

Bonner Talweg 33-35
53113 Bonn

Telefon: 0228/22 24 98
Telefax: 0228/24 38 470

dvd@datenschutzverein.de
www.datenschutzverein.de

Bonn, den 19. April 2007

Stellungnahme

anlässlich der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 23. April 2007 zu dem Gesetzentwurf der Bundesregierung für ein **Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften**, BT- Drs. 16/4138, 14/4456, u.a.

I. Zu dem Gesetzentwurf der Bundesregierung, BT- Drs. 16/4138 vom 29.1.2007:

1. Die Speicherung von Fingerabdrücken in Reisepässen ist, ohne dass der Deutsche Bundestag und die Öffentlichkeit in angemessenem Umfang beteiligt worden wären, kraft Verordnung (EG) Nr. 2252/2004 angeordnet. Ebenso wie die Vorratsspeicherung von Telekommunikationsverbindungsdaten kommt die Verpflichtung nach der Verordnung nicht plötzlich und unverhofft über die Bevölkerung, sondern sie wurde unter Mitwirkung der Bundesregierung entwickelt. Einmal mehr zeigt sich darin auch Bereich der inneren Sicherheit ein erschreckendes **Demokratiedefizit in der Europäischen Union**, welches in der Praxis nicht durch die nationalen Parlamente ausgeglichen werden kann.

2. Für die **biometrische Ausrüstung deutscher Reisepässe** ist ein praktisches Bedürfnis nicht nachgewiesen, so dass sich die informationellen Zumutungen, die mit der Erhebung und Speicherung biometrischer Daten im Passwesen verbunden sind, nicht auf triftige Gründe stützen können. Deutsche Reisepässe zählen nach dem Bekunden der Bundesregierung schon heute im weltweiten Vergleich zu den Spitzenprodukten. Demgegenüber bleibt eine Darstellung und Analyse der tatsächlichen Gefährdung durch ver- oder gefälschte deutsche Reisepässe auch in der Begründung der Bundesregierung zum Gesetzentwurf aus. Zahl und Art der ermittelten Fälle von (Ver-) Fälschungen deutscher

Pässe bleibt ebenso im Dunkeln wie die bekannten Fehlerquellen bei der Erkennung von Fälschungen durch die Vollzugsbeamten. Angesichts des hohen Qualitätsstandards deutscher Reisepässe vieles dafür spricht, dass es vor allem ausländische Dokumente und allenfalls deutsche Ausweisersatzpapiere (soweit sie weiterhin ohne hochwertige technische Ausstattung und mit nur sehr primitiven biometrischen Merkmalen auskommen) sind, die ge- oder verfälscht Verwendung finden. Eine Evaluation des ePasses, wie sie der Bundesbeauftragte für Datenschutz und Informationsfreiheit zu Recht fordert, hat bislang keine Vergleichsdatenbasis und der Erfolg des ePasses wird weitgehend spekulativ bleiben.

Der ePass ermöglicht die **Erfassung und Speicherung biometrischer Daten von EU-BürgerInnen durch ausländische Staaten**, ohne dass die Betroffenen oder die Mitgliedstaaten der Europäischen Union dagegen eine Handhabe hätten. Die Speicherung von Templates an Stelle von Echtdateien hätte demgegenüber die Nutzung von biometrischen Daten zu nicht gewünschten Zwecken wesentlich erschwert und sich als die datensparsamere Lösung erwiesen.

Auch die **Festlegung auf die RFID- Technik** löst Bedenken aus. Denn sie liefert die InhaberInnen von Reisepässen dem Risiko der unbemerkten Erfassung und Speicherung personenbezogener Daten, einschließlich biometrischer Daten, durch Dritte aus. Ungeachtet der getroffenen Sicherheitsmaßnahmen sind Lesevorgänge über die Luftschnittstelle leichter angreifbar als Lösungen, die einen direkten Kontakt mit dem in den Pass eingebrachten Chip erfordern. Die rasante technische Entwicklung und Verbreitung dieser Technik wird die Datensicherheit von ePässen in Zukunft zunehmend gefährden und im besten Falle in immer kürzeren Abständen Gegenmaßnahmen von staatlicher Seite erfordern, wenn nicht neue Sicherheitslücken auftreten sollen. Demgegenüber werden Fehler im gespeicherten Datensatz und bei seiner Übertragung in ein Lesegerät zukünftig jeder Stelle, die Zugriff auf diese Daten hat, vermeidbaren Anlass zu Zweifeln an der Identität der Betroffenen bieten.

Der Gesetzentwurf kommt auch mit der Befugnis für Beförderungsunternehmer nach § 18 Abs. 4 neu PassG ohne Not den von der Bundesrepublik nicht gewünschten Interessen ausländischer Bedarfsträger entgegen: anstatt die Vorabübermittlung von Passagierdaten mit den gegebenen Mitteln politisch einzudämmen, reagiert die Bundesregierung auf diese von einigen Drittstaaten geforderte Übermittlung mit einer speziellen Ermächtigung von inländischen Beförderungsunternehmen. Eine substantielle Erleichterung für die Unternehmen besteht dabei nur bezüglich eines kleinen Teils der in der maschinenlesbaren

Zone abgelegten Daten, da die Unternehmen von den Daten nach § 4 Abs. 2 Pass die Personalien der Flugpassagiere auch zu eigenen Zwecken – weiterhin konventionell - erheben und zur Vermeidung von ausländerrechtlichen Haftungsrisiken auch die Gültigkeit des Reisedokuments müssen. Spürbare Erleichterungen ergeben sich mithin lediglich im Umfang von etwa 22 Zeichen.

3. Bleibt die Entscheidung für einen ePass mit biometrischen Daten und RFID- Technik im Ergebnis sowohl praktisch als auch datenschutzpolitisch eine Fehlentscheidung ohne öffentlichen Rückhalt, kann dagegen ein anderer Effekt der biometrischen Aufrüstung von Identitätsdokumenten schon heute am Gesetzentwurf abgelesen werden: Wo qualitativ hochwertige Daten erfasst werden, wecken sie das **Interesse der Sicherheitsbehörden an der Zweckentfremdung gespeicherter Daten**, und dieses wird regelmäßig auch vom Gesetzgeber befriedigt. Dass rechtliche Schranken der Nutzung von Daten zu polizeilichen und nachrichtendienstlichen Zwecken sich einer fortwährenden Erosion ausgesetzt sehen, kann ohne Weiteres an der Sicherheitsgesetzgebung der letzten Jahre abgelesen werden. Nicht zu Unrecht wird diese Vorgehensweise als „Salamitaktik“ bezeichnet.

Der Gesetzentwurf zur Passgesetznovelle treibt nunmehr die **Nutzung von Lichtbildern** in den Pass- und Personalausweisregistern durch Sicherheitsbehörden voran: Obwohl das Pass- und das Personalausweisregister unbestritten keine Auskunftsdaten für außerpasrechtliche Zwecke sind (etwa § 21 Abs. 3 PassG), werden sie schon heute routinemäßig als Referenzdatenbanken für die Identifizierung namentlich bekannter deutscher Staatsangehöriger herangezogen. Dieser Praxis überwindet den datenschutzrechtlichen Grundsatz der Zweckbindung personenbezogener Daten und ist schon im Hinblick auf die Subsidiarität der Registeranfrage (§§ 22 Abs. 2 Nr. 3 PassG, 2b Abs. 2 PersonalausweisG) rechtswidrig. Der Gesetzentwurf vollzieht mit dem online- Abruf aus den Registern (§ 22a Abs. 2 S. 1 neu PassG, 2c Abs. 2 neu PersonalausweisG) den Übergang zur allgemeinen Zugriffsberechtigung für – zunächst – bestimmte ordnungsbehördliche Zwecke. Darin liegt nicht nur eine technische Vereinfachung: Der online- Zugriff ermöglicht bei vorhandener technischer Infrastruktur in weit größerem Ausmaß als heute die Nutzung der bei den Registerbehörden bereits nahezu flächendeckend vorhandenen Lichtbilder der deutschen Wohnbevölkerung. Das Pass- und Personalausweisrecht beschränkt den Abruf und die Nutzung dieser Daten ebenso wenig auf die Betroffenen im Ordnungswidrigkeitenverfahren (in Abgrenzung zu Dritten) wie die in den §§ 22 Abs. 1, 2a Abs. 1 PersonalausweisG in

Bezug genommenen Gesetze und Verordnungen. Dass für die rechtliche Erlaubnis zum online- Abruf ein zwingendes öffentliches Bedürfnis bestehen soll, kann dabei nicht überzeugen: die Überlastung der Ordnungswidrigkeitenbehörden ist kein Anlass für die Einführung einer datenschutzkritischen Infrastruktur und Alternativen – etwa die Aufhebung der Privilegierung von Verkehrsordnungswidrigkeiten durch eine Verlängerung der bislang außergewöhnlich kurze Verjährungszeit von drei Monaten – sind offenkundig nicht erwogen worden.

Die Zukunft des in dem Gesetzentwurf der Bundesregierung versprochenen Verbots einer bundesweiten biometrischen Datenbank (§ 4 Abs. 3 S. 3 neu PassG, vergl. auch Art. 4 Abs. 3 VO (EG) Nr. 2252/2004) dürfte im Hinblick auf Lichtbilder in der Sache kurz sein: die Kapazität zum online- Abruf lässt es perspektivisch genügen, durch geeignete technische Ausstattung der abrufenden Stellen und Zugriff etwa auf meldebehördliche Daten auch dezentrale **Passregister als Ermittlungsinstrumente für sicherheitsbehördliche Zwecke** zu verwenden.

Die Lebensdauer der Beschränkung des online- Abrufs auf die Verfolgung von Verkehrsordnungswidrigkeiten (§ 22a Abs.2 neu PassG) ist voraussichtlich sogar kürzer als das Gesetzgebungsverfahren: die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates (BT- Drs. 16/4456, dort Nr. 6.) bereits dem online- Abruf von Lichtbildern zur Verfolgung von Straftaten zugestimmt.

II. Zu der Stellungnahme des Bundesrates und der Antwort der Bundesregierung, BT- Drs. 16/4456 vom 28.2.2007:

Der Bundesrat führt in seiner Stellungnahme die absehbare Zukunft von Passdaten vor. Diese soll, ganz im Sinne der Erosion von Verwendungsschranken gegenüber sicherheitsbehördlichen Zwecken, bestimmt sein von dem Wegfall der heute noch in das PassG eingeschriebenen Zweckbindungen.

In der Sache laufen die Forderungen des Bundesrates zu § 16a S. 2 neu PassG (Abgleich biometrischer Daten im ePass mit vorhandenen erkennungsdienstlichen Daten) und zu den §§ 22a Abs. 2 neu PassG, 2c Abs. 2 PersonalausweisG (online- Abruf sämtlicher

Registerdaten insbesondere durch Strafverfolgungsbehörden) auf die weitgehende Nutzung von Passdaten zu polizeilichen Zwecken hinaus. Der Sinn des ePasses – Fälschungssicherheit – und des Passregisters – Vollzug des Passgesetzes – werden unter Aufgabe des verfassungsrechtlich unverfügbaren Grundsatzes der Zweckbindung und des Verbotes der Datenerhebung und –speicherung „auf Vorrat“ zu noch unbestimmten Zwecken in ihr Gegenteil verkehrt. Von den Vorschlägen des Bundesrates ist es nur ein kleiner Schritt zur Integration der Pass- und Personalausweisregister und des Systems biometrischer Ausweise in eine umfassende Infrastruktur sicherheitsbehördlicher Datenbanken.

Mit den Erfahrungen der vergangenen Jahre ist es abzusehen, dass der Deutsche Bundestag sich damit in nicht allzu ferner Zukunft ebenso wird auseinandersetzen haben, ebenso wie mit der Forderung, die heute noch einer strengen Zweckbindung unterliegenden Daten der LKW- Maut zu Hilfsmitteln der Sicherheitsbehörden werden zu lassen, wie es die Melderegister, das Kraftfahrzeugregister, die Bestandsdaten der Geldinstitute und der Telekommunikationsanbieter oder das Ausländerzentralregister schon standardmäßig heute sind.

Dieser Entwicklung gilt es, im Interesse einer freiheitlichen Gesellschaftsordnung, wie sie das Grundgesetz fordert, entgegenzutreten. Denn es wäre mit einer solchen Gesellschaftsordnung nicht vereinbar, wenn die Datenspuren alltäglicher und unvermeidlicher Lebensäußerungen dauerhaft und leichtgängig zu Instrumenten der Verdachtsgewinnung und Kontrolle würden.

Sönke Hilbrans

Rechtsanwalt und Fachanwalt für Strafrecht, Berlin

Vorsitzender der Deutschen Vereinigung für Datenschutz e.V., Bonn