DuD 1997, 266, 269; ders., in: Roßnagel, (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 9.5, Rn. 42f.

[27] S. zu diesem Roßnagel, DuD 2002, 281 ff.; Reichl/Roßnagel/Müller (Fn. 2), Teil I, 4.6.2; Teil II, 2.9.2.

[28] 63. Konferenz der DSB, DuD 2002, 247, unter 5; Golembiewski/Probst (Fn. 10), 69f., 72; Albrecht (Fn. 9), 162 ff.

[29] Z.B. Malaysia, Oman und Brunei.

[30] Für die Aufklärung geringerer Straftaten wäre die Datenverarbeitung erst recht unverhältnismäßig.

[31] Auch das BVerfG hat für eine begrenzte Gendatenbank (Vorbestrafter) hohe Anforderungen formuliert, s. BVerfGE 103, 21.

[32] 63. Konferenz der DSB, DuD 2002, 247, unter 4 und 5; Brandenburg. LDSB, 11. TB 2002, 21.

beim Ausweisinhaber aktuell Volldaten erhoben werden müssen. Für diese ist sicherzustellen, dass sie nur im technisch notwendigen Umfang und Zeitraum zwischengespeichert und nicht aufbewahrt oder gar mit den sonstigen Persönlichkeitsdaten des Ausweisinhabers verknüpft oder zu anderen Zwecken verwendet werden.

Daneben ist der Ort des Abgleichs von Bedeutung. Weil eine Speicherung außerhalb des Ausweises unzulässig ist, könnte ein Abgleich auf der Karte (Matching-on-Card) erforderlich sein. Dies wäre datenschutzrechtlich vorzugswürdig, weil dabei die Referenzdaten den Einflussbereich des Betroffenen nie verlassen. Allerdings stößt Matching-on-Card auf eine Reihe von Problemen. Diese Betriebsart ist bislang nur mit Templates durchführbar, die nicht für alle biometrischen Merkmale standardisiert sind. Außerdem besteht aus staatlicher Sicht das Risiko eines gefälschten Chips, der unabhängig von den neu erhobenen Daten stets ein positives Abgleichergebnis nach außen sendet. Ein echter datenschutzrechtlicher Vorteil ließe sich nur mit einem Sensor auf der Karte erreichen, der jedoch nur für den Fingerabdruck realistisch ist und auch bei diesem bislang auf technische Schwierigkeiten stößt.[33] Bei einer Erhebung der Vergleichsdaten (Volldatensatz) außerhalb der Karte besteht der Vorteil eines Abgleichs auf dem Ausweis allein darin, dass die Referenzdaten nicht missbräuchlich ausgelesen werden können.

Dem Risiko des missbräuchlichen Auslesens kann ebenso durch eine Authentifizierung des Lesegeräts gegenüber der Karte begegnet werden. Soweit dieses Verfahren sicherstellt, dass biometrische Daten nur an zertifizierte Leser übermittelt und diese ausschließlich zu einem Abgleich der Daten benutzt werden können, sind die beiden Verfahren wegen des ohnehin erforderlichen Erhebens von Volldaten in der Peripherie datenschutzrechtlich ähnlich zu beurteilen.

Bezüglich des Datenabgleichs verlangt der Transparenzgrundsatz, die biometrischen Daten gegenüber dem Betroffenen offen und für ihn bemerkbar zu erheben.[34] Um die notwendige Transparenz zu gewährleisten und Datenschutzrisiken auszuschließen, sind kontaktorientierte Systeme kontaktlosen grundsätzlich vorzuziehen, solange nicht durch technische Maßnahmen sichergestellt ist, dass kein unbemerktes Datenauslesen stattfinden kann. Auch hier kommen gegenseitige Authentisierungsverfahren zur Absicherung in Frage.

Solange biometrische Systeme eine Falschabweisung nicht mit an Sicherheit grenzender Wahrscheinlichkeit ausschließen können, werden fälschlicherweise zurückgewiesene Ausweisinhaber einer hohen Belastung ausgesetzt. Gleiches gilt für die Gruppe derjenigen, die dauerhaft oder temporär nicht zur biometrischen Erkennung geeignet sind. Außerdem wird es stets einen Grenzbereich zwischen zum Enrolment geeigneten und ungeeigneten Personen geben. Werden die Merkmalsträger in diesem Grenzbereich als zur Nutzung geeignet definiert, so sind individuell höhere Fehlerquoten zu erwarten, mit dem Ergebnis, dass diese Gruppe sogar schlechter gestellt wird als Ausweisinhaber, die klar ungeeignet sind.

Damit der Einsatz biometrischer Daten beim Ausweis auch insoweit objektiv zumutbar ist, sind Maßnahmen erforderlich, um eine zügige manuelle Nachkontrolle zu ermöglichen. Hier wie bei den Gruppenmerkmalen des Art. 3 Abs. 3 GG gilt, dass die Ungleichbehandlung deswegen schwerwiegend ist, weil sie durch die Betroffenen nicht beeinflusst werden kann.[35] Insoweit sind an die zu fordernden staatlichen Ausgleichsmaßnahmen keine geringen Anforderungen zu stellen. Keinesfalls dürfen Personen also allein wegen der abweisenden Entscheidung des biometrischen Systems zurückgewiesen werden. Ausweiskontrollen müssen technisch so beschaffen sein, dass eine herkömmliche, manuelle Ausweisprüfung jederzeit möglich ist. Darüber hinaus ist die Bereitstellung von hinreichenden personellen und räumlichen Ressourcen erforderlich, um eine Überprüfung in einem Zeitraum zu ermöglichen, der insbesondere an den Grenzen und Flughäfen nicht zu unverschuldeten Verzögerungen auf Seiten der Reisenden führt.

Ein Sonderproblem ist der Einsatz der biometrischen Daten im privaten Umfeld. Der Ausweis kann gemäß § 4 Abs. 1 PersAuswG auch hier als Ausweis- und Legitimationspapier eingesetzt werden. § 4 Abs. 3 PersAuswG verbietet aber die Verwendung zum automatischen Abruf und zur automatischen Speicherung personenbezogener Daten. Das erfasst auch die biometrische Authentifikation, die ohne dies nicht vorstellbar ist. Aufgrund der vielfältigen Nutzungsmöglichkeiten im privaten Bereich erscheint es aber vertretbar, unter dem Vorbehalt der Einwilligung des Ausweisinhabers und der Bindung an zertifizierte Kontrollgeräte, bei denen ein Mitschnitt der erhobenen Daten technisch ausgeschlossen ist, § 4 Abs. 3 PersAuswG entsprechend anzupassen.

6. Ausblick

Biometrische Daten in digitalen staatlichen Ausweisen sind verfassungs- und datenschutzrechtlich dann möglich, wenn die damit verbundenen Grundrechtsrisiken bei der Auswahl der Biometrieverfahren und der Gestaltung der Ausweissysteme durch die beschriebenen technischen, organisatorischen und rechtlichen Sicherungsmaßnahmen auf das geringst mögliche Maß reduziert werden.

Diese Anforderungen des deutschen Verfassungsrechts drohen jedoch durch die internationale[36] und europäische[37] Abstimmungen der Verfahren und Systeme – unter tätiger Mithilfe deutscher Stellen – unterlaufen zu werden. Werden die biometrischen Daten in Reisedokumenten weltweit – wenn auch nur informell – abgestimmt, sind letztlich auch nach deutschem Verfassungsrecht nur noch die Biometrieverfahren und ihre Ausgestaltungen für den Zweck eines Reisedokuments geeignet, die weltweit einsetzbar sind. Werden diese Fragen für die Pässe in einer EU-Verordnung abschließend geregelt, gelten sie in den Mitgliedstaaten unmittelbar, auch wenn hinsichtlich einer gemeinsamen Justiz- und Innenpolitik im Rahmen des Verfahrens nach Art. 62 Nr. 2 a) i.V.m. Art. 67 EGV das europäische Parlament lediglich angehört werden muss und die Entscheidung letztlich nur von den Innenressorts aller Mitgliedstaaten getroffen wird. Angesichts der Regelung in § 1 Abs. 4 PersAuswG, mit der sich der Bundestag ausdrücklich eine abschließende Entscheidung vorbehalten hat, gefährden solche Taktiken nicht nur die Grundrechte, sondern auch die Demokratie.

[33] S. Reichl/Roßnagel/Müller (Fn. 2), Teil I, 4.1.2.2.

[34] Albrecht (Fn. 9), 169.

[35] S. BVerfGE 88, 87 (96); 91, 389 (401).

[36] S. die Dokumente unter http://www.icao.int/mrtd/Home/Index.cfm.

[37] S. Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States. Noch nicht im Amtsblatt veröffentlicht.