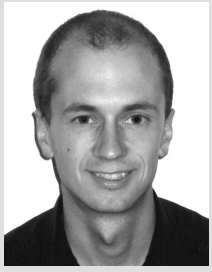
DuD
Datenschutz und Datensicherheit

Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht

Der Gesetzesentwurf der Bundesregierung zur Änderung des Passgesetzes und weiterer Vorschriften

Gerrit Hornung

Die Bundesregierung hat die erste Stufe der Veränderungen 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 existiert seit Anfang 2007 ein Gesetzesentwurf, der die Vorgaben der EG-Verordnung 2252/2004 übernimmt, notwendige Folgeregelungen umsetzt und weitere Veränderungen des Passgesetzes enthält. Der Beitrag skizziert die bisherige Entwicklung, erläutert den Inhalt des Entwurfs und der Stellungnahme des Bundesrates und nimmt eine rechtliche Bewertung vor.



Dr. Gerrit Hornung, LL.M.

Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Mitarbeiter an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

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 hat sich dadurch für die Bürger lediglich die Gebühr[1] und die Art des beizubringenden Gesichtsbildes (standardisierte Frontalaufnahme) verändert. Die zusätzliche Speicherung von Fingerabdrucksdaten bedingt hingegen veränderte Prozesse der Datenerhebung. Außerdem wird künftig die Passkontrolle regelmäßig auch die biometrische Verifikation[2] des Inhabers beinhalten.

Der Gesetzesentwurf der Bundesregierung[3] bezweckt die Normierung dieser Neuerungen. Die Aufnahme von Fingerabdrucksdaten ist für November 2007 geplant und soll keine weitere Gebührenerhöhung mit sich bringen.[4] Aus Anlass der Novelle wurden weitere Änderungen vorgenommen, unter anderem für Transsexuelle,[5] im Bereich von Kinderpässen, bei der Datenübermittlung zur Verfolgung von Verkehrsordnungswidrigkeiten und der Identitätspapiere von Ausländern. Außerdem sollen nach dem Entwurf künftig Doktortitel sowie Ordens- und Künstlernamen in Pass und Personalausweis, den zugehörigen Registern und dem Melderegister nicht mehr enthalten sein.[6] Hinsichtlich der Doktortitel regt sich allerdings Widerstand der Länder.[7]

Die folgenden Ausführungen konzentrieren sich auf die datenschutzrechtlich relevanten Passagen des Gesetzentwurfes, insbesondere im Bereich der Biometrie. Für die Beschreibung des Ablaufs biometrischer Verfahren[8] und der mit ihnen verbundenen grundsätzlichen Rechtsprobleme[9] muss an dieser Stelle auf die einschlägige Literatur verwiesen werden.

[1] Diese wurde von 26,- auf 59,- Euro (von 13,- auf 37,50 Euro bei Ausstellung vor Vollendung des 26. Lebensjahres) angehoben.

[2] "Verifikation" ist die biometrische Erkennung im 1:1-Modus, das heißt der Vergleich neu erhobener Daten mit genau einem (z.B. im Pass) gespeicherten Referenzdatensatz. Im Identifikationsmodus (1:n) wird dagegen aus einer Referenzdatenbank der Datensatz ermittelt, der mit den neuen Daten (am besten) übereinstimmt.

[3] BR-Drs. 16/07 = BT-Drs. 16/4138.

[4] S. die Begründung, BR-Drs. 16/07, 26; Kosten und Verteilung zwischen Bund, Ländern und Kommunen sind nach wie vor strittig, s. ebd., 1 f.

[5] Sofern diese ihren Vornamen, nicht jedoch ihr Geschlecht in den Personenstandsurkunden geändert haben (§§ 1, 8 TSG), können sie nach § 4 Abs. 1 PassG-E einen Pass mit der Angabe des abweichenden Geschlechts erhalten; s. zur Transsexualität aus verfassungsrechtlicher Sicht BVerfGE 49, 286; 60, 123; 88, 87; *Blankenagel*, DÖV 1985, 953 ff.; *Correll*, NJW 1999, 3372 ff.

[6] Dies wird mit der Schwierigkeit der Eintragung ausländischer Doktorgrade, der fehlenden Notwendigkeit für die Identifizierung des Inhabers, dem Widerspruch zu internationalen Standards und dem Ziel des Bürokratieabbaus begründet, s. BR-Drs. 16/07, 24 f., 29 f.

[7] Vgl. BR-Drs. 16/2/07.

[8] S. z.B. *Jain/Bolle/Pankanti*, Biometrics, 1999; *Behrens/Roth*, Biometrische Identifikation, 2001; *Woodward/Orlans/Higgins*, Biometrics. Identity Assurance in the Information Age, 2003.

[9] Vgl. z.B. *Albrecht*, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, 2003; *Gundermann/Probst*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 9.6; *Golembiewski/Probst*, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen, 2003; *Hornung*, Die digitale Identität, 2005; *Meuth*, Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, 2006.

2 Entwicklung

Seit den Anschlägen des 11. September 2001 führt eine Vielzahl von Staaten biometrische Reisepässe ein.[10] Die International Civil Aviation Organization (ICAO)[11] erarbeitete – unter maßgeblichem Einfluss der USA[12] – hierfür technische Standards. Parallel erließ der Rat der Europäischen Union die EG-Verordnung 2252/2004, die als unmittelbar geltendes Recht die Erweiterung der Pässe der Mitgliedstaaten um ein Speichermedium vorschreibt, das ein Gesichtsbild und Fingerabdrücke enthält.[13] 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.[14] In Deutschland wurde die bisherige Entwicklung durch einen Bericht des Büros für Technikfolgenabschätzung,[15] eine Machbarkeitsstudie für die Bundesregierung[16] und eine Reihe wissenschaftlicher Veröffentlichungen[17] begleitet.

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).[18] 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). Entgegen den Bestrebungen einiger Mitgliedstaaten enthält die Verordnung keine Regelung zur Frage nationaler 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 Entwurfsinhalt

3.1 Biometrische Daten im Pass

Die § 4 Abs. 3 bis 6 des Entwurfs (PassG-E) ersetzen die bisherigen Regelungen, die durch das Terrorismusbekämpfungsgesetz eingeführt worden waren. Nach § 4 Abs. 3 PassG-E 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-E 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.[19]

Die Gültigkeit des Passes beträgt – unter technischen Gesichtspunkten problematisch[20] – nach § 5 Abs. 1 PassG-E weiterhin zehn Jahre; neu ist die Gültigkeit von sechs Jahren bis zur Vollendung des 24. Lebensjahres.[21] Die Passmuster (§ 4 Abs. 5 PassG-E) 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-E) werden durch Rechtsverordnungen bestimmt.

3.2 Verfahren, Register und Verwendung

§ 6 Abs. 1 Satz 7 PassG-E bestimmt das persönliche Erscheinen des Passbewerbers; im Hinderungsfall kann nach Satz 8 nur ein vorläufiger Pass beantragt werden. § 6 Abs. 2 Satz 3 PassG-E 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-E 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-E durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt.[22]

Für die Speicherung der biometrischen Daten außerhalb des Passes regelt § 4 Abs. 3 Satz 3 PassG-E (identisch mit § 4 Abs. 4 Satz 2 PassG) das Verbot einer bundesweiten Datei. Für die Fingerabdrücke gilt darüber hinaus – überaus wichtig[23] –, dass diese nach Aushändigung des Passes bei den Passbehörden zu löschen sind (§ 16 Abs. 2 Satz 3 PassG-E). § 16 Abs. 3 Satz 2 PassG-E 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-E 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

[10] In § 4 Abs. 3 PassG wurde die Aufnahme biometrischer Merkmale vorgesehen, die Ausgestaltung jedoch – inhaltlich widersprüchlich und rechtstechnisch unklar – einem weiteren Gesetz vorbehalten; s. *Hornung*, (Fn. 9), 173 ff.

[11] Zur Rolle der ICAO s. *Schäffer*, Der Schutz des zivilen Luftverkehrs vor Terrorismus, 2007.

[12] Gemäß Sec. 303 (c) Enhanced Border Security and Visa Entry Reform Act wollten diese ab dem 26.10.2004 ausgestellte Pässe der 25 Staaten des Visa-Waiver-Abkommens nur mit biometrische Daten akzeptieren; diese Frist wurde zweimal um ein Jahr verlängert.

[13] Verordnung (EG) Nr. 2252/2004 v. 13. Dezember 2004, ABl.EU Nr. L 385 v. 29.12.2004; vgl. *Roßnagel/Hornung*, DÖV 2005, 983 ff.

[14] Zu den daraus resultierenden Problemen der (fehlenden) demokratischen Legitimität s. *Roßnagel/Hornung*, DÖV 2005, 983, 989 f.

[15] Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht, BT-Drs. 15/4000, 2004.

[16] *Reichl/Roßnagel/Müller* (Hrsg.), Digitaler Personalausweis, 2005 (die rechtlichen und technischen Probleme der Biometrie stellen sich bei Pass und Personalausweis weitgehend identisch).

[17] S. u.a. *Hornung* (Fn. 9); *Meuth* (Fn. 9); *Roßnagel/Hornung*, DuD 2005, 69 ff.

[18] Vgl. zum Folgenden ausführlich *Roßnagel/Hornung*, DÖV 2005, 983, 984 ff.

[19] Nach § 4 Abs. 4a PassG-E 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.

[20] Die ICAO empfiehlt eine fünfjährige Gültigkeit; nach Berichten im Februar 2007 haben die in Großbritannien verwendeten Pass-Chips offenbar nur eine Garantie von zwei Jahren, s. http://www.heise.de/newsticker/meldung/84957.

[21] Ebenso beim Personalausweis (§ 2 Abs. 1 PersAuswG-E); bisher beträgt die Gültigkeit fünf Jahre bis zur Vollendung des 26. Lebensjahres.

[22] Hierfür soll ein Konformitätsbescheid ausgestellt werden, s. BR-Drs. 16/07, 39 f.

[23] S.u. 4.4.

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.[24] Die erhobenen Daten sind nach der Prüfung unverzüglich zu löschen.[25]

Nach dem eindeutigen Wortlaut dürfen sonstige Behörden die Daten des Chips nicht auslesen. Im nichtöffentlichen Bereich besteht ein absolutes Verwendungsverbot für die biometrischen Daten.[26]

§ 18 Abs. 4 PassG-E gibt Beförderungsunternehmen die Befugnis, die maschinenlesbare Zone des Passes elektronisch auszulesen, soweit eine Verpflichtung zur Unterstützung öffentlicher Stellen bei der Kontrolle des Reiseverkehrs besteht; dies erstreckt sich ausdrücklich nicht auf die biometrischen Daten. Nach Erfüllung der Unterstützungspflicht sind die erhobenen Daten zu löschen.

3.3 Biometrische Daten bei Ausländern

§ 1 Abs. 4 Satz 2 PassG-E 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-E die Passbehörde zur Feststellung von Passversagungsgründen „oder zur Prüfung von sonstigen Sicherheitsbedenken“, um Auskunft aus dem Ausländerzentralregister zu ersuchen. Bei Ausländern von außerhalb der EU können nach § 6 Abs. 2b Sätze 2 und 3 PassG-E zusätzliche Überprüfungen stattfinden.[27]

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

Bei der Auswertung der nach § 49 AufenthG-E erhobenen Daten leistet gemäß § 89 Abs. 1 AufenthG-E 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-E, 89 Abs. 3 Satz 1 AufenthG-E, 8 Abs. 2 Satz 4 FreizügigG-E). Das wird hinsichtlich § 8 Abs. 2 Satz 4 FreizügigG-E vom Bundesrat abgelehnt.[28]

3.4 Registerabruf

Der Entwurf enthält ferner Ermächtigungen zur Datenübertragung und zum automatisierten Abruf von Lichtbildern aus den Pass- und Personalausweisregistern für Polizei- und Ordnungsbehörden zur Verfolgung von Verkehrsordnungswidrigkeiten (§§ 22a PassG-E, 2c PersAuswG-E).[29] Die Voraussetzungen der §§ 22 Abs. 2 PassG, 2b PersAuswG bleiben unverändert; die Abrufe sind zu dokumentieren.

4 Bewertung

4.1 Rechtliche Anforderungen

Die verfassungsrechtlichen Anforderungen an biometrische Identifikationskarten können hier nur im Überblick[30] angegeben werden. 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 der 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 vorliegenden Novelle erfolgt.[31]

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-E, Art. 1 Abs. 2 Satz 3 der Verordnung). Gegenwärtig werden die biometrischen Gesichtsdaten

[24] Die Begründung nennt beispielhaft §§ 23 BPolG, 6 Abs. 3 PassG, 1 MRRG; hinzu treten Befugnisse nach StPO und Polizeirecht.

[25] Diese Regelung wird vom Bundesrat abgelehnt, s. BR-Drs. 16/1/07, 3 f. und unten 4.3.

[26] 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 *Hornung* (Fn. 9), 204 f.), und aus dem Erstrechtschluss aus § 18 Abs. 4 PassG-E, wonach Beförderungsunternehmen die maschinenlesbare Zone, nicht aber die biometrischen Daten verwenden dürfen.

[27] 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.

[28] S. BR-Drs. 16/1/07, 9.

[29] Der Bundesrates schlägt den Abruf bei allen Straftaten vor, s. BR-Drs. 16/1/07, 5 f.

[30] Vgl. näher die Nachweise in Fn. 9, 13 und 15 bis 17; einige der folgenden Anforderungen sind im Einzelnen umstritten.

[31] Vgl. die Begründung, BR-Drs. 16/07, 23; *Roßnagel/Hornung*, DÖV 2005, 983, 987 f.

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 („Basic Access Control").[32] Hiermit 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-E dar und muss folglich verhindert werden. Entsprechend ist für die Speicherung von Fingerabdrücken eine stärkere kryptographische Absicherung („Extended Access Control")[33] vorgesehen, bei der nur autorisierte Lesegeräte nach gegenseitiger Authentifizierung mit dem Chip auf die Daten zugreifen können.[34]

Die Regelungen zur Datenerhebung der Fingerabdrücke (§§ 4 Abs. 4, 6 Abs. 2 PassG-E) 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-E, die eine diskriminierungsfreie Behandlung von Personen ermöglicht, deren Fingerabdrücke zwar grundsätzlich, aber schlechter zur Authentifikation geeignet sind. Diese Passinhaber haben eine höhere individuelle Falschrückweisungsrate.[35] 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-E) 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-E) 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

Die Zweckbestimmung in § 16a Satz 1 PassG-E ist zu begrüßen, weil sie die Zwecke aus der EG-Verordnung 2252/2004 übernimmt, aber abschließend ist.[36] 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-E.

Diese Regelungen sollten entgegen den Änderungsvorschlägen des Bundesrates beibehalten werden. Letztere sehen 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".[37] Beide Vorschläge würden zu Generalklauseln für die erkennungsdienstliche Behandlung werden; so wäre etwa die Beschränkung dieser Maßnahme auf Beschuldigte eines Ermittlungsverfahrens in § 81b StPO hinfällig.

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 wird dieses Problem nur für die relativ kleine Gruppe der im AFIS erfassten Personen behoben, zum anderen handelt es sich hierbei um einen 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 wird.

Hinsichtlich der Befugnis von Beförderungsgesellschaften zur elektronischen Erfassung der maschinenlesbaren Zone (§ 18 Abs. 4 PassG-E) enthält der Entwurf entgegen seiner Begründung[38] keine Klarstellung; vielmehr verstößt die bereits anzutreffende Praxis eindeutig gegen § 18 Abs. 3 PassG.[39] Die neue Regelung dürfte an sich aufgrund der heute kaum noch erhöhten Gefahren der Verwendung der maschinenlesbaren Zone (vor allem der Passnummer),[40] 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 nach dem Entwurf 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-E) und der Behörde nach Aushändigung (§ 16 Abs. 2 Satz 3 PassG-E), des Verbots der Speicherung bei anderen Stellen (§ 16 Abs. 2 Satz 1 PassG-E) und der Pflicht zur sofortigen Löschung nach Kontrollen (§ 16a Satz 3 PassG-E), dass sie nach der Übergabe an den Inhaber ausschließlich im Pass selbst gespeichert sind; einzige Ausnahme ist die kurzzeitige Verarbeitung bei Kontrollen.

Die Bedeutung dieser Entscheidung ist kaum groß genug einzuschätzen. Vor dem Hintergrund der Risiken zentraler biometri-

[32] http://www.bsi.de/literat/faltbl/F25GRT. htm; s. die Kritik von *Pfitzmann* an dem System, vgl. *Schulzki-Haddouti*, c't 10/2005, 94 f.

[33] Vgl. http://www.bsi.de/fachthem/epass/EACTR03110_v101.pdf.

[34] Zu verbleibenden Risiken (Abhandenkommen von Geräten etc.) s. *Hornung*, (Fn. 9), 348 f.

[35] S. näher *Hornung*, (Fn. 9), 202 f.

[36] Art. 4 Abs. 3 beschränkt die Verwendung der biometrischen Daten „für die Zwecke dieser Verordnung" auf die Prüfung der Echtheit des Dokuments und der Identität des Inhabers, lässt also andere rechtliche Zweckregelungen zu.

[37] BR-Drs. 16/1/07, 3 f.

[38] BR-Drs. 16/07, 44.

[39] S. *Wollweber*, in: Roßnagel (Fn. 9), Kap. 8.5, Rn. 32; gleiches gilt für den Personalausweis, s. *Medert/Süßmuth*, Personalausweisrecht, 3. Auflage 1998, § 4 Rn. 9.

[40] Derartige Personenkennzeichen verursachen unter den Bedingungen moderner Datenverarbeitung nur noch eingeschränkt echte zusätzliche Risiken, s. *Hornung* (Fn. 9), 160 ff. m.w.N.

scher Datenbanken[41] – und seit Vernetzung der Meldebehörden besteht zumindest technisch kaum ein Unterschied zur dezentralen Speicherung – bestand eine wichtige Forderung der Datenschutzbeauftragten[42] und des Gutachtens für die Bundesregierung zum digitale Personalausweis[43] im Verzicht auf jede Speicherung außerhalb der Identitätspapiere. Gerade nach den Erfahrungen mit den durch das Unternehmen Toll Collect erhobenen Maut-Daten[44] wäre damit zu rechnen, dass ansonsten mittelfristig zu Zwecken der Strafverfolgung und Gefahrenabwehr ein Datenbanksystem verwendet würde, das von jedem Bürger Zeit seines Lebens ein unveränderbares und zur allgemeinen Überwachung geeignetes Kennzeichen vorhalten würde.

Das Verbot der Einrichtung einer zentralen Datei in § 4 Abs. 3 Satz 3 PassG-E 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 dezentralvernetztes System ebenfalls erfasst sind.[45]

4.5 Biometrische Daten bei Ausländern

Bei den Regelungen für Ausländer fehlt zwar eine ähnlich strikte Zweckbindung wie in § 16a Satz 1 PassG-E, wegen der für alle Behörden geltenden Löschungspflicht nach der Passprüfung ist aber auch hier eine Verwendung für andere Zwecke ausgeschlossen.[46] Damit wird eine problematische Tendenz zumindest nicht fortgesetzt, in ausländerrechtlichen Regelungen zu biometrischen Identitätspapieren andere rechtsstaatliche Maßstäbe anzulegen.[47]

Einzige Ausnahme ist die Übermittlung an das Bundeskriminalamt zum Zweck der Datenauswertung in § 89 Abs. 1 AufenthG-E. Die biometrischen Daten dürfen dort jedoch nicht gespeichert werden. Die Neufassung des § 89 Abs. 2 AufenthG-E, 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-E nunmehr ausdrücklich aus.

4.6 Registerabruf

Der vorgesehene automatisierte Abruf von Registerbildern zur Verfolgung von Verkehrsordnungswidrigkeiten nach den §§ 22a PassG-E, 2c PersAuswG ist verkehrspolitisch sicher zu begrüßen, hat jedoch eine datenschutzrechtlich problematische Folge. Auch bisher ist die Übermittlung gemäß §§ 22 Abs. 2 PassG, 2b Abs. 2 PersAuswG zulässig, wenn die ersuchende Behörde hierzu ermächtigt ist, sie ohne die Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und „die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können […]“. Der 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.[48] Es ist deshalb zu erwarten, dass dieser Abruf bei Identitätszweifeln standardmäßig erfolgen wird.

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

5 Ergebnis und Ausblick

In der Gesamtschau ist der Gesetzesentwurf aus grundrechtlicher Sicht zu begrüßen, weil er 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 aufweichen,[49] sollten nicht umgesetzt werden.

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. 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“.[50] 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.[51]

[41] S. *Albrecht* (Fn. 9), 159 ff., 162 f.; *Golembiewski/Probst*, (Fn. 9), 69 ff.; *Hornung* (Fn. 9), 191 ff.; *ders*., KJ 2004, 344, 352 f.; *Woodward/Orlans/Higgins* (Fn. 8), 40.

[42] Vgl. *Konferenz der Datenschutzbeauftragten*, DuD 2002, 247; *Landesbeauftragter für den Datenschutz Brandenburg*, 11. TB, 21; *Golembiewski/Probst*, (Fn. 9), 69 ff.

[43] S. *Roßnagel/Hornung*, in: Reichl/Rossnagel /Müller (Fn. 16), 136 ff.

[44] Die derzeitige absolute Zweckregelung in § 4 Abs. 2 ABMG soll nach zwei von LKW-Fahrern begangenen Kapitalverbrechen geändert werden; s. z.B. *Göres*, NJW 2004, 195 ff.; *Pfab*, NZV 2005, 506 ff.; *Otten*, DuD 2005, 657 ff.

[45] Vgl. *Hornung*, (Fn. 9), 52; *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller (Fn. 16), 137 f.

[46] Die Änderungsvorschläge des Bundesrates (BR-Drs. 16/1/07, 9) zu § 8 FreizügG entsprechen denen zum Passgesetz und sind aus den unter 4.3 genannten Gründen abzulehnen.

[47] Das betrifft insbesondere die Verordnungsermächtigung (statt einer gesetzlichen Regelung) für die Ausgestaltungen von Aufenthaltstitel, Ausweisersatz und Bescheinigung für die Aufenthaltgestattung, s. *Golembiewski/Probst*, (Fn. 9), 47 f.; a.A. *Meuth* (Fn. 9), 181 ff.

[48] 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 *Roßnagel*, Rechtswissenschaftliche Technikfolgenforschung, 1993, 105 ff.

[49] S.o. 4.3, 4.5.

[50] Antwort auf die Anfrage der Fraktion DIE LINKE, BT-Drs. 16/161, 4.

[51] S. z.B. *Hornung* (Fn. 9), 165 ff.; 313 ff.; 346 ff. et passim, *Reichl/Roßnagel/Müller* (Fn. 16); *Engel*, DuD 2006, 207 ff.; *Weichert*, in: Roßnagel (Hrsg.), Allgegenwärtige Identifizierung?, 2006, 37 ff.