Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)192 E

**Stellungnahme des BfDI zur Novellierung des Passgesetzes
für die Anhörung im Innenausschuss des Deutschen Bundestages am 23. April 2007**

Die Ratsverordnung vom 13. Dezember 2004 sieht die Integration eines RFID-Chips in die Reisepässe der Unionsbürger vor. Der Chip soll über das digitalisierte Lichtbild hinaus auch die digitalisierten Abdrücke der beiden Zeigefinger enthalten.

Mit der Verordnung 2252/2004 wurde dem Bundestag zu meinem Bedauern die Entscheidung darüber entzogen, ob Fingerabdrücke überhaupt in die Pässe deutscher Staatsangehöriger aufgenommen werden sollten. Aber auch das Europäische Parlament hatte keine Möglichkeiten, die Entscheidung effektiv zu beeinflussen, denn der Rat hat die Verordnung im Rahmen der sog. „Dritten Säule“ der Europäischen Union beschlossen. Die weitreichende Maßnahme, biometrische Merkmale in die Pässe aller EU-Bürgerinnen und Bürger aufzunehmen, ist also allein durch die Regierungen und nicht durch die Parlamente entschieden worden, obwohl dies erhebliche Konsequenzen für die Grundrechte hat.

Zwar hatte der Deutsche Bundestag 2001 vor dem Hintergrund der Anschläge des 11. September 2001 mit Zustimmung zum Passgesetz grundsätzlich seine Zustimmung dazu gegeben, ein biometrisches Merkmal in den Pass aufzunehmen, hatte sich aber vorbehalten, über die Einzelheiten, insbesondere über das zu verwendende Merkmal, selbst zu entscheiden. Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) waren in das Passgesetz (§ 4 Abs. 3 und 4 PassG) und in das Personalausweisgesetz (§ 1 Abs. 4 und 5 PersauswG) Regelungen eingefügt worden, die prinzipiell die Aufnahme biometrischer Merkmale in Ausweisdokumente vorsehen. Die anstehende parlamentarische Diskussion über die datenschutzrechtlichen Risiken, aber auch über die Kosten des „aufgerüsteten“ Reisepasses erfolgt somit verspätet, unter dem normativen Druck der Ratsverordnung und unter beträchtlichem Zeitdruck. Nationale Spielräume für eigenständige Lösungen mit weniger oder jedenfalls ausgereifteren biometrischen Elementen sind damit praktisch nicht mehr gegeben, es sei denn, die Bundesregierung entschlösse sich zu einer entsprechenden Initiative auf EU-Ebene.

Ich hätte es jedenfalls begrüßt, wenn die Aufnahme der Fingerabdrücke nicht verbindlich vorgeschrieben, sondern – fakultativ – nach ausführlicher und umfassender innerstaatlicher Diskussion in das Ermessen der Mitgliedstaaten gestellt worden wäre. Ich halte es schon für bemerkenswert, dass dem EP zunächst der erste Verordnungsentwurf, der noch die fakultative Aufnahme der Fingerabdrücke vorsah, vorgelegt wurde und dem EP erst wenige Tage vor seiner Stellungnahme der – ohne Begründung geänderte – neue Entwurf übermittelt wurde, der nunmehr die obligatorische Aufnahme digitalisierter Fingerabdrucke vorsah. Seine Stellungnahme hat das EP bezeichnenderweise zu dem „alten“ Entwurf abgegeben, der nur eine fakultative Aufnahme der Fingerabdrücke vorsah. Eine Mitentscheidungsmöglichkeit hatte das EP ja – wie bereits ausgeführt – ohnehin nicht.

Zunächst möchte ich auf die Bedenken gegen den Gesetzentwurf eingehen, die unter dem Aspekt der Datensicherheit erhoben werden:

Auf dem Pass wird derzeit das digitale Passfoto auf einem kontaktlosen Chip mit einem Zugangsschutz (Basic Access Control) gesichert gespeichert. Die Daten der maschinenlesbaren Zone (MRZ) werden als Schlüssel genutzt, um den Chip auslesen zu können. Dies bedeutet, dass die im Chip gespeicherten Daten des Passes nur gelesen werden können, wenn die Daten der MRZ bekannt sind. Ab November 2007 sollen bundesweit auch Fingerabdruckdaten des Passinhabers erfasst und in einem besonders geschütztem Bereich auf dem Chip hinterlegt werden. Dieser Bereich wird durch ein gesondertes Verschlüsselungs-/Zugangsverfahren (Extended Access Control) geschützt. Bei diesem Verfahren werden nicht nur die Daten selbst, sondern es wird auch die Kommunikation des Chips mit dem Lesegerät besonders gesichert. Dies bedeutet z.B., dass der Chip prüft, ob es sich um ein berechtigtes Lesegerät handelt. Der Zugang zu den Fingerabdruckdaten kann nur über ein speziell autorisiertes Lesegerät erfolgen. Die Berechtigung (Signatur) der Lesegeräte wird durch nationale Organisationen (in Deutschland das Bundesamt für die Sicherheit in der Informationstechnik) verwaltet. Es ist zu prüfen und festzulegen, welche Lesegeräte und weitergehend welche Staaten auf diese Daten zugreifen dürfen.

Wie die Staaten, die eine Leseberechtigung für die gespeicherten biometrischen Daten haben, mit den Daten umgehen, entzieht sich der Kontroll- und Einflussmöglichkeit deutscher Stellen. Diese Daten könnten also in Personendatenbanken einfließen.

Offen bleibt auch die Frage einer automatisierten Kontrollmöglichkeit. Bei der zweidimensionalen Gesichtserkennung werden unter nicht idealen Lichtverhältnissen hohe Fehlerraten gemessen. Dies umfasst die Nichterkennung wie auch unakzeptable Falscherkennungsraten. Die Bundesregierung hat sich mit der auch für die Passkontrolle beabsichtigten zweidimensionalen Gesichtserkennung voreilig auf ein noch nicht ausgereiftes Verfahren festgelegt.
Bei der neuerlichen Bewertung automatisierter Gesichtserkennungsverfahren hat sich herausgestellt, dass die 3D-Erkennung erheblich bessere Erkennungsraten liefert und das Gesichtserkennungsverfahren der Zukunft sein wird.

Meine Skepsis gegen die sehr kurzfristig getroffene Entscheidung für die Aufnahme der Fingerabdrücke wird durch die Erfahrungen in den USA bestätigt. Die kürzlich veröffentlichen Untersuchungen des US-Rechnungshofs (GAO-07-248, GAO-07-278) haben ergeben, dass die Aufnahme der Fingerabdrücke der zwei Zeigefinger für einen Abgleich mit der Fingerabdruck-Datenbank (AVIS) des FBI nicht den erhofften Sicherheitsgewinn erbracht hat. An den Grenzkontrollstellen der USA sollen deshalb von Ausländern künftig nicht mehr wie gehabt 2-Finger flach erfasst, sondern 10 Finger gerollt aufgenommen werden. Es drängt sich die Frage auf, inwieweit sich hieraus auch Konsequenzen für die EU-Reisepässe ergeben. Insbesondere ist zu befürchten, dass es den Reisenden aus der EU selbst bei Vorlage des E-Passes der zweiten Generation in Zukunft nicht erspart bleiben wird, sich bei der Einreise in die USA zusätzlich zu den im Pass gespeicherten Fingerabdrücken noch einmal alle zehn Fingerabdrücke abnehmen lassen zu müssen, die dann für unabsehbare Zeit von den US-Behörden gespeichert werden.

Interessanterweise ist in den Vereinigten Staaten auch weiterhin nicht vorgesehen, dass die Fingerabdrücke von US-Bürgern in die Pässe aufgenommen oder bei der Ein- oder Ausreise in die USA erhoben werden. Die Europäische Union steht also mit ihrer Entscheidung, die

Fingerabdrücke ihrer Bürgerinnen und Bürger zu erfassen, international weiterhin weitgehend allein. Nur sehr wenige Länder haben sich ebenfalls hierzu entschlossen, verwenden dabei z.T. aber andere technische Methoden, so dass die verschiedenen Systeme selbst nicht kompatibel sind. Angesichts dieser Situation werden also in Zukunft die EU-Bürgerinnen und -Bürger beim Überschreiten der EU-Außengrenzen intensiver kontrolliert als die Angehörigen der meisten anderen Staaten, soweit für sie keine Visumspflicht besteht. Anders als die USA begegnen die europäischen Staaten ihren eigenen Bürgerinnen und Bürgern also mit einem besonderen Misstrauen.

Die Verwendung biometrischer Merkmale für zeitlich beschränkte staatliche Identitätskontrollen bei der Ein- und Ausreise weckt zudem Begehrlichkeiten nach weitergehender, unbeschränkter Verwendung der Daten nicht nur durch staatliche Stellen. Dies ist bereits heute erkennbar.

Ich halte es nur für eine Frage der Zeit, dass auch die Wirtschaft Interesse an einer biometrisch abgesicherten Kundenidentifizierung entwickeln und deshalb lesenden Zugriff auf den Chip im Pass und künftig auch im Personalausweis anstreben wird, wenn die Daten einmal vorhanden sind.

Unabhängig von derartigen Zukunftsszenarien stellt sich bereits ganz aktuell die Frage nach der Sicherheit der zur Aufnahme biometrischer Daten verwendeten Technik. Es ist leider keine bloß theoretische Frage, was geschieht, wenn kein hinreichender Manipulations- und Kopierschutz gewährleistet ist und auch Kriminelle „gestohlene“ Fingerabdruckdaten zur Tatbegehung nutzen können. Damit würden wir der Horrorvision von der schnell und leicht gestohlenen Identität wieder ein deutliches Stück näher kommen, einem Phänomen, das nicht nur in den USA bereits besorgniserregende Dimensionen angenommen hat.

Auch bei der Diskussion über die Biometrie im E-Pass dürfen wir den Blick nicht verengen und weitere, flankierende, kumulierende und sich vielleicht durch Verknüpfung von Datenbeständen oder bundesweiten Online-Zugriff sogar potenzierende Beeinträchtigungen des Grundrechtes auf informationelle Selbstbestimmung nicht aus dem Blick verlieren.

Der Gesetzentwurf wird einigen der zentralen Forderungen des Datenschutzes gerecht:

- So werden in Deutschland beim Auslesen des Biometriechips im Pass keine Zusatzinformationen z.B. zu Erkrankungen oder sonstigen personenbezogenen Merkmalen ausgewertet. Allerdings hat man sich für die Speicherung der sog. Rohdaten („Image“) im RFID-Chip und nicht – wie von Datenschutzseite gefordert – für Auswertungsmuster („Template“) entschieden, so dass aus den Daten gewinnbare Zusatzinformationen ggf. von ausländischen Stellen ausgewertet werden könnten.

- Der Ausleseprozess am „Chipterminal“ erfolgt in der Regel mit Kenntnis und in Gegenwart des Betroffenen, so dass zumindest hier ein gewisses Maß an Transparenz gewährleistet werden soll. Allerdings ist es nicht völlig auszuschließen, dass – zumindest bei der für die Gesichtsbilder vorgesehenen schwächeren Basic Access Control – biometrische Daten auch von einem unberechtigten Dritten

ausgelesen werden können, der den Inhalt der maschinenlesbaren Zone kennt und über die erforderliche Technik verfügt.

In dem im Gesetzentwurf für die Verfolgung von Verkehrsordnungswidrigkeiten vorgesehenen und vom Bundesrat auch zur Strafverfolgung geforderten bundesweiten Online-Zugriff auf die bei den örtlichen Passbehörden gespeicherten Lichtbilder sehe ich eine Entwicklung, die ähnliche Wirkungen entfaltet wie die Speicherung in einer – vom Bundestag bislang aus verfassungsrechtlichen Gründen zu Recht abgelehnten – bundesweiten Zentraldatei, weil beim Online-Zugriff die Verfahrenssteuerung praktisch auf die abrufenden Stelle übergehen würde. Zudem könnte mit dem Online-Zugriff die technische Möglichkeit geschaffen werden, auf die biometrischen Daten nicht nur gezielt im Einzelfall, sondern in einer Vielzahl von Fällen zuzugreifen und die dabei abgerufenen Daten mit Aufnahmen aus der Videoüberwachung zu verknüpfen. Eine derartige Verfahrensgestaltung würde der von Verfassung wegen gebotenen Datensparsamkeit widersprechen.

Allerdings kann die Beschleunigung des Informationsaustauschs auch unter Beachtung von Datenschutzanforderungen erreicht werden, wenn dabei Verfahren eingesetzt werden, bei denen die Verfahrenssteuerung – wie bisher – bei den für die Speicherung verantwortlichen kommunalen Stellen bleibt. So halte ich es für vertretbar, wenn die von der Polizei angeforderten Lichtbilder auch elektronisch – etwa per gesicherter E-Mail – übermittelt werden, ohne dass dies zu den genannten Datenschutzrisiken führt.

Zu den einzelnen Regelungen ist folgendes anzumerken:

- Positiv ist die Verpflichtung, die biometrischen Daten gegen unbefugtes Auslesen zu sichern (§ 4 Abs. 3 Satz 2) und das Verbot einer zentralen, bundesweiten Datenbank der biometrischen Daten (§ 4 Abs. 3 Satz 3 PassG-E). Positiv zu bewerten ist auch das implizite Verbot der Übermittlung von Biometriedaten an die Dienste (§ 6 Abs. 2b Satz 2 PassG-E) , die Verpflichtung der Passbehörde zur Löschung der Fingerabdruckdaten spätestens mit Aushändigung des Passes (§ 16 Abs. 2 Satz 3 PassG-E) und die Löschungsverpflichtung des Passherstellers nach Herstellung des Passes (§ 16 Abs. 3 Satz 2 PassG-E).

- Die Forderung des Bundesrats, die Biometriedaten des E-Passes für den automatisierten Abgleich mit erkennungsdienstlichen Dateien der Polizeivollzugsbehörden zu verwenden, lehne ich ab. Dieser Vorschlag stellt Millionen rechtstreuer Bundesbürger unter Generalverdacht. Eine derartige Maßnahme würde deshalb erheblichen verfassungsrechtlichen Bedenken begegnen. Ich begrüße es daher, dass die Bundesregierung diese Forderung zu § 16a nicht aufgegriffen hat.

- Auch der Forderung, die Fingerabdruckdaten verdachtsunabhängig und auf unbestimmte Zeit vorzuhalten, sollte nicht gefolgt werden. Damit würde jeder Passinhaber praktisch erkennungsdienstlich behandelt und seine Daten würden lebenslang gespeichert. Eine derartige bundesweite, verdachtslose Speicherung ohne irgendeine, auch nur ansatzweise präzisierte Schwelle für einen im Zeitpunkt der Erhebung noch sehr vagen Zweck (evtl. spätere Strafverfolgung bzw. künftige polizeiliche Prävention) und ohne jegliche konkrete, gegenwärtige Veranlassung durch die max. ca. 50-60 Millionen Betroffenen, würde gegen die im

Volkszählungsurteil 1983 und im Juli 2005 nochmals vom Bundesverfassungsgericht in seinem Urteil vom 27.7. 2005 zum Niedersächsischen SOG (1 BvR 668/04, NJW 2005, S. 2603 ff.) konkretisierten verfassungsrechtlichen Vorgaben zum Grundrecht auf informationelle Selbstbestimmung verstoßen. Selbst bei zurechenbarer (!), vom Straftäter ausgelösten Speicherung von Fingerabdruckdaten ist die Erforderlichkeit weiterer Speicherung jeweils spätestens nach 10 Jahren zu prüfen (§ 32 Abs. 3 BKA-G).

Ich trete dafür ein, alle Neuregelungen mit Datenschutzbezug fundiert, objektiv und unter unabhängigen wissenschaftlicher Begleitung zu evaluieren.