Rechtsgrundlage für den biometrischen Reisepass: Das Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften vom 24. Mai 2007[1]

Dr. Gerrit Hornung, LL.M.

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

Abstract: Die Bundesregierung hat die erste Stufe der Veränderung des Reisepasses – die Ergänzung um einen RFID-Chip mit biometrischen Gesichtsdaten – ohne Veränderung der passrechtlichen Grundlagen vorgenommen. Für die nunmehr in der zweiten Stufe geplante zusätzliche Speicherung der Fingerabdrucksdaten verabschiedete der Bundestag Ende Mai 2007 gesetzliche Grundlagen, die die Vorgaben der EG-Verordnung 2252/2004 übernehmen, notwendige Folgeregelungen umsetzen und weitere Veränderungen des Passgesetzes und anderer Gesetze enthalten. Der Beitrag skizziert die bisherige Entwicklung, erläutert den Inhalt des Gesetzes und nimmt eine rechtliche Bewertung vor.

1 Einleitung

In Deutschland werden seit dem 1. November 2005 neue Reisepässe ausgegeben, die einen kontaktlosen (RFID-)Chip enthalten, auf dem biometrische Daten des Gesichts gespeichert sind. Bislang haben sich dadurch für die Bürger lediglich die Gebühr und die Art des beizubringenden Gesichtsbildes verändert. Die Gebühr wurde von 26,- auf 59,- Euro (beziehungsweise von 13,- auf 37,50 Euro bei Ausstellung vor Vollendung des 26. Lebensjahres) angehoben. Anstelle des bisherigen Halbprofils ist eine standardisierte Frontalaufnahme bereitzustellen. Die zusätzliche Speicherung von Fingerabdrucksdaten bedingt hingegen veränderte Prozesse der Datenerhebung. Außerdem wird künftig die Passkontrolle regelmäßig auch die biometrische Verifikation des Inhabers beinhalten.

Der Gesetzesentwurf der Bundesregierung [BRe07] bezweckte die Normierung dieser Neuerungen. Er wurde im Bundestag von CDU/CSU und SPD mit leichten Veränderungen gegen den Widerstand der Fraktionen der FDP, von BÜNDNIS 90/DIE GRÜNEN und DIE LINKE am 24. Mai 2007 auf der Basis der Beschlussempfehlung des Innenausschusses [Inn07] verabschiedet.

[1] Eine frühere Version dieses Beitrags ist erschienen in Datenschutz und Datensicherheit (DuD) 2007, 181 ff.

Die Aufnahme von Fingerabdrucksdaten ist für November 2007 geplant und soll keine weitere Gebührenerhöhung mit sich bringen [BRe07, 26]. Kosten und Verteilung zwischen Bund, Ländern und Kommunen sind allerdings nach wie vor strittig [BR07a, 1 f.]. Aus Anlass der Novelle wurden weitere Änderungen vorgenommen, unter anderem für Transsexuelle,[2] im Bereich von Kinderpässen, bei der Datenübermittlung zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten und der Identitätspapiere von Ausländern. Außerdem werden künftig Ordens- und Künstlernamen in Pass und Personalausweis, den zugehörigen Registern und dem Melderegister nicht mehr enthalten sein. Die von der Bundesregierung geplante Streichung des Doktortitels [BRe07, 24 f., 29 f.] wurde dagegen wegen des Widerstand der Länder [BR07b] nicht umgesetzt.

Die folgenden Ausführungen konzentrieren sich auf die neuen Regelungen zur Biometrie und behandeln insbesondere die datenschutzrechtliche Perspektive. Für die Beschreibung des Ablaufs biometrischer Verfahren [z.B. JBP99; BeRo01, WOH03] und der mit ihnen verbundenen grundsätzlichen Rechtsprobleme [z.B. Al03, GuPr03; GoPr03; Ho05; Me06] muss an dieser Stelle auf die einschlägige Literatur verwiesen werden.

2 Entwicklung

Seit den Anschlägen des 11. September 2001 führt eine Vielzahl von Staaten biometrische Reisepässe ein. Treibende Kraft waren zunächst die USA, die gemäß Sec. 303 (c) Enhanced Border Security and Visa Entry Reform Act ab dem 26. Oktober 2004 ausgestellte Pässe der 25 Staaten des Visa-Waiver-Abkommens nur mit biometrische Daten akzeptieren wollten; diese Frist wurde zweimal um ein Jahr verlängert. Die International Civil Aviation Organization (ICAO, näher [Sc07]) erarbeitete technische Standards. In Deutschland wurde die bisherige Entwicklung durch einen Bericht des Büros für Technikfolgenabschätzung [TAB04], eine Machbarkeitsstudie für die Bundesregierung zum identisch geplanten digitalen Personalausweis [RRM05] und eine Reihe wissenschaftlicher Veröffentlichungen [u.a. Ho05; Me06; RoHo05] begleitet.

Parallel erließ der Rat der Europäischen Union die EG-Verordnung 2252/2004 [EU04], die als unmittelbar geltendes Recht die Erweiterung der Pässe der Mitgliedstaaten um ein Speichermedium vorschreibt, das ein Gesichtsbild und Fingerabdrücke enthält [RoHo05]. Das Europäische Parlament musste im Verfahren nach Art. 67 Abs. 1 EGV lediglich angehört werden; seine Forderung nach einem Verzicht auf die Fingerabdrucksdaten wurde nicht berücksichtigt. Gemäß der europäischen Verordnung sind die biometrischen Daten zu sichern, und das Speichermedium muss geeignet sein, Integrität, Authentizität und Vertraulichkeit der Daten sicherzustellen (Art. 1 Abs. 2 Satz 3) [vgl. RoHo05, 984 ff.]. Die Inhaber haben ein Recht zur Überprüfung, gegebenenfalls zur Berichtigung und Löschung der Daten (Art. 4 Abs. 1), deren Zweck auf die Überprüfung der Authentizität des Dokuments und der Identität des Inhabers beschränkt ist (Art. 4 Abs. 3).

[2] Sofern diese ihren Vornamen, nicht jedoch ihr Geschlecht in den Personenstandsurkunden geändert haben (§§ 1, 8 TSG), können sie nach § 4 Abs. 1 PassG n.F. einen Pass mit der Angabe des abweichenden Geschlechts erhalten; s. zur Transsexualität aus verfassungsrechtlicher Sicht [BVG87; BVG93; Bl85; Co99].

Entgegen den Bestrebungen einiger Mitgliedstaaten enthält die Verordnung keine Regelung zur Frage nationaler biometrischer Register; dies bleibt den Staaten überlassen. Diese mussten die erste Erweiterungsstufe (Gesichtsdaten) bis zum August 2006 vornehmen und haben hierfür in Bezug auf Fingerabdrucksdaten bis zum Februar 2008 Zeit.

3 Inhalt des Gesetzes

3.1 Biometrische Daten im Pass

Die § 4 Abs. 3 bis 6 PassG in der neuen Fassung (n.F.) ersetzen die bisherigen Regelungen, die durch das Terrorismusbekämpfungsgesetz eingeführt worden waren. Nach § 4 Abs. 3 PassG n.F. sind „aufgrund der Verordnung (EG) Nr. 2252/2004 […] Pässe mit einem elektronischen Speichermedium zu versehen, auf dem das Lichtbild, Fingerabdrücke, die Bezeichnung der erfassten Finger [und] die Angaben zur Qualität der Abdrücke […] gespeichert werden. Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern".

§ 4 Abs. 4 PassG n.F. bestimmt, dass vorrangig der flache Abdruck beider Zeigefinger, bei deren Fehlen, ungenügender Eignung oder Verletzung ersatzweise der des Daumens, Mittelfingers oder Ringfingers zu speichern ist. Ist die Abnahme von Fingerabdrücken „aus medizinischen Gründen, die nicht nur vorübergehender Art sind" unmöglich, wird auf die Speicherung verzichtet. Besonderheiten bestehen für Kinder. Nach § 4 Abs. 4a PassG n.F. erhalten diese bis zum vollendeten zwölften Lebensjahr einen Kinderreisepass ohne Chip. Die Ausstellung mit Chip ist möglich, bis zum vollendeten sechsten Lebensjahr jedoch ohne Fingerabdrücke.

Die regelmäßige Gültigkeit des Passes beträgt nach § 5 Abs. 1 PassG n.F. weiterhin zehn Jahre. Dies ist unter dem Gesichtspunkt der technischen Haltbarkeit problematisch; aus diesem Grund empfiehlt die ICAO eine fünfjährige Gültigkeit. Nach Berichten im Februar 2007 haben die in Großbritannien verwendeten Pass-Chips offenbar nur eine Garantie von zwei Jahren.[3] Neu ist die Gültigkeit von sechs Jahren bis zur Vollendung des 24. Lebensjahres, die auch für den Personalausweis gelten wird (§ 2 Abs. 1 PersAuswG n.F.). Bisher beträgt die Gültigkeit bei beiden Dokumenten fünf Jahre bis zur Vollendung des 26. Lebensjahres.

Die Passmuster (§ 4 Abs. 5 PassG n.F.) sowie das Verfahren, technische Anforderungen für Erfassung und Qualitätssicherung der biometrischen Daten und das Vorgehen bei Fehlen von Fingern, ungenügender Qualität und Verletzungen (§ 6a Abs. 3 PassG n.F.) werden durch Rechtsverordnungen bestimmt, die noch zu erlassen sind.

[3] S. http://www.heise.de/newsticker/meldung/84957.

3.2 Verfahren, Register und Verwendung

§ 6 Abs. 1 Satz 7 PassG n.F. bestimmt das persönliche Erscheinen des Passbewerbers zum Enrolment; im Hinderungsfall kann nach Satz 8 nur ein vorläufiger Pass beantragt werden. § 6 Abs. 2 Satz 3 PassG n.F. enthält die Ermächtigung zur Abnahme und elektronischen Erfassung der Fingerabdrücke des Passbewerbers und statuiert eine Mitwirkungspflicht. Die Übermittlung an den Passhersteller erfolgt gemäß § 6a Abs. 1 PassG n.F. durch Datenübertragung, wobei „Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen [sind], die insbesondere die Vertraulichkeit und Unversehrtheit der Daten sowie die Feststellbarkeit der übermittelnden Stelle gewährleisten"; dies wird nach § 6a Abs. 2 Satz 2 PassG n.F. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt. Hierfür soll ein Konformitätsbescheid ausgestellt werden [BRe07, 39 f.].

Für die Speicherung der biometrischen Daten außerhalb des Passes regelt § 4 Abs. 3 Satz 3 PassG n.F. (identisch mit § 4 Abs. 4 Satz 2 PassG a.F.) das Verbot einer bundesweiten Datei. Für die Fingerabdrücke gilt darüber hinaus – datenschutzrechtlich überaus wichtig (s.u. 4.4) –, dass diese nach Aushändigung des Passes bei den Passbehörden zu löschen sind (§ 16 Abs. 2 Satz 3 PassG n.F.). § 16 Abs. 3 Satz 2 PassG n.F. stellt klar, dass der Passhersteller auch die biometrischen Daten nach Herstellung des Passes zu löschen hat. Absatz 6 verpflichtet die Passbehörde „Einsicht in die im Chip gespeicherten Daten zu gewähren".

§ 16a PassG n.F. regelt die Identitätsüberprüfung mittels biometrischer Daten. Satz 1 stellt klar, dass die im Chip gespeicherten Daten ausschließlich zur Prüfung der Echtheit des Passes und der Identität des Inhabers „und nur nach Maßgabe der Sätze 2 und 3 ausgelesen und verwendet werden" dürfen. Die folgenden Sätze bestimmen, dass Polizeivollzugsbehörden, Zollverwaltung sowie Pass-, Personalausweis- und Meldebehörden die elektronischen Daten auslesen, die biometrischen Daten des Inhabers erheben und beide miteinander vergleichen dürfen, „soweit [sie] die Echtheit des Passes oder die Identität des Inhabers überprüfen dürfen". Die Norm verweist also auf entsprechende spezialgesetzliche Befugnisse, etwa §§ 23 BPolG, 6 Abs. 3 PassG, 1 MRRG und Befugnisse nach der Strafprozessordnung und dem Polizeirecht. Die erhobenen Daten sind nach der Prüfung unverzüglich zu löschen. Diese Pflicht wurde gegen den Widerstand des Bundesrats [BR07a, 3 f.] beibehalten (s.u. 4.3.).

Nach dem eindeutigen Wortlaut dürfen sonstige Behörden die Daten des Chips nicht auslesen. Im nichtöffentlichen Bereich besteht sogar ein absolutes Verwendungsverbot für die biometrischen Daten. Das folgt aus § 18 Abs. 3 PassG, wonach der Pass hier weder zum automatischen Abruf personenbezogener Daten noch zu deren automatischer Speicherung verwendet werden darf (vgl. zum gleichlautenden § 4 PersAuswG [Ho05, 204 f.]) und aus dem Erstrechtschluss aus § 18 Abs. 4 PassG n.F., wonach Beförderungsunternehmen die maschinenlesbare Zone, nicht aber die biometrischen Daten verwenden **d**ürfen.

§ 18 Abs. 4 PassG n.F. gibt diesen Beförderungsunternehmen die Befugnis, die maschinenlesbare Zone des Passes elektronisch auszulesen und zu verarbeiten, soweit sie aufgrund internationaler Abkommen oder Einreisebestimmungen zur Mitwirkung an Kontrolltätigkeiten im internationalen Reiseverkehr und zur Übermittlung personenbezogener Daten verpflichtet sind. Dies erstreckt sich ausdrücklich nicht auf die biometrischen Daten. Nach Erfüllung der Unterstützungspflicht sind die erhobenen Daten zu löschen. Verstöße gegen § 18 Abs. 4 PassG n.F. werden nach § 25 Abs. 2 Nr. 5 PassG n.F. als Ordnungswidrigkeit geahndet.

3.3 Biometrische Daten bei Ausländern

§ 1 Abs. 4 Satz 2 PassG n.F. schafft die Möglichkeit, auch nichtdeutschen Diplomaten, Konsularbeamten und sonstigen im amtlichen Auftrag tätigen Personen und ihren Familienangehörigen einen Pass auszustellen. In diesem Fall ermächtigt § 6 Abs. 2b Satz 1 PassG n.F. die Passbehörde zur Feststellung von Passversagungsgründen „oder zur Prüfung von sonstigen Sicherheitsbedenken“, um Auskunft aus dem Ausländerzentralregister zu ersuchen. Bei Ausländern von außerhalb der Europäischen Union können nach § 6 Abs. 2b Sätze 2 und 3 PassG n.F. zusätzliche Überprüfungen stattfinden: Name und sonstige Identifizierungsinformationen dürfen an den Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz, den Militärischen Abschirmdienst, das Bundeskriminalamt und das Zollkriminalamt übermittelt werden; zusätzlich können die Fingerabdrucksdaten an das Bundeskriminalamt übermittelt werden.

Das Gesetz enthält überdies Ermächtigungsgrundlagen für die Prüfung der Dokumentenechtheit und der Identität des Inhabers bei ausländischen Pässen und Passersatzpapieren (§ 16 Abs. 1a AsylVfG n.F., §§ 49 Abs. 1, 48 Abs. 1 AufenthG n.F., § 8 Abs. 2 FreizügigG n.F.), sonstigen Identitätspapieren (§ 16 Abs. 1a AsylVfG n.F.) sowie Aufenthaltstiteln und Bescheinigungen über die Aussetzung der Abschiebung (§§ 49 Abs. 1, 48 Abs. 1 AufenthG n.F.). Die biometrischen Daten dürfen ausgelesen, die Daten des Inhabers erhoben und beide miteinander verglichen werden. In allen Fällen wird dies auf Fingerabdrücke, Lichtbild und Irisbild beschränkt.

Bei der Auswertung der nach § 49 AufenthG n.F. erhobenen Daten leistet gemäß § 89 Abs. 1 AufenthG n.F. das Bundeskriminalamt Amtshilfe; anders als bei deutschen Pässen ist hier ein Abgleich mit erkennungsdienstlichen Datenbanken zulässig. Die Daten sind nach der Überprüfung bei allen Behörden zu löschen (§§ 16 Abs. 6 AsylVfG n.F., 89 Abs. 3 Satz 1 AufenthG n.F., 8 Abs. 2 Satz 4 FreizügigG n.F.). Dies wurde hinsichtlich § 8 Abs. 2 Satz 4 FreizügigG n.F. gegen den Widerstand des Bundesrats [BR07a, 9] beibehalten.

3.4 Registerabruf

Das Gesetz enthält ferner Ermächtigungen zur Datenübertragung und zum automatisierten Abruf von Lichtbildern aus den Pass- und Personalausweisregistern für Polizei- und Ordnungsbehörden zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten (§§ 22a PassG n.F., 2c PersAuswG n.F.).

Die Voraussetzungen der §§ 22 Abs. 2 PassG, 2b PersAuswG bleiben unverändert. Der Abruf ist nur zulässig, wenn die Passbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde. Außerdem dürfen nur die örtlichen Polizeivollzugsbehörden Daten abrufen, und die Abrufe sind zu dokumentieren.

4 Bewertung

4.1 Rechtliche Anforderungen

Die verfassungsrechtlichen Anforderungen an biometrische Identifikationskarten können hier nur im Überblick angegeben werden [näher z.B. Al03; GoPr03; GuPr03; Ho05; Me06; RoHo05; TAB04; RRM05]; einige der folgenden Anforderungen sind im Einzelnen umstritten. Um das verfassungsrechtliche Kriterium der Eignung zu erfüllen, für die Betroffenen objektiv zumutbar und praktisch handhabbar zu sein, müssen die eingesetzten Verfahren hinreichend niedrige Fehlerraten (Falschakzeptanz und Falschrückweisung) aufweisen. Unter Erforderlichkeitsgesichtpunkten sind Merkmale vorzuziehen, die keine überschießenden Informationen (vor allem über die Gesundheit) enthalten, keine dauerhaften Spuren in der Umwelt hinterlassen und nicht unmerklich erhoben werden können. Die Verwendung von Templates (extrahierte Datensätze) ist grundsätzlich vorzugswürdig, weil diese weniger Informationen über den Inhaber enthalten.

Zur Datensicherung sind geeignete Verschlüsselungs-, Signatur- und Authentifizierungsmechanismen einzusetzen. Ferner ist die missbräuchliche Speicherung der Daten bei Herstellung und Kontrolle technisch auszuschließen. Für Bürger, die temporär oder dauerhaft (z.B. durch Erkrankungen oder Behinderungen) nicht zur biometrischen Authentifikation geeignet sind, sind effektive und diskriminierungsfreie Rückfallsysteme vorzuhalten. Schließlich ist die Speicherung biometrischer Daten in (zentralen wie dezentralen) Registern für die Passkontrolle und – jedenfalls in Deutschland – für die Vermeidung von Mehrfachregistrierungen nicht erforderlich, für die Zwecke der allgemeinen Strafverfolgungsvorsorge hingegen objektiv unzumutbar (unverhältnismäßig im engeren Sinne) und hat deshalb zu unterbleiben.

4.2 Ausgestaltung und Herstellung des Passes

Die Normen zur Ausgestaltung des Passes beschränken sich weitgehend auf den Verweis auf die Verordnung (EG) Nr. 2252/2004. Diese Gesetzestechnik ist korrekt, weil wegen der unmittelbaren Geltung der Verordnung (Art. 249 EGV) die Einführung tatsächlich auf deren Basis und nicht aufgrund der Novelle erfolgt [Bre07, 23; RoHo05, 987 f.].

Das Hauptproblem besteht in der technischen Realisierung der gesetzlichen Vorgaben, insbesondere der Sicherung „gegen unbefugtes Auslesen, Verändern und Löschen“ (§ 4 Abs. 3 Satz 3 PassG n.F., Art. 1 Abs. 2 Satz 3 der Verordnung). Gegenwärtig werden die biometrischen Gesichtsdaten durch eine Authentifizierung geschützt, die den Zugriff auf die Daten nur erlaubt, wenn das Lesegerät über einen spezifischen Schlüssel verfügt, den es aus den – zuvor automatisiert optisch gelesenen – Passdaten berechnet.

Mit diesem „Basic Access Control“ [KN07, 178] werden die Nachteile der kontaktlosen Schnittstelle ausgeglichen, über die die Daten sonst unmerklich auslesbar wären. Bei Verlust oder Diebstahl ist ein Zugriff jedoch möglich. Dies stellt ein „unbefugtes Auslesen“ nach § 4 Abs. 3 Satz 3 PassG n.F. dar und muss folglich verhindert werden. Entsprechend ist für die Speicherung von Fingerabdrücken eine stärkere kryptographische Absicherung („Extended Access Control“) vorgesehen, bei der nur autorisierte Lesegeräte nach gegenseitiger Authentifizierung mit dem Chip auf die Daten zugreifen können [KN07, 178 ff].[4]

Die Regelungen zur Datenerhebung der Fingerabdrücke (§§ 4 Abs. 4, 6 Abs. 2 PassG n.F.) geben detailliert Auskunft über die Art der Daten und den Erhebungsvorgang. Begrüßenswert ist auch die Speicherung einer Qualitätsangabe der Fingerabdrücke nach § 4 Abs. 3 Satz 1 PassG n.F., die eine diskriminierungsfreie Behandlung von Personen ermöglicht, deren Fingerabdrücke zwar grundsätzlich, aber schlechter zur Authentifikation geeignet sind. Diese Passinhaber haben eine höhere individuelle Falschrückweisungsrate [näher Ho05, 202 f.]. Durch die Angabe und geeignete Verwaltungsvorschriften für Kontrollbeamte kann vermieden werden, dass hieraus Nachteile entstehen.

Im Rahmen des Herstellungsprozesses sind die Vorgaben über die Datensicherung bei der Übertragung (§ 6a Abs. 1 PassG n.F.) und deren Sicherstellung durch das BSI hervorzuheben. Dagegen muss bezweifelt werden, ob die Speicherung der Fingerabdrucksdaten bei den Passbehörden bis zur Aushändigung des Passes (§ 16 Abs. 2 Satz 2 PassG n.F.) unter dem Gesichtspunkt der Vermeidung einer neuen Datenerhebung bei Produktionsfehlern gerechtfertigt werden kann. In diesem Fall ist vielmehr eine Neuerhebung gerade sinnvoll, weil der Fehler auch im Rahmen des Erhebungsprozesses entstanden sein kann. Die Daten sollten deshalb nach der Übermittlung an den Passhersteller (und dessen Bestätigung des Dateneingangs) gelöscht werden.

Absolut notwendig ist jedenfalls, im Interesse des Inhabers die Funktionsfähigkeit des Chips und der gespeicherten Daten bei der Ausgabe festzustellen. Ansonsten besteht das Risiko, erstmals im Rahmen einer Grenz- oder Polizeikontrolle einen Fehler festzustellen, unter Verdacht zu geraten und weitere Nachteile zu erleiden. Es ist deshalb überaus problematisch, dass bislang bei der Ausgabe keine Funktionskontrolle der gespeicherten Gesichtsdaten erfolgt.

4.3 Verwendung

Hervorzuheben ist die Zweckbestimmung in § 16a Satz 1 PassG n.F. (Prüfung der Echtheit des Dokuments und der Identität des Inhabers). Die Zwecke entsprechen der EG-Verordnung 2252/2004, die jedoch nur eine Zweckbestimmung „für die Zwecke dieser Verordnung“ enthält und somit andere rechtliche Zweckregelungen zulässt. Das deutsche Gesetz ist dagegen abschließend. So ist insbesondere ein Abgleich mit erkennungsdienstlichen Datenbanken ausgeschlossen. In ihrer Eindeutigkeit positiv ist auch die absolute Löschungspflicht nach Abschluss der Prüfung in § 16a Satz 3 PassG n.F.

[4] Zu verbleibenden Risiken (Abhandenkommen von Geräten etc.) s. [Ho05, 348 f.].

Aus verfassungsrechtlicher Sicht ist zu begrüßen, dass diese Regelungen entgegen den Änderungsvorschlägen des Bundesrates beibehalten wurden. Letztere sahen vor, den automatisierten Abgleich der Daten mit erkennungsdienstlichen Dateien der Polizeivollzugsbehörden standardmäßig – also bei jeder Identitätsprüfung – zuzulassen, und die Daten nicht zu löschen, soweit und solange sie „im Rahmen eines Strafverfahrens oder zur Abwehr einer Gefahr für die öffentliche Sicherheit oder Ordnung benötigt werden" [BR07a, 3 f.]. Beide Vorschläge wären zu Generalklauseln für die erkennungsdienstliche Behandlung geworden; so wäre etwa die Beschränkung dieser Maßnahme auf Beschuldigte eines Ermittlungsverfahrens in § 81b StPO hinfällig gewesen.

Das Argument des Bundesrates für den regelmäßigen Abgleich – bei Täuschung oder Bestechung von Mitarbeitern der Passbehörde könne die Identitätstäuschung mittels eines Passes, der die Daten einer anderen Person enthalte, nicht entdeckt werden – ist aus zwei Gründen nicht überzeugend: Zum einen wäre dieses Problem nur für die relativ kleine Gruppe der im AFIS erfassten Personen behoben worden, zum anderen handelt es sich hierbei um einen seltenen Sonderfall, der die standardmäßige Übermittlung an das AFIS bei normalen Grenz- und Polizeikontrollen nicht rechtfertigt. Schlussendlich begegnet es massiven verfassungsrechtlichen Bedenken, wenn die Verwendung sensibler biometrischer Daten auf rechtsstaatlich ohnehin problematische Begriffe wie die „Gefährdung der öffentlichen Ordnung" gestützt werden soll.

Hinsichtlich der Befugnis von Beförderungsgesellschaften zur elektronischen Erfassung der maschinenlesbaren Zone (§ 18 Abs. 4 n.F.) enthält die Novelle entgegen ihrer Begründung [BRe07, 44] keine Klarstellung; vielmehr verstößt die bereits anzutreffende Praxis derzeit eindeutig gegen § 18 Abs. 3 PassG [Wo03, Rn. 32; SüKo06, § 18 PassG Rn. 8 ff.]. Die neue Regelung dürfte an sich aufgrund der heute kaum noch erhöhten Gefahren der Verwendung der maschinenlesbaren Zone (vor allem der Passnummer),[5] der Pflicht zur sofortigen Löschung und des ausdrücklichen Verbots der Verwendung der biometrischen Daten akzeptabel sein. Problematisch ist allerdings, dass hierbei die Zugangsdaten für das Basic Access Control (s.o.) durch Private verwendet werden.

4.4 Keine Register für Fingerabdrücke

Bei der Registerspeicherung besteht in Zukunft ein Unterschied zwischen den biometrischen Daten von Gesicht und Fingern. Während erstere bei den Passbehörden gespeichert werden, ergibt sich für letztere aus dem Zusammenspiel der Löschungspflichten des Passherstellers nach Herstellung (§ 16 Abs. 3 Satz 2 PassG n.F.) und der Behörde nach Aushändigung (§ 16 Abs. 2 Satz 3 PassG n.F.), des Verbots der Speicherung bei anderen Stellen (§ 16 Abs. 2 Satz 1 PassG n.F.) und der Pflicht zur sofortigen Löschung nach Kontrollen (§ 16a Satz 3 PassG n.F.), dass sie nach der Übergabe an den Inhaber ausschließlich im Pass selbst gespeichert sind; einzige Ausnahme ist die kurzzeitige Verarbeitung bei Kontrollen. Versuche der CDU/CSU, dies in der Endphase des Gesetzgebungsverfahrens noch zu verändern, scheiterten am Widerstand der SPD.

[5] Derartige Personenkennzeichen verursachen unter den Bedingungen moderner Datenverarbeitung nur noch eingeschränkt echte zusätzliche Risiken, s. [Ho05, 160 ff.] m.w.N.

Die Bedeutung dieser gesetzgeberischen Entscheidung ist kaum groß genug einzuschätzen. Vor dem Hintergrund der Risiken zentraler biometrischer Datenbanken [Al03, 159 ff., 162 f.; GoPr03, 69 ff.; Ho05, 191 ff.; Ho04, 352 f.; WOH03, 40] – und seit Vernetzung der Meldebehörden besteht zumindest technisch kaum ein Unterschied zur dezentralen Speicherung – bestand eine wichtige Forderung der Datenschutzbeauftragten [KD02; LDB02, 21; GoPr03, 69 ff.] und des Gutachtens für die Bundesregierung zum digitale Personalausweis [RRM05, 136 ff.] im Verzicht auf jede Speicherung außerhalb der Identitätspapiere. Gerade nach den Erfahrungen mit den durch das Unternehmen Toll Collect erhobenen Maut-Daten[6] wäre damit zu rechnen gewesen, dass ansonsten mittelfristig zu Zwecken der Strafverfolgung und Gefahrenabwehr ein Datenbanksystem verwendet worden wäre, das von jedem Bürger Zeit seines Lebens ein unveränderbares und zur allgemeinen Überwachung geeignetes Kennzeichen vorgehalten hätte.

Das Verbot der Einrichtung einer zentralen Datei in § 4 Abs. 3 Satz 3 PassG n.F. gilt folglich nur für biometrische Gesichtsdaten. Hier ist ein zentraler Abgleich aufgrund der (noch) relativ hohen Fehlerraten derzeit ohnehin unrealistisch. Sollte sich dies in Zukunft ändern, ist deutlich zu betonen, dass das Verbot so zu interpretieren ist, dass funktionale Äquivalente wie ein dezentral-vernetztes System ebenfalls erfasst sind [Ho05, 52; RRM05, 137 f.].

4.5 Biometrische Daten bei Ausländern

Bei den Regelungen für Ausländer fehlt zwar eine ähnlich strikte Zweckbindung wie in § 16a Satz 1 PassG n.F., wegen der für alle Behörden geltenden Löschungspflicht nach der Passprüfung ist aber auch hier eine Verwendung für andere Zwecke ausgeschlossen. Die Vorschläge des Bundesrates, die dies abändern wollten [BR07a, 9], entsprachen denen zum Passgesetz und wurden aus den unter 4.3 genannten Gründen zu Recht nicht umgesetzt.

Mit dem neuen Gesetz wird eine problematische Tendenz zumindest nicht fortgesetzt, in ausländerrechtlichen Regelungen zu biometrischen Identitätspapieren andere rechtsstaatliche Maßstäbe als für Inländer anzulegen.[7] Einzige Ausnahme ist die Übermittlung an das Bundeskriminalamt zum Zwecke der Datenauswertung in § 89 Abs. 1 AufenthG n.F. Die biometrischen Daten dürfen dort jedoch nicht gespeichert werden. Die Neufassung des § 89 Abs. 2 AufenthG n.F., der die Nutzung der nach § 49 AufenthG erhobenen Daten zur Identitätsfeststellung, Strafverfolgung und Gefahrenabwehr ermöglicht, nimmt die biometrischen Daten des Passes und die zum Abgleich erhobenen Daten nach § 49 Abs. 1 AufenthG n.F. nunmehr ausdrücklich aus.

---

[6] Die derzeitige absolute Zweckregelung in § 4 Abs. 2 ABMG soll nach zwei von LKW-Fahrern begangenen Kapitalverbrechen geändert werden; s. z.B. [Gö04; Pf05; Ot05].

[7] Das betrifft z.B. die Verordnungsermächtigung (statt einer gesetzlichen Regelung) für die Ausgestaltungen von Aufenthaltstitel, Ausweisersatz und Bescheinigung für die Aufenthaltgestattung, s. [GoPr03, 47 f.]; a.A. [Me06, 181 ff.].

4.6 Registerabruf

Der automatisierte Abruf von Registerbildern zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten nach den §§ 22a PassG, 2c PersAuswG n.F. ist vor allem verkehrspolitisch zu begrüßen, hat jedoch eine datenschutzrechtlich problematische Folge. Auch bisher war die Übermittlung gemäß §§ 22 Abs. 2 PassG, 2b Abs. 2 PersAuswG zulässig. Erforderlich war – und ist – die gesetzliche Ermächtigung der ersuchenden Behörde, ferner, dass diese ohne die Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und dass „die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können […]". Der neue automatisierte Abruf der Daten des Halters wird aber für den jeweiligen Bediensteten so schnell und einfach sein, dass jede andere Form der Datenerhebung „mit unverhältnismäßig hohem Aufwand" verbunden sein dürfte.[8] Es wäre deshalb zu erwarten gewesen, dass dieser Abruf bei Identitätszweifeln standardmäßig erfolgt wäre.

Um dies zumindest einzuschränken, erfolgte die Beschränkung auf die Zeiten, in denen die Passbehörde nicht erreichbar ist, und auf die jeweiligen lokalen Polizeivollzugsbehörden. Es bleibt abzuwarten, ob dies in der Praxis tatsächlich zu einer Begrenzung der automatisierten Abfragen führen wird.

Solange im Anschluss an den Abruf ein manueller Abgleich (etwa mit Bildern von Verkehrskameras) stattfindet, sind die praktischen Folgen überschaubar. Gerade hier zeigen sich jedoch die potentiellen datenschutzrechtlichen Gefahren auch einer dezentralen Registerspeicherung biometrischer Daten.

5 Ergebnis und Ausblick

In der Gesamtschau ist die Novelle aus grundrechtlicher Sicht zu begrüßen, weil sie die Vorgaben der EG-Verordnung 2252/2004 verwirklicht, ohne weitergehende Regelungen zu treffen. Das betrifft die klare Regelungstechnik bei der Datenerhebung und -verwendung, die strikte Zweckbindung, die Vermeidung weiterer Kontrollbefugnisse, vor allem aber den Verzicht auf jede dauerhafte Speicherung der Fingerabdrucksdaten außerhalb des Passes. Die Änderungsvorschläge des Bundesrates, die vor allem die Zweckbindung der hochsensiblen biometrischen Daten durch generalklauselartige Ermächtigungsgrundlagen aufgeweicht hätten (s.o. 4.3, 4.5), wurden zu Recht nicht umgesetzt.

Zu betonen ist, dass sich die tatsächliche Grundrechtsrelevanz der neuen Pässe erst in der konkreten technischen Gestaltung der verwendeten Systeme und im praktischen Einsatz erweisen wird. Angesichts der nie auszuschließenden Möglichkeit von Falschrückweisungen wird es etwa entscheidend darauf ankommen, ob und welche Form von Zusatzkontrollen bei vergeblichen Matchingversuchen vorgenommen wird.

---

[8] Dies ist ein Beispiel für die faktische Änderung materiellrechtlicher Befugnisnormen allein durch das Fortschreiten der verwendeten Technik (d.h. ohne Veränderung des Wortlauts), s. dazu allgemein [Ro93, 105 ff.].

Auch der Umgang mit defekten Pässen wird erst in der Praxis festgelegt werden. Bislang verlautet von Seiten der Bundesregierung, der Inhaber werde in diesem Fall „der bisher üblichen visuellen Kontrolle unterzogen“ [BRe06, 4], und die US-Regierung hat sich ähnlich geäußert [US07]. In der Tat dürfte es kaum zu rechtfertigen sein, dem Bürger das Risiko aufzuerlegen, einen ungültigen Pass vorzulegen, dessen Funktionsfähigkeit er selbst nicht kontrollieren kann. Wenn allerdings potentielle Straftäter durch eine nicht erkennbare Zerstörung des Chips der biometrischen Kontrolle entgehen könnten, würden letztlich Begründung und Sinn des gesamten Projekts in Frage gestellt.

Alle diese Fragen werden schließlich auch für den neuen, „digitalen“ Personalausweis relevant werden, der für 2008 angekündigt ist und neben biometrischen Daten auch Authentifizierungs- und (optional) Signaturfunktionen enthalten soll [s. z.B. Ho05, 165 ff.; 313 ff.; 346 ff. et passim; RRM05; En06; We06].

Literaturverzeichnis

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

[Bl85] Blankenagel, A.: Das Recht, ein „Anderer“ zu sein, Die Öffentliche Verwaltung 1985, S. 953-963.

[BeRo01] Behrens, M.; Roth, R.: Biometrische Identifikation, Gießen 2001.

[BR07a] Bundesrat: Empfehlungen des federführenden Ausschusses für Innere Angelegenheiten und des Finanzausschusses zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften, BR-Drs. 16/1/07 v. 5.2.2007.

[BR07b] Bundesrat: Antrag der Freistaaten Thüringen und Bayern zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften, BR-Drs. 16/2/07 v. 14.2.2007.

[BRe06] Bundesregierung: Antwort auf die Anfrage der Fraktion DIE LINKE, BT-Drs. 16/161 v. 15.12.2006.

[BRe07] Bundesregierung: Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften, BR-Drs. 16/07 v. 29.1.2007.

[BVG78] Bundesverfassungsgericht, Beschluss v. 11.10.1978, 1 BvR 16/72, Amtliche Sammlung, Band 49, S. 286-304.

[BVG93] Bundesverfassungsgericht, Beschluss v. 26.1.1993, 1 BvL 38, 40, 43/92, Amtliche Sammlung, Band 88, S. 87-103.

[Co99] Correll, C.: Im falschen Körper, Neue Juristische Wochenschrift 1999, S. 3372-3377.

[En06] Engel, C.: Auf dem Weg zum elektronischen Personalausweis, Datenschutz und Datensicherheit 2006, S. 207-210.

[EU04] Europäische Union (2004): Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. EU Nr. L 385 v. 29.12.2004, S. 1-6.

[Gö04] Göres, U.: Rechtmäßigkeit des Zugriffs der Strafverfolgungsbehörden auf die Daten der Mauterfassung, Neue Juristische Wochenschrift 2004, S. 195-198.

[GoPr03] Golembiewski, C.; Probst, T.: Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, Kiel 2003 (abrufbar unter http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf).

[GuPr03] Gundermann, L.; Probst, T.: Biometrie, Kap. 9.6, In: (Roßnagel, A., Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

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

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

[Inn07] Innenausschuss des Deutschen Bundestages: Beschlussempfehlung und Bericht zu dem Gesetzentwurf der Bundesregierung, (BT-Drs. 16/4138), BT-Drs. 16/5445 v. 23.5.2007.

[JBP99] Jain, A.K.; Bolle, R.; Pankanti, S.: Biometrics. Personal Identification in Networked Society, Boston 1999.

[KD02] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließungen der 63. Konferenz v. 7./8.3.2002, Datenschutz und Datensicherheit 2002, S. 246-249.

[KN07] Kügler, D.; Naumann, I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen, Datenschutz und Datensicherheit 2007, S. 176-180.

[LDB02] Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg: 11. Tätigkeitsbericht, Kleinmachnow 2002.

[Me06] Meuth, L.: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, Berlin 2006.

[Ot05] Otten, G.: Zweckbindung im Autobahnmautgesetz, Datenschutz und Datensicherheit 2005, S. 657-660.

[Pf05]; Pfab, A.: Rechtsprobleme bei Datenschutz und Strafverfolgung im Autobahnmautgesetz, Neue Zeitschrift für Verkehrsrecht 2005, S. 506-510.

[Ro93] Roßnagel, A.: Rechtswissenschaftliche Technikfolgenforschung, Umrisse einer Forschungsdisziplin, Baden-Baden 1993.

[RoHo05] Roßnagel, A.; Hornung, G.: Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck, Die Öffentliche Verwaltung 2005, S. 983-990.

[RRM05] Reichl, H.; Roßnagel, A.; Müller, G. (Hrsg.): Digitaler Personalausweis. Eine Machbarkeitsstudie, Wiesbaden 2005.

[Sc07] Schäffer, H.: Der Schutz des zivilen Luftverkehrs vor Terrorismus. Der Beitrag der International Civil Aviation Organisation (ICAO), Baden-Baden 2007.

[SüKo06] Süßmuth, W.; Koch, H.W.: Pass- und Personalausweisrecht, 4. Auflage, 2. Lieferung, Stand Mai 2006, Stuttgart 1998.

[TAB04] Büro für Technikfolgenabschätzung beim Deutschen Bundestag: Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht, BT-Drs. 15/4000, 2004.

[US07] U.S. Department of State: The U.S. Electronic Passport Frequently Asked Questions, abrufbar unter http://travel.state.gov/passport/eppt/eppt_2788.html.

[We06] Weichert, T.: Identitätskarten – sind Sicherheit *und* Datenschutz möglich? In: (Roßnagel, A., Hrsg.): Allgegenwärtige Identifizierung?, Baden-Baden 2006, S. 37-42.

[Wo03] Wollweber, H.: Datenschutz im Melde-, Ausweis- und Passwesen, Kap. 8.5, In: (Roßnagel, A., Hrsg.), Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

[WOH03] Woodward, J. D., Jr.; Orlans, N. M.; Higgins, P. T.: Biometrics. Identity Assurance in the Information Age, New York 2003.