Deutscher Bundestag **Protokoll Nr. 16/37**
16. Wahlperiode

Innenausschuss

Protokoll

37. Sitzung

(Bandabschrift)

Öffentliche Anhörung

am Montag, 23. April 2007, von 14.00 Uhr bis ca.17.00 Uhr
10557 Berlin, Konrad-Adenauer-Straße 1
Paul-Löbe-Haus, Raum 2 300

Vorsitz: Sebastian Edathy, MdB

Öffentliche Anhörung von Sachverständigen
zum

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften
BT-Drucksache 16/4138

Antrag der Abgeordneten Gisela Piltz, Dr. Karl Addicks, Uwe Barth, weiterer Abgeordneter und der Fraktion der FDP

Sicherheitslücken bei biometrischen Pässen beseitigen
BT-Drucksache 16/854

Antrag der Abgeordneten Gisela Piltz, Dr. Karl Addicks, Daniel Bahr (Münster), weiterer Abgeordneter und der Fraktion der FDP

Keine Einführung des elektronischen Personalausweises
BT-Drucksache 16/3046

Antrag der Abgeordneten Wolfgang Wieland, Volker Beck (Köln) und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Datenschutz und Bürgerrecht bei der Einführung biometrischer Ausweise wahren
BT-Drucksache 16/4159

Bericht gem. § 56a GO-BT des Ausschusses für Bildung, Forschung Technikfolgenabschätzung

Technikfolgenabschätzung
hier: TA-Projekt: Biometrie und Ausweisdokumente - Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung
Zweiter Sachstandsbericht
BT-Drucksache 16/4000

Seite

I. Anwesenheitsliste Mitglieder des Deutschen Bundestages

Bundesregierung

Bundesrat

Fraktionen und Gruppen

II. Liste der Sachverständigen für die Öffentliche Anhörung am 23. April 2007

1.	Prof. Dr. Christoph Busch	Fraunhofer Institut für Graphische Datenverarbeitung, Darmstadt
2.	Lukas Grunwald	DN-Systems Enterprise Internet Solutions GmbH, Hildesheim
3.	Sönke Hilbrans	Deutsche Vereinigung für Datenschtz e.V., Berlin
4.	Prof. Dr. Andreas Pfitzmann	Technische Universität, Dresden
5.	Peter Schaar	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn
6.	Dr. Gerhard Schabhüser	Abteilungsleiter Kryptographie BSI, Bonn
7.	Jörg Ziercke	Präsident des Bundeskriminalamtes, Wiesbaden

III. Sprechregister der Sachverständigen und Abgeordneten

IV. Protokollierung der Anhörung (Bandabschrift)

Vors. **Sebastian Edathy**: Liebe Kolleginnen und Kollegen, liebe Gäste, ich eröffne die 37. Sitzung des Innenausschusses in der laufenden Wahlperiode, die in Form einer öffentlichen Sachverständigenanhörung zu einem Gesetzentwurf der Bundesregierung bezüglich einer angestrebten Änderung des Passgesetzes und weiteren Vorlagen stattfindet. Mein Name ist Sebastian Edathy, ich bin Vorsitzender des Innenausschusses und werde die heutige Anhörung leiten. Ich danke Ihnen, sehr geehrte Herren Sachverständige, dass Sie der Einladung des Ausschusses nachgekommen sind, um die Fragen der Kolleginnen und Kollegen aus dem Innenausschuss sowie aus den mitberatenden Ausschüssen zu den Vorlagen zu beantworten. Die Ergebnisse der heutigen Anhörung sollen dazu dienen, die weiteren Beratungen, insbesondere zum Gesetzentwurf der Bundesregierung, vorzubereiten. Ich begrüße alle anwesenden Gäste und Zuhörer. Begrüßen darf ich auch für die Bundesregierung Herrn PSts Peter Altmaier. Wir haben Sie, sehr geehrte Herrn Sachverständige, darum gebeten, eine schriftliche Stellungnahme zu dem Gesetzentwurf und den damit verbundenen Fragestellungen bzw. den vorliegenden Anträgen abzugeben. Für die eingegangenen Stellungnahmen bedanke ich mich im Namen des Innenausschusses. Sie sind an die Mitglieder des Ausschusses sowie an die Mitglieder der mitberatenden Ausschüsse verteilt worden und werden dem Protokoll über die heutige Anhörung angefügt. Ich gehe davon aus, dass das Einverständnis der Sachverständigen zur öffentlichen Durchführung der Anhörung auch die Aufnahme der schriftlichen Stellungnahmen in eine spätere Gesamtdrucksache umfasst. Von der heutigen Anhörung wird eine Bandabschrift gefertigt. Das vorläufige Wortprotokoll wird den Sachverständigen mit der Möglichkeit zur Vornahme von Korrekturen übersandt. Im Anschreiben, das diesem Entwurf beigefügt wird, werden den Sachverständigen Details zur weiteren Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus dem autorisierten Protokoll und den schriftlichen Stellungnahmen, wird dann nicht nur gedruckt und an die Kolleginnen und Kollegen der beteiligten Ausschüsse verteilt, sondern zudem auch ins Internet des Bundestages eingestellt. Wie schon der Einladung zur heutigen Sitzung bzw. der Tagesordnung entnommen werden konnte, ist für die Anhörung insgesamt eine Zeit bis etwa 17.00 Uhr vorgesehen. Ich gehe da von Ihrem Einverständnis aus. Zunächst bitte ich die Sachverständigen, bevor die Möglichkeit besteht, seitens der Kolleginnen und Kollegen Fragen zu stellen, um eine Eingangsstellungnahme zur Anhörungsthematik, die bitte einen Zeitrahmen von 5 Minuten nicht überschreiten sollte. Es schließt sich dann die Befragung durch die Abgeordneten an, wobei ich die Fragesteller schon jetzt darum bitten darf, jeweils den oder die Sachverständigen zu benennen, an denen die jeweilige Frage gerichtet wird. Entsprechend der alphabetischen Reihenfolge würde ich nun zunächst Herrn Prof. Busch als Sachverständigen um sein Eingangsstatement bitten. Herr Prof. Busch, Sie haben das Wort.

SV **Prof. Dr. Christoph Busch**: Vielen Dank, meine Damen und Herren, für die Gelegenheit zur Stellungnahme. Ich habe eine Stellungnahme vorgelegt. Aus Zeitgründen möchte ich mich auf einzelne Aspekte dieser Stellungnahme beschränken. Ich stehe aber für Fragen zu allen Punkten meiner schriftlichen Stellungnahme zur Verfügung.

Das Passgesetz verweist auf Gemeinschaftsrecht. Dennoch sollte die Begründung dieses Gesetzes deutlich formuliert werden. Insbesondere sollte die in der EG-Verordnung vorliegende Begründung aus nationaler Perspektive und heutiger Sicht diskutiert werden. Aus meiner Wahrnehmung ist das Wesentliche sicher das Ziel, das mit dem biometrischen Pass erreicht werden kann, nämlich die Bindung zwischen dem Pass und dem Inhaber des Personaldokumentes zu stärken. Dies kann bei der Grenzkontrolle genutzt werden, um Personen zu detektieren, die mit einem nicht für sie selbst ausgestellten Dokument die Grenze passieren wollen. Die Entscheidung, auf EU-Ebene zusätzlich zu dem von der ICAO als obligatorisch spezifizierten Lichtbild zwei Fingerbilder in den ePass zu integrieren, war damit begründbar, dass zum Zeitpunkt der Entscheidung durch die Auswertung einer Zwei-Finger-Präsentation eine gegenüber der Auswertung eines einfachen 2D-Lichtbildes höhere Erkennungsleistung erzielt werden konnte. Sofern jedoch die biometrisch gestützten Grenzkontrollen an den EU-Außengrenzen allein auf Zwei-Finger-Präsentation basieren sollten, würde die Europäische Union nach meiner Einschätzung quasi zu einer „biometrischen Insel“. Die Prüfung der Bindung von biometrischer Charakteristik zum ePass könnte lediglich für EU-Bürger vorgenommen werden, da Bürger anderer Herkunft keine entsprechenden Referenzen in ihren Pässen vorweisen könnten. Darüber hinaus könnte die Möglichkeit eines Ersatzverfahrens, die sich mit der Aufnahme einer zweiten biometrischen Charakteristik ergibt, nicht genutzt werden. Meine Empfehlung ist daher, beim Ausbau der biometrischen Grenzkontrolle die Verifikation sowohl mit zwei 2D-Lichtbildern, als auch mit Fingerbildern in gleichem Umfange zu betreiben.

Ich habe in Abschnitt 2 meiner Stellungnahme mögliche Risiken diskutiert. Das sind Risiken, die allgemein in der Diskussion um den ePass genannt werden. Dabei ist meine Betrachtungsweise, dass ein Risiko sich nach der Versicherungsmathematik als Produkt aus Eintrittswahrscheinlichkeit und Schadenswert ergibt. Wenn wir eine Risikoanalyse betreiben, müssen wir zu den identifizierten Risiken Gegenmaßnahmen betrachten, Kosten und Aufwand dieser Gegenmaßnahmen berücksichtigen und kommen dann nach Installation möglicher Gegenmaßnahmen zu einer Identifikation des akzeptablen Restrisikos.

Unter Punkt 2.5.2. hatte ich Bezug genommen auf den Punkt der personalisierten Bomben, ein Szenario, das vom Kollegen Pfitzmann in die Diskussion gebracht wurde. Bei bekannter Information aus der maschinenlesbaren Zone, der so genannten MRZ, einer wichtigen Person - nehmen wir als Szenario den „Kennedy-Mord“ - könnte eine Bombe genau dann gezündet werden, sobald der zur bekannten MRZ passende ePass in der Nähe detektiert wird. Wir wissen aus den Studien des BSI, dass der Abstand dazu noch in einer Größenordnung des eingesetzten Proximity-Chips liegen muss, also kleiner 25 Zentimeter. Ich hatte formuliert, ich halte dies für einen möglichen Angriff, einen denkbaren Angriff. Anders als es in der Presse dargestellt wurde, halte ich es

nicht für eine dramatische Situation. Das Risiko ist aus meiner Sicht durch ein physikalisches Shielding mit einer abstrahlsicheren Tüte bspw. einer Pass-Schutzhülle - so wie ich sie seit 10 Jahren bereits verwende - kontrollierbar. Der Aufwand für die Anpassung einer solchen Pass-Schutzhülle, die ich auf der Innenseite mit Alu-Folie gefüttert habe, beträgt kostenmäßig nicht mal einen Cent, denn es sind Reste einer Küchenalu-Rolle und vom Zeitaufwand weniger als 5 Minuten.
Unter Punkt 2.7. habe ich die unzureichende Qualität der biometrischen Charakteristika der Datensubjekte, also der Person, für die der ePass ausgestellt wurde, betrachtet. Durch Umweltbedingungen oder handwerkliche Tätigkeit kann es sein, dass die Fingerbilderkennung nicht mit ausreichender Qualität erfolgen kann. Zwischen den Experten ist es strittig, welcher Prozentsatz dabei abgeschätzt werden muss. Eine realistische Einschätzung der Bedeutung dieses Risikos lässt sich nach meiner Meinung erst nach der gegenwärtigen Erprobungsphase mit der Fingerbilderfassung, die nach dem jetzigen § 23a PassG durchgeführt wird, abgeben.
Unter Punkt 2.8 habe ich die Alterung der Referenzdaten betrachtet. Der biometrische Vergleich mit einem zehn Jahre alten Fingerbild wird noch einen guten Vergleichswert erbringen. Der biometrische Vergleich mit einem zehn Jahre alten Gesichtsbild ist sowohl bei den manuellen Inspektionen durch einen Grenzbeamten schwierig als auch in einem ähnlichen Umfang schwierig für eine biometrische Gesichtsbilderkennung, die automatisch durchgeführt wird. Dieser Zusammenhang bedeutet nicht notwendiger Weise eine Verschlechterung gegenüber dem bisherigen Kontrollprozess. Meine Bewertung dazu ist: Wenn die Statistik zu Falsch-Rückweisungsraten an der Grenzkontrolle einen überproportionalen Anstieg bei hohem Alter der Referenzdaten im ePass zeigen sollte, dann müsste reagiert werden. In diesem Fall müsste ggf. die Gültigkeit des ePasses auf 5 Jahre angepasst werden.
Unter Punkt 3. ein paar Detail-Kommentare. Entschuldigen Sie, dass ich unter § 1 Abs. 1 den juristischen Formulierungen nicht ganz folgen konnte. Ich konnte nicht verstehen, warum die Formulierung „Passpflicht bei Geltungsbereich“ nicht auf die Schengen-Außengrenzen angepasst werden kann. Unter § 4 Abs. 3 heißt es: „Eine bundesweite Datenbank der biometrischen Daten wird ausgeschlossen.“ Diese Formulierung schließt regionale Datenbanken nicht ausdrücklich aus. Nach Einschätzung von Prof. Rossnagel aus dem vergangenen Jahr sind vernetzte dezentrale Datenbanken mit einer bundesweiten Datenbank in rechtlicher Hinsicht gleichzusetzen. Auch in den Unterlagen des beigefügten TAB-Berichts wurde auf Seite 51 ein ähnlicher Zusammenhang festgestellt. Aus meiner Lesart würde sich ein Widerspruch von § 4 zu § 22a ergeben, da Lichtbilder durchaus als biometrische Daten zu betrachten sind. Unter § 5 Abs. 1 könnte es nach meiner Ansicht erforderlich werden, die Gültigkeit von 10 Jahren an einen kürzeren Zeitraum anzupassen. Zu § 16 habe ich editorische Vorschläge. Die Formulierung „Biometrische Merkmale“ sollte durch „Biometrische Daten“ ersetzt werden. Biometrische Daten beinhalten sowohl biometrische Lichtbilder und Fingerbilder in jeder Verarbeitungsstufe, biometrische Referenzen und auch biometrische Merkmale, die in Templates gespeichert werden, oder sonstige biometrische Eigenschaften nach den Definitionen der ISO. Im gleichen Kontext auf der Seite 21, Seite 23 und Seite 26 sollte die Formulierung „die Iris“ durch „das Irisbild“

ersetzt werden, denn wir speichern nicht die biometrische Charakteristik, sondern ein Bild dieser biometrischen Charakteristik.
Unter Punkt 5 möchte ich als Stellungnahme zur Drucksache 16/3046 auf die Einführung des elektronischen Personalausweises eingehen. Die Aufnahme der ICOA-9303-kompatiblen Logischen Daten Struktur in den elektronischen Personalausweis ist erforderlich, wenn das Dokument nach § 1 Abs. 3 des Passgesetzes zum Verlassen des Geltungsbereiches des Grundgesetzes über eine Auslandsgrenze berechtigen soll und diese Auslandsgrenze zugleich Außengrenze des Schengen-Raumes ist. Der Anteil der Bürger, die dazu nicht den Pass selbst einsetzen, ist allerdings vermutlich gering. Nach meiner Ansicht sollte die Chance genutzt werden mit dem elektronischen Personalausweis ein Personaldokument in Umlauf zu bringen, das dem Bürger optional - wenn er dies möchte - die Nutzung der biometrischen Authentisierung auch in nicht-hoheitlichen Anwendungsfällen ermöglicht. Eine entsprechende Empfehlung habe ich auch im TAB-Bericht, Seite 78, gefunden. Die Daten könnten bei ausreichender Chip-Kapazität in einer getrennten logischen Datenstruktur abgelegt werden, ggf. sogar unter Einsatz einer Match-on-Card Lösung. Zu Nr. 2 der Drucksache habe ich auch einige editorische Anmerkungen. Ich denke, grundsätzlich kann eine biometrische Referenz aus gespeicherten Samples bestehen. Mir ist die Bedenkenformulierung unklar, das können wir gerne diskutieren. Zu Nr. 4 dort möchte ich darauf hinweisen, dass vor wenigen Wochen vom National Institute of Standards and Technology neue Testergebnisse publiziert wurden, die durchaus einen sehr positiven Entwicklungstrend zeigen.
Abschließend zu Punkt Nr. 5 und Punkt Nr. 7: Hier wird nach meiner Lesart der Eindruck erweckt, dass eine Nutzung biometrischer Daten bei der Authentisierung in privaten Online-Geschäften die Weitergabe biometrischer Daten an den Dienste-Anbieter notwendig macht. Dies ist nicht der Fall. Es lassen sich durchaus alternative Konzepte, z.B. Match-on-Card zur biometrischen Authentisierung realisieren, ohne dass das Recht auf informationelle Selbstbestimmung eingeschränkt wird.

Vors. **Sebastian Edathy**: Vielen Dank, dann hat als nächster Sachverständiger Herr Grunwald das Wort.

SV **Lukas Grunwald**: Auch ich bedanke mich bei Ihnen, meine Damen und Herren. Wir haben uns aus dem Sichtwinkel eines IT-Sicherheitsunternehmens die Spezifikation angeguckt und sind zu der Erkenntnis gekommen, dass etliche Forderungen aus dem Passgesetz nicht nach der aktuellen ICAO-Spezifikation erfüllt sind. U.a. gibt es das Beispiel, dass im Gesetz gefordert wird, dass die gespeicherten Daten gegen unbefugtes Auslesen, Verändern oder Löschen zu sichern seien. Dies ist nach der ICAO-Spezifikation weder mit Basic Access Control, also der jetzt schon in Betrieb befindlichen Sicherheitsmechanismen zum Schutz gegen das unberechtigte Auslesen, noch mit der Extendet Access Control zu erfüllen. Das Problem ist, dass die ICAO-Spezifikation konträr zu allen anerkannten Praktiken der IT-Sicherheit aufgebaut ist und somit sich zusätzliche vermeidbare Risiken aus der aktuellen Praxis des ePasses sich ergeben. U.a. besteht das Risiko, dass maliziöse Schadsoftware durch einen z.B.

duplizierten RFID-Chip in die Inspektionssysteme eingebracht werden kann. Diese Inspektionssysteme werden nach allen Vermutungen zzt. Produkte sein, d.h. Standard-PCs mit all ihren Sicherheitsproblemen und weitaus komplexere Systeme als abgeschottete und vollkommen audierbare Systeme. Durch Manipulation z.B. der logischen Datenstruktur eines ICAO-Dokumentes ist es durchaus möglich, Schadsoftware und auch Manipulationssoftware in die dahinterliegenden Systeme einfließen zu lassen und somit diese Systeme soweit zu manipulieren, dass auch nicht signierte oder kryptographisch mangelhafte Dokumente als gültig erkannt werden. Das zweite Problem, das existiert, ist, dass der Schlüssel für die Basic Access Control auf das Dokument aufgedruckt ist, und aus der MRZ - also der maschinenlesbaren Zone - ein Schlüssel aufgebaut werden kann, der dann benutzt werden kann, um eindeutig Personen, die einen ePass tragen, zu trecken und zu verfolgen. Und das dritte Problem besteht mit der Standard Access Control nach EAC. Dort ist das Fehlen eines Zeitnormals, also der Einbau einer Uhr in den ePass, so gravierend, dass es keine Möglichkeit gibt, Zugangsschlüssel, die nach Extended Access Control Zugriff auf die biometrischen Daten des Trägers gestatten, zu verifizieren. Dies ist ungefähr vergleichbar mit einem Fahrkartenkontrolleur, der entsprechende Fahrkarten kontrollieren soll, aber keinerlei Möglichkeit hat, die aktuelle Zeit zu bestimmen oder das Datum zu bestimmen. Das einzige, was er weiß, ist, welche Fahrkarte er das letzte Mal kontrolliert hat. Dadurch steht das Risiko, dass Länder, mit denen die biometrischen Daten einmal geteilt worden sind, diese Zugangsschlüssel speichern können, und später, auch wenn ihnen der geteilte Zugriff auf die biometrischen Daten der Bürger des entsprechenden Schengen-Bereichs aberkannt wird, weiter unberechtigt auf die biometrischen Daten zugreifen können, weil kein Rückrufmechanismus existiert.
Des Weiteren sehen wir erhebliche Probleme bei der Datenübermittlung zu § 6a Abs. 1, dort muss ein Sicherheitssystem aufgebaut werden, was weit mehr als nur Verschlüsselung bietet, denn die Verschlüsselung von den Daten von der entsprechenden Stelle, wo dem Bürger der Fingerabdruck abgenommen wird, bis hin zur Bundesdruckerei ist nur ein kleiner Teil und man sollte aus der Informationssicherheit das Gesamtsystem betrachten, d.h. auch alle organisatorischen Maßnahmen und alle weiteren Maßnahmen. Als Vergleich kann man z.B. das Verfahren sehen, unter dem die Stammdaten von Kontoinhabern an das BaFin übermittelt werden. Zum Schluss muss beachtet werden, dass allein das optische Auslesen der MRZ genügt, um Informationen zu gewinnen, wie z.B. auch an das biometrische Template, um also an ein perfektes Bild nach biometrischen Maßstäben heranzukommen. Es hilft dabei nicht, wenn diese Informationen nur innerhalb der Bundesrepublik Deutschland sicher sind, schließlich sind ePässe auch dazu da, dass damit verreist wird und diese somit weltweit gewissen Risiken ausgesetzt sind. Ich bedanke mich, und freue mich auf Ihre Fragen.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Grunwald. Als nächster Sachverständiger hat das Wort Herr Hilbrans.

SV **Sönke Hilbrans**: Herzlichen Dank, Herr Vorsitzender, verehrte Damen und Herren Abgeordnete. Der ePass mit biometrischen Merkmalen einschließlich Fingerabdrücken auf einem RIFD-Chip wird kommen. Der Deutsche Bundestag und sein Innenausschuss zählen eher zu den letzten Gesetzgebungsorganen, die sich damit intensiv befassen können und sollen. Nun ist der ePass und vor allem die Verordnung (EG) Nr. 2252/04 nicht vom Himmel gefallen, sondern sie ist von der Bundesregierung im europäischen Rechtsetzungsprozess mit vorangetrieben worden. Sie erkennen daran, wie bspw. auch an der Vorratsspeicherung von Telekommunikationsdaten, die ebenfalls auf Gemeinschaftsrecht beruhen soll, dass die Gesetzgebungsorgane in der Bundesrepublik Deutschland mit zu den letzten gehören, die brisante bürgerrechtlich bedeutende Entscheidungen mitverantworten sollen. Man kann das Demokratiedefizit in der Europäischen Union nennen, und dieses Demokratiedefizit bricht sich nicht erst seit der Stärkung der Dritten Säule in der Europäischen Union verstärkt Bahn. Kommen wir also zu den Möglichkeiten, die dem nationalen Gesetzgeber überhaupt noch verblieben sind und stellen zunächst fest, dass die Sinnhaftigkeit biometrischer Praktiken, biometrischer Daten in Reisepässen bis heute fragwürdig ist. Ein praktisches Bedürfnis gerade für die biometrische Auf- und Ausrüstung deutscher Reisepässe scheint mir nicht nachgewiesen. Es gibt jedenfalls keine öffentlich bekannte Evaluation der Qualität der konventionellen Pässe. Deutsche Reisepässe sind traditionsmäßig und, das hat die Bundesregierung auch immer wieder so betont, im internationalen Vergleich Spitzenprodukte. Wenn Sicherheitsrisiken durch manipulierte, ge- oder verfälschte Dokumente bestehen, dann gehen sie, vor allem was die Bundesrepublik Deutschland betrifft, zunächst einmal nicht von deutschen Reisepässen aus. Die Evaluation des ePasses wird vor diesem Hintergrund weiterhin fragwürdig bleiben und der Sinn des ePasses, zumindest für die Bundesrepublik Deutschland, bleibt spekulativ. Man wird einen Effekt im Wesentlichen feststellen können, nämlich dass durch den ePass die durchaus kostenintensive Forschung und Entwicklung an biometrischen Technologien in der Bundesrepublik Deutschland eine erhebliche Förderung erfahren hat und dass die Tendenz hin zu biometrischen Daten auf Ausweispapiere sich sicherlich als Technologie- und Wirtschaftsförderung positiv auf die entsprechenden Branchen auswirkt. Das hätte man vielleicht auch billiger haben können. Biometrische Erfassung - auch und gerade von Fingerabdrücken - und ihre Einbringung auf RIFD-Chips sind eine riskante Technologie. Sie erlauben nämlich ausländischen Bedarfsträgern, welche die Bürgerinnen und Bürger dazu veranlassen können, ihnen zumindest zeitweilig die Reisepässe zu überlassen, sich biometrische Daten von Bürgern der Bundesrepublik Deutschland zu verschaffen. Diese sind in hoher Qualität auf den Reisepass aufgebracht und die Speicherung und Verwendung dieser Daten kann die Bundesrepublik Deutschland nicht im Ansatz kontrollieren. Den Staat treffen aber, gerade wenn er eine riskante Technologie unter das Volk bringt, wie hier, die ePass-Schutzpflichten. Es bleibt trotz der Anstrengungen, die ePässe fälschungssicher und auch gegen unberechtigten Zugriff sicher zu gestalten, nur eine Frage der Zeit, bis die weite Verbreitung der RFID-Technik und die weite Verbreitung von know how in diesem technologischen Bereich, der auch durch Technologieexport von der Bundesrepublik Deutschland durchaus mitbetrieben wird, die Fälschungssicherheit und Datensicherheit

des ePasses erheblich bedroht. Es ist nur eine Frage der Zeit, bis hier technisch nachgelegt werden muss. Nutzung von Lichtbildern, meine Damen und Herren, ist ein zweiter wesentlicher Gegenstand des Gesetzgebungsentwurfs. Ich spreche von der Nutzung von Lichtbildern, die anfallen bei der Ausstattung von Pässen und Personalausweisen mit möglichst fälschungssicheren Komponenten. Nun können wir alle am Pass- wie am Personalausweisgesetz ablesen, dass das Pass- und Personalausweisregister keine Auskunftsdateien für außerpassrechtliche Zwecke sein sollen. Die Betonung liegt auf „sollen“, denn tatsächlich ist in der polizeilichen Praxis heute die Durchbrechung der Zweckbindung des Pass- und Personalausweisgesetzes für die Register schon eine Standardmaßnahme und die Abfrage von gespeicherten Lichtbildern von Bürgerinnen und Bürgern, die namentlich bekannt sind, ohne Weiteres zu realisieren. Mit der Implementierung eines automatischen Abrufverfahrens leistet das Gesetz dieser Zweckentfremdung personenbezogener Daten weiterhin erheblichen Vorschub. Ich werfe die Frage nach Alternativen auf, die Sie haben. Der Gesetzentwurf im Moment kennt die Online-Abfrage von Lichtbildern nur zur Verfolgung von Verkehrsordnungswidrigkeiten. Da besteht ein besonderes praktisches Bedürfnis, weil es dem Gesetzgeber bislang gefallen hat, durch eine ungewöhnlich kurze Verjährungszeit von nur drei Monaten die Behörde unter erheblichen Druck zu setzen. Diese kurze Verjährungsfrist ist eine Privilegierung, die ganz außergewöhnlich im Ordnungswidrigkeitenrecht ist. Der Zeitdruck für die Ermittlungsbehörden soll durch die technologische Lösung des Online-Abrufes aus der Materie herausgenommen werden. Meine Damen und Herren, verlängern Sie doch einfach die Verjährungsfrist für Verkehrsordnungswidrigkeiten. Ich komme zum Schluss mit einer Bemerkung zu dem Verbot einer bundesweiten biometrischen Datenbank. Meine Damen und Herren, es bedürfte einer solchen Datenbank nicht. Mit der Kapazität zum Online-Abruf lässt sich praktisch ihr Effekt erzeugen. Denn der vom Gesetzentwurf angestrebte Online-Abruf wird im Verein mit den Online-Zugriffsmöglichkeiten auf die Melderegister diejenigen Behörden, die an diese Systeme angeschlossen sind, schon morgen in die Lage versetzen, den gleichen Effekt zu erzielen wie ein zentrales Passregister, nämlich, dass den Behörden ohne Weiteres die Lichtbilder zur Verfügung stehen. Ich verweise im Übrigen, weil der Vorsitzende mir als Sachverständigen nur eine kurze Redezeit gegeben hat, auf die Stellungnahme der Deutschen Vereinigung für Datenschutz, die Sie vielleicht schon als Tischvorlage vorliegen haben. Sie ist dem Ausschuss heute Morgen noch zugegangen. Ich danke Ihnen.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Sachverständiger. Es war Einvernehmen bei den Obleuten, dass wir das Eingangsstatement auf 5 Minuten begrenzen, damit wir uns dann anschließend in der Diskussion mit Nachfragen beschäftigen können. Die schriftlichen Stellungnahmen sind - denke ich - von den Kolleginnen und Kollegen bereits gelesen worden. Und wenn es etwas gibt, worüber man sich nicht verständigen kann, dann ist das die Dauer von 5 Minuten. Das Wort hat der Sachverständige, Prof. Pfitzmann.

SV **Prof. Dr. Andreas Pfitzmann**: Das Großprojekt „elektronischer Reisepass“ hat aus meiner Sicht vier wesentliche Eigenschaften, zwei sind gut, zwei sind kritisch. Gut ist, wir werden digitale Speicher- und Prozessortechnologie auf dem Reisepass haben. Das ist zunächst sicherheitstechnisch einmal ein Fortschritt. Wir werden digital signiert die Daten auf dem Pass haben, d.h. also, Verfälschungen dieser Daten sind sehr gut erkennbar. Das ist der zweite Fortschritt. Dann gibt es noch eine dritte und vierte Eigenschaft, die sind kritisch, teilweise sehr kritisch. Biometrie auf dem Ausweis und insbesondere Fingerabdrücke auf dem Ausweis sind sicherheitstechnisch eine Katastrophe. Ich werde Ihnen das gleich begründen. Die Ausweise per Funk auslesbar zu machen, schafft zusätzliche Risiken. Ich kenne überhaupt keinen Grund, warum man die eingehen sollte. Also, ich kenne keinen Grund, warum man es nicht kontaktbehaftet macht. Alle Bemühungen des BSI, dann mit der Fehlentscheidung, man macht es per Funk, noch halbwegs den Schaden zu minimieren, erkenne ich an, aber kontaktbehaftet wäre deutlich besser. Sie haben meine Unterlagen bekommen. Ich werde mich jetzt einfach auf den Punkt A) konzentrieren, weil ich nicht möchte, dass ich Ihnen Behauptungen in den Raum stelle, die Sie glauben oder nicht, sondern ich möchte sie Ihnen begründen. Und ich möchte sie deswegen begründen, damit Sie es nachvollziehen können und dann vielleicht entsprechend handeln. Fingerabdrücke in Pässen helfen Kriminellen und nicht nur Strafverfolgern. Und es gibt gute Gründe, dass sie Kriminellen mehr helfen werden als Strafverfolgern, denn sie werden polizeiliche Ermittlungen deutlich erschweren. Die Schlussfolgerung aus dieser Sache ist, keine Fingerabdrücke in Pässe. Ich weiß, dass das nicht konform ist zu manchen Dingen, die auf EU-Ebene bereits beschlossen sind. Aber ich halte die Sache für dermaßen kritisch, dass ich denke, dass Sie als nationaler Gesetzgeber einen großen Fehler, den die EU gemacht hat, nicht auch vollziehen sollten, bis dahin, dass ich dem einzelnen Bürger eine Art Notwehrrecht zugestehen würde, sich dieser Sache zu verweigern. Warum? Jetzt kommt die Begründung: Die Aufnahme des biometrischen Merkmals „Fingerabdruck“ in Pässe und insbesondere seine Prüfung werden Menschen daran gewöhnen, ihre Fingerabdrücke an von ihnen nicht kontrollierbaren Geräten in hoher Qualität abzugeben. Es geht mir jetzt nicht darum, dass die Pässe unsicher sind, sondern die Menschen werden ihren Fingerabdruck bei vielerlei Gelegenheit abgeben. Damit werden Fingerabdrücke vielen Akteuren zugänglich, z.B. Grenzbeamten, Hoteliers, Läden. Alle diese werden sich dieser Technik anschließen, selbst dann, wenn sie Geräte zur Erfassung von Fingerabdrücken haben, die überhaupt nicht mit dem Pass zusammenarbeiten. Sie werden dort ein Gerät hinstellen und die Fingerabdrücke abnehmen und die Bundesbürger werden ihre Fingerabdrücke dort abgeben, denn sie sind entsprechend konditioniert. Damit haben fremde Geheimdienste und auch Kriminelle nach kurzer Zeit eine große Sammlung von deutschen Fingerabdrücken, und sie werden natürlich von diesen Mitteln in ihrem Sinne Gebrauch machen. Gebrauch machen bedeutet - sie finden die entsprechenden Videos im Internet, ich kann auch gerne die URLs vorlesen, wenn Sie darauf Wert legen -. Sie können mit Fingerabdrücken, mit Bildern von Fingerabdrücken so gute Fingerreplikate herstellen, dass gängige Fingerabdrucksensoren problemlos zu überlisten sind. Schlimmer noch ist, wenn Sie noch ein bisschen Biologie und Chemie kennen, und das ganze mit ein

paar Aminosäuren anreichern, dann werden Sie damit am Tatort auch Fingerabdrücke hinterlassen können, die für die Forensik eine große Herausforderung darstellen, ob Sie die von natürlichen Fingerabdrücken unterscheiden können. Damit wird es Kriminellen wie auch fremden Geheimdiensten gelingen, falsche Spuren an Tatorten zu hinterlassen. Sei es, um die Polizei in die Irre zu schicken - das wird Kriminelle ungeheuer freuen - oder aber als fremde Geheimdienste Personen in eine Notlage zu bringen, dass sie sich rechtfertigen müssen, dass sie mit diesem Verbrechen nichts zu tun haben. Und der vernehmende fremde Geheimdienst wird sagen: „Wissen Sie, wenn Sie mit uns zusammenarbeiten, sind Sie alle diese Probleme los.“ Das ist aus meiner Sicht der kritischste Punkt, den ich Sie bitte, nicht passieren zu lassen. Die Auswirkungen, wenn Sie es passieren lassen, wären katastrophal. Eine Erläuterung noch zu dem, was Herr Busch gesagt hat, diese Aluminiumtüte, die wir alle brauchen werden, wenn Sie die RFID-Chips passieren lassen. Aber die ist handhabbar, die ist ein Pfennigartikel, die ist zwar unbequem. Aber Fingerabdrücke, das ist wirklich katastrophal schlimm. Ich danke Ihnen.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Pfitzmann. Dann hat als nächster Sachverständiger das Wort der Bundesdatenschutzbeauftragte, Herr Peter Schaar.

SV **Peter Schaar**: Vielen Dank, Herr Vorsitzender, meine sehr verehrten Damen und Herren Abgeordnete. Ich bin mir bewusst, dass wir es hier mit der Umsetzung einer europäischen Ratsverordnung zu tun haben und insofern die Freiheitsgrade des deutschen Gesetzgebers, hier Einfluss zu nehmen, außergewöhnlich begrenzt sind. Gleichwohl möchte ich darauf zurückkommen, dass der Deutsche Bundestag, als er sich kurz nach den Anschlägen auf das World Trade Center und das Pentagon entschloss, in seinen Anti-Terror-Paketen auch die Einführung biometrischer Daten vorzusehen, sich bestimmte Entscheidungen vorbehalten hat, die ihm nach dieser europäischen Ratsverordnung so nicht mehr zur Verfügung steht. Gleichwohl ist es sinnvoll, sich mit der Einführung biometrischer Daten, insbesondere des Fingerabdrucks, noch mal auseinanderzusetzen. Nicht nur - Herr Prof. Pfitzmann hat hier richtig auf die technischen Aspekte hingewiesen – hinsichtlich der Sicherheit, sondern auch im Hinblick auf die Frage der Praktikabilität bestehen erhebliche Zweifel an der Sinnhaftigkeit der geplanten Aufnahme der Fingerabdrücke in die ePässe. Es handelt sich dabei, wie sich das mittlerweile herausgestellt hat, um einen europäischen Sonderweg. Kaum ein Staat auf der Welt ist diesem Weg bisher gefolgt, und ich nehme auch an, dass sich daran nicht viel ändern wird. Selbst die Verfahren, die bei den europäischen ePässen verwendet werden, werden in anderen Staaten, in denen Fingerabdrücke in Pässe aufgenommen werden, nicht angewandt. In den USA wird die Verwendung der Fingerabdrücke aus den von Prof. Pfitzmann genannten Gründen ausdrücklich abgelehnt. Im Übrigen ist bekannt geworden, dass das US-Governmental Accounting Office in einer jüngst durchgeführten Studie festgestellt hat, dass das dort verwendete Verfahren für die Einreisekontrolle bestimmte Sicherheitsmängel aufweist, so dass man in Zukunft wohl damit rechnen muss, dass die Vereinigten Staaten in Zukunft nicht mehr das Zwei-Finger-System verwenden werden, sondern dass es hier

zu einer sehr viel umfassenderen Datenspeicherung aller zehn Finger kommen wird, und dass auch die Inhaber der europäischen ePässe in Zukunft diese Fingerabdrücke abzugeben haben. D.h., der Vorteil, den wir uns auch teilweise damit versprochen haben, dass wir den gerade aus den USA kommenden Forderungen zur Einführung biometrischer Merkmale in Europa gefolgt sind, dieser Vorteil scheint sich so nicht zu bewahrheiten. Im Übrigen stellt sich auch die Frage, ob die Begründung, die bei der Beschlussfassung auf europäischer, aber auch auf deutscher Ebene angeführt wurde, der Kampf gegen den Terrorismus, wirklich schlüssig war vor dem Hintergrund der seither gemachten Erfahrung. Dazu kann Herr Ziercke bestimmt sehr viel mehr sagen, als ich das vermag. Soweit mir bekannt ist, sind die Anschläge sowohl des 11. September 2001, als auch die schrecklichen Attentate in Madrid und London so durchgeführt worden, dass - hätte man seinerzeit die biometrischen Reisepässe schon gehabt – sich daran wohl nichts geändert hätte, dass sie sich nicht hätten verhindern lassen. Das ist zumindest eine Frage nach der Plausibilität der Begründung, die seinerzeit angeführt wurde, und die viele von uns auch damals überzeugt hatte.
Ein letzter Punkt, auf den ich hier eingehen möchte, ist die Frage des Online-Zugriffs. Ich habe diesen Online-Zugriff in meiner Stellungnahme problematisiert, und zwar deshalb, weil er aus zwei Gründen eine Qualitätsänderung darstellt. Einmal technisch: Die bisher in über 5.000 dezentralen Dateien geführten Passregister werden auf diese Art und Weise auch hinsichtlich der biometrischen Daten miteinander vernetzt, denn ansonsten ließe sich ein solcher Online-Zugriff nicht realisieren. Damit entsteht faktisch eine virtuelle umfassende bundesweite Datei, die ausweislich des Gesetzes nicht gewollt ist. Deshalb halte ich dieses Mittel für nicht adäquat. Zweiter Aspekt: Die Verantwortlichkeit für den Abruf, die Übermittlung wechselt dann von der Stelle, die die Daten bereitstellt, auf die abrufende Stelle. Auch das ist bei Online-Verfahren eben ein qualitativer Unterschied gegenüber einer aktiven Übermittlung. Ich hätte nichts dagegen gehabt, auch die elektronische Übermittlungsform ausdrücklich zuzulassen. Der Datenschutz will solche modernen Techniken nicht verhindern. Er will auch nicht verhindern, dass Sicherheitsbehörden davon profitieren. Ein solches angemesses und wesentlich schneller zu realisierendes Mittel besteht in der Nutzung aktiver Übermittlungsverfahren. Derartige Verfahren werden wohl teilweise auch bisher schon eingesetzt, insbesondere durch Versendung der Daten mittels gesicherter e-Mails. So etwas weiter auszubauen würde nicht auf meinen Widerspruch stoßen. Vielen Dank.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Schaar, dann als nächster Sachverständiger, Herr Dr. Schabhüser, bitte.

SV **Dr. Gerhard Schabhüser**: Guten Tag, Herr Vorsitzender, meine Damen und Herren. Ich möchte jetzt weniger ein Grundsatzstatement abgeben, sondern Ihnen ein bisschen die IT-Sicherheit erläutern, die im ePass implementiert worden ist. Und dazu möchte ich zunächst einmal die Sicherheitsziele noch einmal in den Vordergrund stellen, die mit der Integration von Biometrie in Pässen erzielt werden sollen. Zweitens dann, die technische Lösung kurz beschreiben und drittens, potentielle Bedrohungen und dem gegenübergestellte Sicherheitsmaßnahmen kurz diskutieren. Die Ziele, die mit

der Einführung der Biometrie in Pässen erreicht werden sollten, sind primär zweierlei. Erstens: Die Fälschungssicherheit des Dokumentes zu erhöhen. Herr Pfitzmann ist schon darauf eingegangen, durch IT-Sicherheitsmechanismen wird das erzeugt. Zweitens: Die Bindung des Passes an den Inhaber zu stärken. Und dazu ist dann die Biometrie notwendig, in der ersten Stufe das digitale Gesichtsbild, in der zweiten Stufe - und darüber reden wir heute primär - ist es die Einführung von Zwei-Fingerabdruck-Bildern. Die Ziele werden dadurch erreicht, dass erstens ein RFID-Chip in den Pass integriert wird, der in der ersten Stufe primär ein Datenspeicher ist, mehr nicht. Ich komme gleich auf das Thema „Basic Access Control. Und in der zweiten Stufe ist der RFID-Chip ein Authentisierungstoken und eben ein Zugriffsschutzmechanismus, um die Fingerabdrücke angemessen zu schützen. Zum Einsatz kommen neben den physikalischen Schutzmechanismen des Passes, die wir heute schon haben, physikalische Schutzmechanismen des Chips, die auf einem hohen Sicherheitsniveau sind, so wie sie heute bei qualifizierten Signaturen benutzt werden - genau diese Chips werden zusammen mit einer Funkschnittstelle in diesen Pässen genutzt - und kryptographische Sicherheitsmechanismen, so dass ich als erstes bei den bedrohten Maßnahmen vielleicht die Fälschungssicherheit adressieren möchte. Die ist gesichert, einmal aus den physikalischen Maßnahmen des Passes - die kennen wir aus klassischer Dokumentensicherheit - und durch digitale Signaturen. Herr Pfitzmann hat es gesagt, das hebt den Schutz der Manipulation von Daten auf ein qualitativ anderes Niveau. Das würde ich mal so sagen. Natürlich haben wir das Problem: „Digitale Daten lassen sich beliebig kopieren“. Dagegen muss man was tun. Das steht heute in der Presse immer unter „klonen“ des Chips. „Klonen“ des Chips in der ersten Ausbaustufe, die wir heute haben: ja. In der zweiten Stufe nicht mehr, weil dann Authentisierungsmechanismen des Chips hinzukommen. In der ersten Stufe heißt es aber nicht, dass ein Pass „geklont“ werden kann, weil wir einen zusätzlichen Sicherheitsmechanismus haben, der das physikalische Dokument oder Inhalte des physikalischen Dokuments an den Inhalt der signaturgeschützten Daten des Passes bindet, nämlich der Inhalt der MRZ und zusätzlicher Daten. Dieses wird im Kontrollprozess immer mit abgeglichen, so dass ein „Klonen“ des Chips allein nicht reicht. Man muss ein „Klonen“ des Chips und des Passes haben. Wohlgemerkt, nur dann hätte man „einen geklonten Pass“, was - denke ich - heute technisch nicht möglich ist. In der zweiten Stufe, wenn eben Extended Access Control und damit impliziert eine Chip-Authentisierung integriert wird, ist das aus meiner Sicht technisch wirklich unmöglich aufgrund der Schutzmechanismen, die im Chip implementiert sind, und der kryptographischen Mechanismen, die eingesetzt werden, die wir heute auch im klassischen staatlichen Geheimschutz einsetzen zum Schutz staatlich eingestufter Informationen bis streng geheim für eine Dauer von 20, 30, teilweise 40 Jahren. Ein weiterer Punkt - und das wird häufig mit Vertraulichkeit verwechselt - ist die Zugriffskontrolle. Das hatten wir heute schon mal adressiert. Basic Access Control ist ein Mechanismus, der es verhindern soll, dass einfach im Vorbeigehen gerade einmal die Daten ausgelesen werden, mehr nicht. Es ist kein primäres Vertraulichkeitsverfahren, denn was zu schützen ist, sind neben den Daten, die man für Basic Access Control braucht - Detailwissen über den Pass, dann kenne ich den

Namen auch - als zusätzliche Information nur noch das digitalisierte Bild da, was sich in einer Entfernung von 20 cm aus dem Pass herauslesen lässt. Das schaffe ich deutlich besser, wenn ich mit einer anständigen Digitalkamera ein Foto mache, so dass der Schutzmechanismus „Basic Access Control“ primär den Schutzmechanismus widerspiegeln soll, den wir heute beim Pass haben. Beim Pass haben wir heute folgenden Schutzmechanismus: ist er zugeklappt, kann keiner die Daten lesen. Wenn ich den Pass irgendjemanden aushändige und der diesen aufklappen kann, dann kann er gleichzeitig ein Foto von der Passkarte machen und hat genau die gleiche Information, die innen drin im Chip steht. Und dieses wird durch das Basic Access Control weitestgehend simuliert. Das ist die Zielsetzung des Basic Access Control. Die Zielsetzung des Extended Access Control ist deutlich mehr, da geht es darum, die Fingerabdrücke zu schützen. Da - denke ich - hat Deutschland eine Vorreiterrolle in Europa gespielt, dass dieser Mechanismus Extendet Access Control überhaupt vorhanden ist. Es ist auf Aktion der deutschen Vertreter in den Gremien zurückzuführen und von der Struktur ist es so gelöst, dass nur autorisierte Leser eine Chance haben, diese Daten auszulesen. „Nur autorisiert“ heißt, die passausstellende Nation hat die Kontrolle über die Leser, die hinterher diese Daten auslesen dürfen und kann diese auch zurückziehen mit einem Mechanismus, der einem Revokationsmechanismus nahe kommt, der aber natürlich nicht selbst aktiv ist, weil es passintern keine Batterie gibt, denn dann würden wir nicht über Laufzeiten von 10 Jahren reden, aber effektiv ist, um Missbrauch an dieser Stelle zu verhindern. Und damit möchte ich an dieser Stelle stoppen, danke.

Vors. **Sebastian Edathy**: Danke, Herr Dr. Schabhüser. Als letzter in der Reihe der Sachverständigen aufgrund des „Z“ im Nachnamen hat der Sachverständige Herr Jörg Ziercke, Präsident des Bundeskriminalamtes, das Wort.

SV **Jörg Ziercke**: Vielen Dank, Herr Vorsitzender, meine sehr verehrten Damen und Herren Abgeordnete. Aufgrund der vielen Vorbemerkungen komme ich gleich zur Bedeutung und zum polizeilichen Mehrwert biometrischer Systeme in Ausweisen. Neben der Bekämpfung der Fälschungskriminalität ist es angesichts des Problems der missbräuchlichen Benutzung echter Identitätsdokumente durch Unberechtigte wesentliche Zielsetzung der Einführung biometrischer Verfahren, die bisherigen auf Gesichtskontrollen gestützten Verfahren der Einreise, Aufenthalts- und Identitätskontrolle, durch Einsatz messtechnischer Verfahren zu erweitern. Die verschiedenen Sachfahndungsbestände weisen hohe Zahlen als verloren oder als gestohlen gemeldete Dokumente aus und dokumentieren daher die Bedeutung dieses Konfliktphänomens für die innere Sicherheit in Deutschland. So sind z.B. im Gesamtbestand in Deutschland aktuell insgesamt ca. 10,6 Mio. Gegenstände ausgeschrieben, darunter ca. 3 Mio. ausgeschilderte Dokumente. Im Schengener Informationssystem sind aktuell sogar 17,3 Mio. Sachen zur Fahndung ausgeschrieben, darunter alleine ca. 14,4 Mio. ausgestellte Dokumente. Im Interpolsystem 24/7 sind aktuell 1,675 Mio. Dokumente aus Deutschland und 13,55 Mio. Dokumente aus 122 Staaten der Welt zur Fahndung ausgeschrieben. Es sind konkrete Fälle belegbar, bei

denen Verdachtspersonen, sei es im Bereich Terrorismus, der Organisierten Kriminalität oder auch Kriegsverbrecher, quer durch Europa gereist sind, durch viele Staaten gekommen sind mit ge- und verfälschten Ausweispapieren, ohne bei nachgewiesener Kontrolltätigkeit tatsächlich erkannt zu werden. In Deutschland gab es 7.154 Feststellungen von Urkundsdelikten im Jahr 2005 unmittelbar an den Grenzen. Eine annähernd gleich bleibende Zahl in den letzten Jahren waren davon ca. 3.100 Verfälschungen von Dokumenten, 2.700 Totalfälschungen und 665 Missbrauch von Ausweispapieren. Bei der Bundespolizeidirektion in Koblenz sind ca. 5.400 Ausweisdokumente im Jahr 2005 auf Fälschungsverdacht untersucht worden. Die Untersuchung der Bundespolizei und aus dem benachbarten Ausland ergeben erhebliche Anteile, nämlich zwischen 10 und 70 %, je nach Stichproben und Ort der missbräuchlichen Verwendung von Dokumenten am Gesamtaufkommen urkundenbezogener Delikte. Diesem Deliktsfeld wird durch die Einführung biometrischer Merkmale - ich denke aus polizeilicher Sicht verständlich - im Personaldokument und ihrer Kontrolle wirksam begegnet. Dabei werden bei einem maschinell gestützten Vergleich die im Prozess erhobenen biometrischen Merkmale an der Person mit der dokumentierten Identität abgeglichen und so die Zugehörigkeit von Reisedokument und dessen Besitzer verifiziert. Ich komme zu einigen Einzelfragen. Zunächst zur Frage der Speicherung von Fingerabdruckdaten: Aus polizeilicher Sicht könnte eine recherchierbare Speicherung, z.B. im Bereich der Interpol-Fahndung mit Fingerabdruckdaten oder bei der Identifizierung Vermisster oder unbekannter Toter, so auch bei Einsätzen der Identifizierung des BKA eine Verbesserung der Ermittlungsansätze und der Beschleunigung der Ermittlung bedeuten. So wurden in Deutschland im Jahr 2006 exakt 1.043 Personen vermisst, von denen nur 534 in 2006 identifiziert werden konnten, 371 Personen wurden zunächst als unbekannte Tote aufgefunden, davon konnten in 2006 nur 205 identifiziert werden. Es wäre auch ein Abgleich von einem Tatort gefundene Fingerspuren möglich, sofern die Tatortspuren allerdings von den Zeigefingern stammen. Voraussetzung bei diesen Überlegungen ist allerdings, dass recherchierfähige Bestände vorliegen. Zweitens zum Online-Abruf von Lichtbilddaten: Durch die Zulassung des automatisierten Abrufs von Lichtbildern aus dem Pass- und Ausweisregister durch Polizei und Ordnungsbehörden bei Straßenverkehrsordnungswidrigkeiten bleiben unter eng umgrenzten Voraussetzungen bereits heute Verwaltungsabläufe möglich, die man zukünftig durch moderne Informationstechnik vereinfachen und deutlich beschleunigen könnte. Ich will aus der Praxis das gängige Beispiel im Grunde schildern. So sind Fälle der täglichen Polizeipraxis bei Ermittlung von Delikten der Verkehrsunfallflucht, wo sich Zeugen melden, die Fahrzeugkennzeichen und Fahrer gesehen haben, das sofortige Aufsuchen der Wohnanschrift des Fahrzeughalters unmittelbar nach dem Unfall sehr häufig negativ. Denkbar ist, dass ein anderer als der eingetragene Fahrer den Unfall verursacht hat. Deshalb greift die Polizei in solchen Fällen auf eine Wahllichtbildvorlage, so heißt es, um den Fahrer durch den Zeugen vorläufig identifizieren zu lassen. Dies kann auch zur Entlastung des Halters dienen, wenn er selbst nicht gefahren ist. Der Online-Zugriff auf diese Bilddaten würde hier die Ermittlung deutlich beschleunigen und evtl. Unbeteiligte frühzeitig schonen. Eine Erweiterung der Möglichkeit zum

automatisierten Abruf von Lichtbilddaten durch Polizei für Zwecke der Strafverfolgung ist daher sinnvoll. Das gilt auch bei Verhütung von Straftaten bzw. der allgemeinen Gefahrenabwehr, wie schon dargestellt, so z.B. bei der Fahndung von Vermissten oder hilflosen Personen. Im Hinblick auf die derzeit zu beobachtende Diskussion verweise ich noch einmal darauf, dass es bei dem vorgeschlagenen Online-Abruf von Lichtbildern um die Beschleunigung der Beschaffung von Lichtbildern bekannter Personen oder bekannten Pass- und Personalausweisbehörden geht. Nun kurz zu den angeblichen Sicherheitslücken im elektronischen Reisepass: Ich will nicht das wiederholen, was von BSI hier gesagt worden ist, aber noch eine allgemeine Eingangsbemerkung. Die verschiedentlich vorgebrachten Argumente zu angeblichen Sicherheitslücken im elektronischen Reisepass sind in der Sache nach unserer Überzeugung stark übertrieben, teilweise sind es realitätsferne Versuchsanordnungen, die zu Ängsten bei der Bevölkerung von biometrischen Ausweispapieren führen sollen. So sind z.B. Hinweise auf Versuche aus den Niederlanden schon deshalb unzulässig, weil dort das Extended Access Control-Verfahren bei diesen Versuchsanordnungen nicht zum Einsatz kam. Behauptung, die ein aktives Mitleben des RFID-Chips aus 10 Meter Entfernung feststellen, entbehren jeglicher Grundlage, typischerweise sind es 10 bis 20 cm zum Dokument einer Person, deren Daten, z.B. Pass-Nr., Ausstellungs- und Ablaufdatum, die man bereits vorher kennen muss, die Person muss also bereits bekannt sein. Ein Bild von dieser Person zu erhalten, wäre mit einem Fotoapparat aus größerer Entfernung viel einfacher möglich. Die Fingerabdrücke sind nicht zu erlangen, da sie durch das EAC-Verfahren geschützt sind. Ich weiß nicht, was ein derartiger Versuch wem eigentlich beweisen soll.
Ich komme zum Bombenszenario aus Dresden: Die dazu veröffentlichten Beispiele sind meiner Ansicht nach absolut realitätsfern. Die Abschirmung des Passes durch so genannte leitende Materialien durch einen Schutzumschlag - das hat der erste Sachverständige schon gezeigt - ich habe hier einen ähnlichen. Man benutzt diesen Umschlag nur, um den Ausweis dort hineinzustecken, und dann ist dieses Szenario völlig entzaubert. Ich halte es im Übrigen für völlig realitätsfern. Auch die zweite Bemerkung: Fingerabdrücke an Tatorten, die dazu führen sollen, dass man das alles grundsätzlich zu überdenken hat. Die Geschichte der Fingerabdrücke ist so alt wie diese Geschichte, dass man evtl. an Tatorten Fingerabdrücke mutwillig hinterlegen könnte. Das wissen organisierte Kriminelle schon seit 100 Jahren weltweit. Es sind überhaupt keine Beweise vorhanden, dass das in dieser Form überhaupt jemals ein Problem gewesen ist, aber entscheidend ist etwas anderes. Der Fingerabdruck hat keine absolute Bedeutung im Strafverfahren. D.h., er ist nur ein Hinweis darauf, dass es weitere Ermittlungen bedarf, um festzustellen, ob sich eine Person berechtigt oder unberechtigt an einem Tatort aufgehalten hat. Es ist keinerlei Beweis im Hinblick auf eine Tat. Vielen Dank.

Vors. **Sebastian Edathy**: Wir würden jetzt einsteigen in die Befragung der Sachverständigen. Ich schlage vor, dass wir zunächst eine Runde der Berichterstatterinnen und Berichterstatter veranstalten. Dann hat zunächst der Kollege

Clemens Binninger von der Unionsfraktion das Wort. Wie einleitend bemerkt, bitte kurz ansprechen bei der Frage an wen sie gerichtet ist. Herr Binninger, bitte.

BE **Clemens Binninger**: Ich habe zunächst die Fragen an Herrn Ziercke und Herrn Schabhüser. Herr Ziercke, im derzeitigen Gesetzentwurf ist vorgesehen, dass die biometrischen Daten bei entsprechendem Verdacht bei Drittstaatsangehörigen auch Online mit dem BKA Datenbestand abgeglichen werden können. Halten Sie es für hilfreich, dass wir so etwas nicht auch für bei entsprechendem Verdacht immer vorausgesetzt, bei deutschen Passangehörigen haben sollten. Es könnte sein, dass man den Verdacht auf einen veränderten Pass hat, trotz falscher Personalien - das Dokument ist also echt, aber die Personalien sind falsch - das ist denkbar, der Bundesrat hat in seiner Stellungnahme darauf hingewiesen. Hier ist zwar der Pass für echt zu halten, aber das Geburtsdatum leicht zu verändern. Dann bräuchte man so eine Möglichkeit. Frage: Halten Sie das für sicherheitsfördernd und auch praxisnotwendig? Und die Frage an Herrn Schabhüser: Ich bin kein Techniker, aber könnten Sie noch einmal das Beispiel schildern - ich habe es aus Ihrer Stellungnahme entnommen, wo Sie deutlich machen, wie viele Tage Zeit man eigentlich bräuchte, um etwas auszulesen, was in der Realität gar nicht vorkommt, weil man sowohl das Dokument als auch den Passinhaber verfügbar haben müsste, Und eine Zusatzfrage - vielleicht an beide Sachverständige: Es wurde vorher von einzelnen Sachverständigen sehr stark darauf abgehoben, was man mit diesen biometrischen Fingerabdrücken alles machen könnte. Da frage ich mich: Das kann ich doch alles heute schon. Fingerabdrücke von anderen Personen kann ich mir doch heute auf vielfältigste Weise einfacher besorgen. Dazu brauche ich keinen biometrischen Pass. Die Verquickung zwischen biometrischem Pass, und Missbrauch von Fingerabdrücken schien mir hier überhaupt nicht plausibel, sondern es ist Realität, solange es Ganoven gibt, möchte ich fast mal sagen. Wenn Sie dazu noch etwas sagen könnten.

Vors. **Sebastian Edathy**: Vielen Dank, dann zunächst Herr Ziercke und dann Herr Dr. Schabhüser, bitte.

SV **Jörg Ziercke**: Zunächst zur Frage des Online-Abgleichs im BKA. Dazu muss man wissen, dass jeder Online-Abgleich natürlich auch Zeit kostet. Dieser Zeitbedarf muss vor dem Hintergrund der Grenzkontrollen oder dort, wo die Kontrollmaßnahme stattfindet, in Einklang gebracht werden mit den Geschäftsprozessen vor Ort. D.h., ich brauche für eine Überprüfung im AFIS-System bis zu 60 Sekunden, das kann auch längerfristiger sein, insbesondere dann, wenn es möglicherweise mehrere Treffer geben sollte, so dass der Zeitfaktor aus der Sicht des BKA mit ein entscheidender ist.
Die weitere Frage ist, wenn ein Abgleich erfolgt über zwei Finger, also über die beiden Zeigefinger, dann ist das wiederum ein Faktor, der dazu führen kann, dass es einen „out-put“ gibt an möglichen Treffern mit einer entsprechenden Anzahl an Überprüfungsfällen, die dann wiederum Zeit erfordern. Vorstellbar ist das selbstverständlich, aber ich möchte darauf aufmerksam machen, die zwei Finger, die

dort nur zugrunde gelegt werden, sind natürlich was die Überprüfungen in einem solchen Datenbestand angeht, ein grundsätzliches Problem.
Zur Frage der Fingerabdrücke jetzt im biometrischen Pass - ich habe es eben schon deutlich gemacht, ich kann Ihnen da nur zustimmen - die Fingerabdrücke sind bisher auch in jeder Form, die hier angesprochen worden ist, immer wieder als Problem hingestellt worden. Dieses ist ohne biometrischen Pass in der Praxis längst erkannt worden. Und ich habe deutlich gemacht, dass Fingerabdrücke auch in der Forensik kein absoluter Beweis sind, dass sich alle Beteiligten, die Fingerabdrücke am Tatort finden, sehr wohl des Umstandes bewusst sind, dass man weitere Spuren suchen muss, DNA-Spuren suchen muss, dass man Situationsspuren darstellen muss, dass Tatorte umfangreich ermittelt werden müssen. Dass es insbesondere auf die Alibiüberprüfung von Personen ankommt, so dass diese absolute Bedeutung, die einer der Sachverständigen hier in diesen Bereich hineingelegt hat, aus meiner Sicht so überhaupt nicht gegeben ist.

Vors. **Sebastian Edathy**: Vielen Dank, dann bitte Herr Schabhüser.

SV **Dr. Gerhard Schabhüser**: Herr Binninger, zu der Frage: Wie viele Tage brauche ich zum aktiven Auslesen eines Chips? Und jetzt muss ich ergänzen, wenn ich nicht die Inhalte im Wesentlichen schon kenne, also im Szenario: Ich versuche bei einem vorbeigehenden Menschen gerade mal - vielleicht auch nicht vorbeigehend, dazu werde ich gleich etwas sagen - den Inhalt des Chips auszulesen. Dazu muss ich das Basic Access Control-Protokoll, so wie ich es eben beschrieben habe, überwinden und dazu müsste ich die Pass-Nr., das Geburtsdatum und das Ablaufdatum des Passes kennen. Um diese Daten herauszufinden, das Bild zu lesen, und dann hinterher den Namen auslesen zu können, worüber ich vorher keine Informationen habe, muss ich das ausprobieren, immer wieder ausprobieren, bis ich die richtige Pass-Nr., das Geburtsdatum und Ablaufdatum des Passes habe. Da kann man jetzt darüber philosophieren, wie viele unbekannte Werte vorhanden sind. Ich bin an der Stelle sehr vorsichtig und sage, es sind vielleicht nur noch 20 Bit unbekannt, das ist relativ wenig in der Kryptographie, aber durch die Tatsache, dass der Chip selbst zum Beantworten des Protokolls ungefähr 1 Sekunde braucht, brauche ich eben zwei hoch zwanzig Sekunden, um einzudringen. Ein Jahr hat zwei hoch fünfundzwanzig Sekunden, also muss man das ganze Jahr - 365 Tage - durch 32 teilen, dann kommt man auf die Tage, die benötigt werden, also 12 Tage. In der Zeit muss der Mensch stillstehen, 25 cm in der Nähe muss das Lesegerät sitzen, sonst geht das nicht. Das scheint mir definitiv unrealistisch.
Was kann ich mit Fingerabdrücken machen? Die andere Frage hat Herr Ziercke meiner Meinung nach schon hinreichend erläutert. Natürlich, ich komme heute auch schon an Fingerabdrücke heran, auch wenn ich den Pass in der Hand habe, wird auf der Pass-Karte - die ist relativ glatt - auch ein Fingerabdruck sitzen, den kann man dann auch wieder nutzen. Oder wenn ich hier heute den Raum verlasse, wird mein Fingerabdruck auf den Gläsern sicherlich in verschiedenster Form vom linken Zeigefinger, rechten Zeigefinger auch verfügbar sein. Mit krimineller Energie komme ich da ran.

Vors. **Sebastian Edathy**: Ich darf dann fragen, wer für die FDP-Fraktion sprechen möchte? Herr Wolff, dann haben Sie jetzt das Wort, bitte.

Abg. **Hartfrid Wolff (Rems-Murr)**: Liebe Kolleginnen und Kollegen, ich möchte drei Schlussfolgerungen aus den bisherigen Statements der Sachverständigen ziehen. Zunächst einmal ist eines meines Erachtens unwidersprochen geblieben, die Feststellung von Herrn Schaar, dass diese Maßnahmen nicht zur Verhinderung von Straftaten gelten. Im Gegenteil, Herr Ziercke sprach sogar davon, dass man damit potentiell Vermisste suchen könnte. Ich fragte mich, denkt er tatsächlich an einen RFID-Chip oder sogar schon an Ordnungsmechanismen. Interessant ist die Tatsache, dass offensichtlich innerbehördlich wie auch extern eine stärkere Transparenz, auch der persönlichen Daten inklusive der biometrischen Daten, da ist. Um das jetzt objektiv festzuhalten, und was mich beeindruckt hat, Herr Ziercke, die erhebliche Anzahl von Missbrauch von Pässen insgesamt, auch von gestohlenen Pässen, das würde natürlich auch automatisch, wenn dort ein entsprechender Chip existieren würde, auch eine größere Transparenz von biometrischen Merkmalen ergeben. Da schließen sich folgende Fragen aus meiner Sicht an: Direkt die Frage an Herrn Schaar und an Herrn Grunwald. Die Frage der Übermittlung der biometrischen Daten, das betrifft zum einen die Übermittlung von Passbehörden an die Bundesdruckerei. Wie sicher ist diese Übermittlung tatsächlich? Und wie sehen tatsächlich die Sicherheitskonzepte der Behörden vor Ort aus, der kommunalen Passbehörden? Können wir davon ausgehen, dass dieses Behördennetzwerk auch ausreichend sicher ist und dass wir einen vergleichbaren Standard auf Bundesebene haben? Das nächste ist für mich: Es war interessant, wie Herr Schabhüser ausführte, dass Duplikate nicht möglich seien, das haben wir von anderen Sachverständigen gerade anders gehört. Da schließt sich aber für mich an, wenn wir die Online-Überprüfung haben, dass hier weitere Gefahren existieren können. Ich glaube, Herr Grunwald und Herr Hilbrans haben es schon angedeutet: die möglichen Angriffe von Computerviren. Wie sieht es da konkret aus? Wie konkret sind diese Gefahren, wenn da externe Eingriffe da sind? Und da schließt sich die dritte Frage an Herrn Schabhüser an: Sie sprachen davon, jetzt ist es sicher und haben das Basic Access Control sehr stark nach oben gehoben. Mich interessiert daran die Tatsache, jetzt ist es sicher. Wie sieht es in der Weiterentwicklung aus? Diese Pässe sollen ja 10 Jahre lang gelten. Ist da tatsächlich die Sicherheit für die Zukunft auch gewährleistet? Und eine letzte Frage noch an Herrn Schaar: Ist es aus Ihrer Sicht, was den Eingriff in Grundrechte angeht, ein Unterschied und wenn ja, welcher, wenn Sie einerseits eine zentrale Abrufbarkeit einer zentralen Datenbank haben, oder eben eine dezentrale Speicherung einer vernetzten Datenbank? Sehen Sie da erhebliche Unterschiede. Vielen Dank.

Vors. **Sebastian Edathy**: Angesprochen sind - und ich bitte auch in dieser Reihenfolge die Fragen zu beantworten - Herr Grunwald, Herr Hilbrans, Herr Schaar und Herr Schabhüser. Herr Grunwald, bitte.

SV **Lukas Grunwald**: Kommen wir erst mal zur Übermittlung der entsprechenden Daten. Man muss sich das heute folgendermaßen vorstellen: Dort, wo die Pässe erstellt werden, wo von den Bürgern die Fingerabdrücke abgenommen werden, das ist ein großer dezentraler Bereich, meistens in irgendwelchen Passämtern, irgendwelchen Bürgerbüros oder anderen Bereichen, wo vielerlei Informationen erhoben werden, Fehlerinformationen bearbeitet werden, vom Antrag auf Hartz-IV-Leistungen, über Wohngeld bis hin zu den entsprechenden Reisedokumenten. Dort muss beachtet werden, dass dieses Verwaltungspersonal keinerlei Kompetenz im Bereich IT-Sicherheit und Datenschutz hat. Und man muss beachten, es ist nicht damit geholfen, eine Kryptobox irgendwo in einen Verwaltungsbereich reinzustellen, dass dann nur die Daten auf der Leitung, d.h. von der Kryptobox bis zur …….. gesichert sind. Aber was ist z.B. mit dem Netz innerhalb dieser Bürgerbüros, was ist mit den Angestellten, was ist mit den gesamten Verfahren auch auf den Rechnern, die auch für vielerlei andere Funktionen von Hartz-IV-Software, das bedeutet Internetzugang auf den Rechnern, irgendwelche Online-Zugriffe bis hin zu dieser Leitung. Da müssten dann dedizierte Konzepte erarbeitet werden, und das Sicherheitsniveau müsste angeglichen werden, z.B. zu den entsprechenden Bankenrechenzentren, die dazu benutzt werden, um z.B. die Daten zentral von den Bankenrechenzentren die Stammdaten an die BaFin zu übertragen, d.h. die gesamte Sicherheit und der gesamte Aufwand für die Bürgerbüros ist zzt. gar nicht zu beziffern. Sicherlich sind die Kosten, um so ein Sicherheitsniveau zu erzeugen, was auch für den Bürger und auch für die Bilanz der Daten angemessen ist, nicht damit getan, einfach eine Kryptobox hinzustellen. Dazu kommen Audits, dazu kommen regelmäßige Sicherheitsüberprüfungen, die u.a. auch in der Homepage des BSI nachgelesen werden können. Dort sind auch u.a. mit dem Grundbuchhandbuch und diversen anderen Anleitungen Richtlinien für die Behörden abgelegt, die das Sicherheitsniveau genau definieren. Zu der Gefahr der Viren und der anderen Schadsoftware muss gesagt werden, solange ich mich nur auf einem Smartcontroler bewege, habe ich ein relativ kleines System mit wenig Komplexität. Nun hat die IK ein hochkomplexes System eingefügt, was leider erst das Entgegennehmen der Daten und dann die Überprüfung, ob die Validität zulässt. Das ist konträr zu sämtlichen Best-Practices der IT-Sicherheit. Ich nehme keine Daten entgegen, wenn ich ihnen schon nicht vertrauen kann. Hierbei werden Daten entgegengenommen und das Vertrauen erst nachträglich dargestellt, indem anhand einer so genannten kryptographischen Signatur geprüft wird, nachdem die Daten schon im System eingelesen wurden. Es ist ungefähr vergleichbar, als wenn Sie den Grenzbeamten einfach mal fragen: Können Sie den USB-Stick mal kurz in Ihren Rechner stecken. Das wird sicherlich keiner machen. Nachdem diese Daten dann angenommen worden sind, werden sie erst verarbeitet und erst dann kann eine Überprüfung der entsprechenden Daten stattfinden. Dies ermöglicht natürlich auch neuartige Angriffe, indem wir jetzt von uns bekannten Medien - das sind auch die Reisepässe, die den Bürgern in die Hand gegeben werden - einfach Daten, die innerhalb der Inspektionssysteme hineingeholt werden. So wäre das Szenario möglich, dass durch eine Manipulation die nächsten 10 oder 20 folgenden Pässe, obwohl über unzureichende kryptographische Maßnahmen

oder gar keine Signatur verfügen, auch als gültig anerkannt werden, nachdem das Lesegerät entsprechend manipuliert sein könnte.

Vors. Sebastian Edathy: Vielen Dank, dann Herr Hilbrans, bitte.

SV **Sönke Hilbrans**: Ich kann mich Herrn Grunwald im Wesentlichen anschließen. Vielleicht noch eines, nämlich dass die IT-Infrastruktur wie auch der Ausbildungsstand zwischen den Bundesländern schon sehr stark abweichen. Das ist auch zum Teil innerhalb der Bundesländer so. Was die Qualität und Sicherheit der Kommunikation angeht, verbieten sich im Moment zumindest pauschale Antworten.

Vors. **Sebastian Edathy**: Dann Herr Schaar, bitte.

SV **Peter**: Die Frage nach Sicherheit der Datenübermittlung muss man auf verschiedenen Ebenen und für verschiedene Phasen beantworten. Zum einen geht es um die Beantragung und Ausstellung des Passes. Dann geht es um den Lesevorgang bei einer Kontrolle und schließlich geht es um die Diskussion über die Sicherheit beim Online-Zugriff von Dritten auf die dezentralen Passdateien. Zum ersten Punkt gibt es einen Sicherheitsaspekt, auf den der Bundesrat hingewiesen hat, nämlich auf Seite 5 seiner Stellungnahme. Dort heißt es, dass es möglich sei, einen echten Pass mit unrichtigen Angaben, z.B. durch Täuschung oder die Bestechung eines Mitarbeiters der passausstellenden Behörde zu erlangen. Das ist ein nichttechnisches Risiko, das zwar prinzipiell gegeben ist, aber sicherlich in unseren Verwaltungsstrukturen nicht so häufig stattfindet. Aber es ist nicht vollständig von der Hand zu weisen. Wenn Sie nach der technischen Sicherheit fragen, dann ist es so, dass ich als Bundesdatenschutzbeauftragter zusammen mit meinen Mitarbeitern in den Konzeptionsprozess für das Enrolment auch einbezogen worden bin und keine Beanstandung hatte. Es wird hier gewährleistet - soweit man das nach derzeitiger Sicht sagen kann -, dass dieser Prozess ausreichend gesichert ist. Dies gilt auch für die Übermittlung der Daten an die Bundesdruckerei und die anschließende Verarbeitung der biometrischen Daten dort und die Einbringung in die Pässe. Gleichwohl ist es natürlich so, dass es immer ein Restrisiko gibt. Das ist hier nicht anders als in anderen Bereichen, wobei ich allerdings auch sagen muss, wir haben es in vielen anderen Bereichen mit Daten zu tun, die weitaus sensibler sind, die auch gesichert werden können. Für mich ist das nicht die zentrale Schwachstelle. Beim Lesevorgang ist ja auf die verschiedenen technischen Aspekte hingewiesen worden. Basic Access Control ist das schwächere Verfahren, Extended Access Control das stärkere. Die von Herrn Grunwald angeführten Szenarien sind nicht abwägig, aber sie sind nicht allzu realistisch, auch im Hinblick auf den Aufwand, der zu treiben ist, um zusätzliche Informationen zu bekommen. Eine vollständige Sicherheit ist durch Basic Access Control nicht zu gewährleisten, das ist wahr. Zum Auslesen müssen zwei Voraussetzungen gegeben sein: Erstens die Kenntnis von den Daten, die in der maschinenlesbaren Zone vorhanden sind und zweitens ein entsprechendes Lesegerät. Das sind die beiden Voraussetzungen, die man braucht. Wenn diese Voraussetzungen

gegeben sind, kann man die Daten auslesen, bekommt dann aber als Zusatzinformation nur das Bild, nicht den Fingerabdruck. Der Fingerabdruck ist zusätzlich gesichert durch Extended Access Control. Auch dabei ist es zwar nicht 100%ig auszuschließen, dass es möglich ist, die kryptographischen Sicherungsmaßnahmen zu überwinden, aber es ist extrem unwahrscheinlich. Wesentlich problematischer ist allerdings, was passiert mit den Daten, wenn sie denn ausgelesen worden sind? Wo landen sie dann? Und das entzieht sich natürlich der Kontrollmöglichkeit der deutschen Stellen. Sofern es ausländische Behörden sind, bei denen die Daten landen, dass sie dann möglicherweise in zentralen Datenbanken landen, Was wir hier nicht haben wollen, kann durchaus in anderen Staaten entstehen, wenn ich einreise, oder wenn dort mein Pass an anderer Stelle kontrolliert wird. Völlig ungeklärt ist hingegen die Frage: wie sieht es mit der Sicherheit eines möglichen Online-Zugriffs aus? Wir haben mehr als 5.000 kommunale Stellen, die diese Pass- und Personalausweisregister führen. Wenn darauf der Online-Zugriff gewährleistet werden soll - mit sehr unterschiedlichen Strukturen - in der Büroumgebung, da gebe ich meinen Vorrednern auch Recht - dann ist das ein ganz erhebliches zusätzliches Risiko. Es ist damit verbunden, dass diese Strukturen - wie wir immer wieder als Datenschutzbeauftragte bei unseren Prüfungen feststellen - häufig massive Sicherheitslücken aufweisen. Wenn man jetzt dort zusätzlich einen entsprechenden Zugriffsmechanismus installieren will, dann ist das ein weiterer Zugriffspfad, der verwendet werden kann. Die Daten müssen dann auch zu den abrufberechtigten Stellen transportiert werden. Die Frage, wie die Übermittlung gesichert werden kann, muss man auch bedenken. Aber es ist ein zusätzliches Risiko, das ist nicht von der Hand zu weisen. Wie man dieses beherrschen will, ist mir - ehrlich gesagt - noch nicht klar geworden. Und darüber enthalten der vorliegende Gesetzentwurf und die unterschiedlichen anderen Materialien, die ich kenne, bisher keine Aussagen.
Im Hinblick auf die verfassungsrechtliche Würdigung unterschiedlicher Dateisysteme, Herr Abgeordneter Wolff, sehe ich vom Schutzgut informationelles Selbstbestimmungsrecht her keinen Unterschied zwischen einer bundesweiten Datei und einer virtuellen Datei, die durch die Vernetzung verschiedener dezentraler Dateien entsteht. Die Online-Zugriffsmöglichkeit setzt technische Zugriffspfade voraus. Und damit führt sie zu einer entsprechenden Vernetzung, wenn auch nicht in der ersten Ausbaustufe, so doch zumindest in einem späteren Stadium. Insofern sehe ich das aus der verfassungsrechtlichen Perspektive vollständig gleich.

Vors. **Sebastian Edathy**: Vielen Dank, dann Herr Dr. Schabhüser, bitte.

SV **Dr. Gerhard Schabhüser**: An mich ist die Frage gestellt worden: Jetzt sind die Verfahren sicher, was ist in 10 Jahren? Dazu gibt es zwei Aspekte zu berücksichtigen. Das eine sind die kryptographischen Fragestellungen. Die Kryptographie, die in diesem Kontext eingesetzt wird, ist nach meiner Einschätzung - und ich verantworte immerhin den Hochsicherheitsbereich in der Bundesrepublik Deutschland, also den Verschlusssachenbereich bis streng geheim - kann man mit dem Verfahren 20 bis 30 Jahre durchaus leben. Sie werden so lange sicher sein. Das Verfahren „Triple DES“,

was im Basic Access Control eingesetzt wird, haben wir nicht im staatlichen Geheimschutz eingesetzt. Es ist aber hinreichend gut evaluiert, um mit seinen 112 Bit Schlüsseln, die beim Extended Access Control wirklich zum Einsatz kommen, eben auch die Sicherheit über diese Laufzeit durchaus zu gewährleisten. Die Chip-Sicherheit - das ist der zweite Punkt, den man adressieren muss - die wird permanent gepflegt. Jede Generation Chip bekommt neue Sicherheitsfeatures herein. Die Technik wächst weiter. Das geht voran. Natürlich ist es so, dass ein 10 Jahre alter Chip dann nicht mehr die Sicherheit aufweist, wie ein gerade frisch aus der Produktion gekommener Chip. Das ist heute bei den Pässen auch so. Mein 10 Jahre alter Chip, mein Pass oder Personalausweis hat andere Sicherheitsmerkmale, als der heute ausgestellte. Aber das Sicherheitsniveau ist immer noch hoch, und das würde ich auch an dieser Stelle in 10 Jahren sagen. Ein dritter Punkt, den ich vielleicht adressieren möchte, ist die Übertragung der Passdaten. Herr Schaar hat es schon beschrieben. Die Übertragung der Passdaten wird durch Sicherheitsanforderungen, die vom BSI zusammen mit dem BKA und auch mit dem Datenschutz erstellt wurden, dann hinterher geprüft und von den Verfahrensentwicklern entsprechend umgesetzt. Auch dort gehe ich davon aus - und nach jetziger Einschätzung ist das auch so - dass die Verfahren hochsicher sind, auch für längere Zeit. Wobei man an dieser Stelle viel schneller reagieren kann, weil das eben eine Anwendung in der Infrastruktur ist.

Vors. **Sebastian Edathy**: Vielen Dank, dann hat das Fragerecht für die SPD-Fraktion der Abg. Hofmann, bitte.

BE **Frank Hofmann (Volkach)**: Vielen Dank, Herr Vorsitzender. Ich würde gern Herrn Busch fragen zu der These von Herrn Pfitzmann. Ich habe das so verstanden, dass hier eine Verbreitung der Fingerabdrücke befürchtet wird. Und mich interessiert dann, wie ist es, wenn diese Fingerabdrücke so verbreitet sind, können die in die RFID-Chips eingelesen werden? Kann man sich so etwas vorstellen, oder können die auch unberechtigt ausgelesen werden? Ist so etwas vorstellbar und in der Praxis auch möglich? Im zweiten Bereich würde ich Ihre These kurz aufgreifen. Sie sprachen davon, dass die Haltbarkeit der Chips möglicherweise von 10 Jahren nicht gewährleistet ist. Deshalb wollte ich noch einmal in die Sachverständigenrunde fragen, ob andere Sachverständige auch dazu etwa Informationen beitragen könnten, wie es mit dieser 10 Jahres-Frist ist? Und einen kurzen dritten Bereich noch an Herrn Ziercke. Zu der Frage der Online-Speicherung von Fingerabdrücken und einem möglichen Abgleich mit BKA gespeicherten Fingerabdrücken. Für mich ist da die erste Frage: Die beim BKA gespeicherten Fingerabdrücke haben Speicherfristen, glaube ich. Die sonst Gespeicherten beim Einwohnermeldeamt hätten keine. Die Frage ist, ob man nicht im § 81b der Strafprozessordnung schon so weitgehend Möglichkeiten hat, Fingerabdrücke im Strafprozess und auch für die Gefahrenabwehr zu holen, dass das andere eigentlich nicht mehr notwendig ist. Und zum Dritten natürlich, was auch dabei eine Rolle spielt. Wir haben hier nur ein Bild vorliegen, während das BKA alles „verformelt“. Es müsste ja auch erst wieder gängig gemacht werden, das könnte ich mir schlecht vorstellen und zudem glaube ich, brauche ich den Online-Abruf nicht für Vermisste oder unbekannte

Tote und auch weniger für Verkehrsordnungswidrigkeiten. Ich glaube, wenn, dann würde man das auf andere oder schwerere Formen von Kriminalität begrenzen.

Vors**. Sebastian Edathy**: Dann bitte ich um die Beantwortung, zunächst den Sachverständigen, Herrn Prof. Busch.

SV **Prof. Dr. Christoph Busch**: Sie haben zwei Fragen an mich gestellt. Die erste Frage bezüglich der Fingerabdrücke; die Teilfrage dazu, ob sie aus dem Pass ausgelesen werden können: Ich denke, das ist durch die Äußerung von Herrn Schabhüser, aus meiner Sicht hinreichend beantwortet worden. Das ist eine Frage der kryptographischen Stärke der eingesetzten Protokolle, da gibt es für mich keinen Grund, dem BSI dort als Experteninstitution zu widersprechen. Das Hineinkopieren - so habe ich Sie verstanden - in den Pass ist durch die digitale Signatur, die über diese Datengruppe angebracht wird, ausgeschlossen. D.h. selbst wenn man „klonen“ kann - ich persönlich kann es nicht - und seine Daten dort hineinkopieren könnte, würde es bei der Prüfung des Dokumentes mittels der Signatur detektiert werden. Der Aspekt, den Herr Pfitzmann eingeworfen hat, ist, dass durch die Verbreitung der biometrischen Pässe mit Fingerabdrücken ein Gewohnheitseffekt bei der Bevölkerung eintritt. Das sehe ich auch so, aber ich sehe die Dramatik in dieser Gewohnheit nicht, sondern ganz im Gegenteil. Ich denke, durch diese Pilotanwendung wäre für andere - aus meiner Sicht positiv belegte - Zutrittskontrollen die Biometrie ein eingeführtes und gewohntes Verfahren. Zu der Frage, wo ich meine Fingerabdrücke hinterlasse: Da dürfen wir uns nicht täuschen. Die Fingerabdrücke als biometrische Samples, ob sie in analoger oder digitaler Form vorliegen, sind so genannte „flüchtige biometrische Daten“. Ich habe sie bereits auf einem Glas hinterlassen, auf vielen CD-Hüllen, an Türklinken etc.. Wenn man möchte, kann man an meine Fingerabdrücke gelangen. Wenn man diesen Punkt kontrollieren möchte, dann muss man darüber nachdenken, ob man für höhere Sicherheitsansprüche nicht-flüchtige Verfahren einsetzt, sagen wir für die Zugangskontrolle zu Hochsicherheitsbereichen, Kernkraftwerken usw., die 3D-Gesichtserkennung, Fingervenenerkennung und dergleichen mehr. Zur Haltbarkeit: Diesen Punkt habe ich aus zwei Gründen aufgenommen. Zum einen, weil ich überzeugt bin, dass die biometrische Leistungserkennung (….)
Zwischenrufe (nicht rekonstruierbar)

SV **Prof. Dr. Christoph Busch**: (…) flüchtige Daten, also, wenn Sie den Fingerabdruck betrachten, den ich jetzt hier hinterlassen habe. Er ist flüchtig, denn ich habe eine analoge Repräsentation meiner Papillarleisten auf diesem Glas hinterlassen. Das Bild kann man abnehmen. Bei der Tatortanalyse wird man genau dieses tun. Es gibt andererseits eine biometrische Charakteristik, die können wir bspw. Gesichtsgeometrie nennen. Das ist die Form meines Gesichtes. Anders als das 2D-Gesichtsbild ist es sehr schwer, ohne meine Kooperation ein 3D-Modell meines Gesichtes zu bekommen. Auch das Fingervenenbild ist nur sehr schwer zu erlangen, ohne dass ich dabei beteiligt bin, weil ich das Fingervenenbild nicht an einem Glas hinterlasse. Beantwortet das die Frage? Gut. Zu der Haltbarkeit: Punkt eins ist, dass wir noch keine Aussage darüber

machen können, wie leistungsfähig die heutigen Algorithmen mit Referenzdaten sind, bei denen die 2D-Gesichtsbilder 10 Jahre alt sind. Bei den Fingerbildern gibt es Aussagen dazu, das ist nicht das Problem. Ich gehe davon aus, dass die Außengrenze mit beiden biometrischen Modalitäten ausgebildet sein sollte. Insofern wird für die Verifikation aufgrund eines 10 Jahre alten Gesichtsbildes ggf. ein Problem entstehen. Das ist auch heute so, wenn wir einen alten Pass analysieren, da ändert sich nichts. Der zweite Aspekt, das ist einfach eine persönliche Erfahrung. Ich habe seit 10 Jahren eine RFID-Zugangskontrollkarte zum Fraunhofer Institut in Darmstadt. Das ist diese Karte hier, und die trage ich täglich mit mir, denn ich möchte ja Zugang haben. Es ist mindestens die dritte Karte, die ich bekommen habe, weil die anderen einfach die Funktion nicht mehr erfüllen konnten. Ich denke, dass das BMI dazu mit den Chip-Lieferanten entsprechende Gespräche geführt hat, dass man da vermutlich auch über Garantieleistungen gesprochen hat. Eine Haltbarkeit von 10 Jahren widerspricht meiner persönlichen Erfahrung. Jetzt kann ich sagen, das ist natürlich eine mindere Qualität und wir werden in den Pässen höhere Qualität haben. Beantwortet das die Frage?

Vors. **Sebastian Edathy**: Gibt es weitere Sachverständige, die sich hier - bevor Herr Ziercke das Wort bekommt - zum Thema „Haltbarkeit des Chips“ äußern möchten? Herr Grunwald, bitte.

SV **Lukas Grunwald**: Wir haben bei uns im Labor gewisse Tests durchgeführt und die Tatsache, dass die RFID-Chips, die in den Pässen eingesetzt sind, teilweise gebondet sind, d.h. es ist eine kleine Wicklung aus Kupfer, die auf dem Chip aufgebracht ist, und diese Stellen haben sich nicht gerade sehr persistent erwiesen. Wir würden davon ausgehen, dass eine Haltbarkeit nicht länger als 4 bis 5 Jahre gegeben ist, aufgrund allein der mechanischen Belastung, wenn man sieht, wie wir teilweise mit unseren Pässen umgehen. Der wird in der Handtasche transportiert, der wird regelmäßig öfter ein bisschen gewalkt. Das Ding wird auf den Lesegeräten von den entsprechend kontrollierenden Beamten so aufgedrückt, dass man entsprechend die Sachen abnehmen kann. Gehen wir nicht davon aus, dass die Chips 10 Jahre halten werden.

Vors. **Sebastian Edathy**: Dazu weitere Wortmeldungen? Das ist nicht der Fall, dann hat Herr Ziercke das Wort, bitte.

SV **Jörg Ziercke**: Der Abg. Hofmann hat gefragt, was die Online-Speicherung (gemeint: Online-Abfrage) von Fingerabdrücken im Verhältnis zum AFIS-System, zum Fingerabdrucksystem des BKA betrifft. Ich habe grundsätzlich schon gesagt, beim biometrischen Ausweis sind es nur zwei Finger, die Zeigefinger. Und wir haben im BKA-AFIS eine Datei, in der sich alle zehn Finger befinden und in der Regel die Handflächen. Das zeigt schon die Begrenzung bei entsprechenden Recherchen. Die Speicherfristen, die Sie angesprochen haben, gelten für Fingerabdrücke, ähnlich wie für Kriminalakten, die angelegt werden bei den Länderpolizeien und auch beim BKA. D.h., es muss eine Prognose da sein, dass jemand wahrscheinlich wieder in Erscheinung

treten wird, diese muss begründet sein. Nur dann darf eine Speicherung erfolgen. Wenn das nicht der Fall ist, greifen Aussonderungsfristen und dann würden die Daten im BKA gelöscht werden. Im Vergleich dazu blieben diese Daten, der Zeigefinger, langfristig, wenn nicht auf Dauer erhalten. Wenn sie nicht vergleichbar sind mit dem BKA-Bestand, dann sind sie es eben nicht. Das erleben wir heute bei vielen Datenabgleichen, dass es durchaus sein kann, dass in dem einen oder anderen Fall vor ein oder zwei Jahren die Spur gelöscht worden ist, und dann beginnt man im Grunde mit der Arbeit von vorne, aber das ist das Wesen von Aussonderungsfristen. Das soll auch so sein. Im Hinblick auf Recherchen - hatte ich auch gesagt - bei dezentraler Speicherung muss es sich um recherchierbare Systeme handeln. Ob das bezahlbar ist, weiß ich nicht. Das ist eine Dimension, die wir auch im BKA beim AFIS-System haben, das muss man sich sehr genau ansehen.(….)
Zwischenrufe (nicht rekonstruierbar)
SV **Jörg Ziercke**: (….) Nein, es müsste eine Verformelung da sein. Das Bild wird ja bei uns auch umgesetzt in eine Formel. Aus diesem Grund heraus muss eine Verformelung stattfinden. Deshalb spreche ich auch ganz bewusst vom AFIS-System. Eine solche Software müsste dann schon vorhanden sein. Ansonsten, nur was Vermisste angeht, Verkehrsordnungswidrigkeiten, da habe ich nicht von Fingerabdrücken gesprochen, sondern nur von den Lichtbildern.

Vors. **Sebastian Edathy**: Vielen Dank für die Beantwortung der Fragen. Dann hat für die Fraktion DIE LINKE. der Kollege Jan Korte das Wort.

BE **Jan Korte**: Vielen Dank, Herr Vorsitzender. Ich habe zuerst an Herrn Ziercke eine Nachfrage, die sich aus Ihrer Stellungnahme ergibt. Mich würde dann doch noch mal ein bisschen konkreter interessieren, welche Art von Missbrauch es eigentlich in Passangelegenheiten gibt, was Sie schon vorgetragen haben. Das hörte sich nun nach den Zahlen, die Sie vorgetragen haben, so an, als ob fast die Hälfte der Bürger der Europäischen Union nur damit beschäftigt ist, Pässe zu fälschen und zu verschieben. Was genau ist darunter zu verstehen, auch die Dokumente, die zur Fahndung ausgeschrieben sind. Das würde ich noch mal etwas genauer von Ihnen wissen. An Herrn Hilbrans hätte ich noch mal die Frage, ob Sie noch mal genau darstellen könnten, auch vor allem aus datenschutzrechtlichen Gesichtspunkten, was jetzt eigentlich die Neuerung ist und der qualitative Unterschied zwischen einem Online-Abruf und dem bis dato gültigen Foto-Abruf bzw. Fotovergleich. Und auch wie das politisch einzuordnen ist, denn wir diskutieren hier natürlich nicht im luftleeren Raum, sondern wir diskutieren heute auch diese Frage im Zusammenhang mit immer weiterer Verschärfung von Sicherheitsgesetzen und natürlich auch mit Stellungnahmen von Schäuble und anderen, die auch in diesem Gesamtkontext reinpassen. Das würde ich gerne wissen. Die zweite an Herrn Hilbrans: Was glauben Sie, wenn jetzt dieses Gesetz so umgesetzt würde, was weckt das insbesondere bei den Diensten, bei den Polizeibehörden möglicherweise für weitgehende Sehnsüchte, die auf jeden Fall vorhanden sind, und leider auch meistens dann gesetzgeberisch umgesetzt werden. Wo sehen Sie dort die Missbrauchsgefahr und was könnte der nächste Schritt sein?

Vors. **Sebastian Edathy**: Dann zur Beantwortung bitte Herr Hilbrans und dann Herr Ziercke.

SV **Sönke Hilbrans**: Vielen Dank, Herr Vorsitzender. Zunächst zum qualitativen Unterschied noch einmal von Online-Abruf einerseits und der bisher standardmäßig erfolgenden Einzelfallabfrage, die die ersuchte Stelle dann dazu benötigt, die Daten in einem geeigneten Format weiterzureichen. Der Online-Abruf ist 24 Stunden am Tag im Idealfall möglich. Es treten aber in der Regel dadurch nur geringe Zeitgewinne ein. Der Online-Abruf erfolgt zudem unter absoluter Ausschaltung der datenbesitzenden Stellen. Es ist ausschließlich die an den Daten interessierte Stelle, welche die Kontrolle über den Online-Abruf hat. Das ist zwar, gemessen am Bundesdatenschutzgesetz, ein Ausnahmefall. Es ist im Passgesetz allerdings - weil die rechtliche Herrschaft über den Abruf von Passdaten auch heute schon weitgehend bei den Sicherheitsbehörden liegt - nicht so ganz ungewöhnlich. Mit dem Online-Abruf - der Bundesdatenschutzbeauftragte hat es schon gesagt - ist es perspektivisch möglich, so etwas wie eine virtuelle Zentraldatei zu schaffen. Es gibt eine vierstellige Zahl von Passbehörden in Deutschland, die mehr schlecht als recht elektronisch ausgestattet sind. Wenn der Online-Abruf flächendeckend möglich ist, da bedarf es nicht viel, z.B. der ebenfalls onlineabruffähigen Melderegister, um ohne Weiteres, fast wie in einer bundesweiten Zentraldatei, gezielt an die Daten aus den Passregistern heranzukommen. Dabei reden wir nach der gegenwärtigen Fassung des Gesetzentwurfs eigentlich nur über das Lichtbild. Aber Sie fragen ja auch nach den Begehrlichkeiten, die das wecken kann. Die können Sie im Prinzip schon der Stellungnahme des Bundesrates entnehmen. Das sind vielleicht nicht die allerersten Schritte, aber das ist doch ein wesentlicher Teil dessen, was auf uns zukommen kann, wenn es denn dem Bundesrat und wenn es der Bundesregierung gefällt. Das ganze hat ein das aktuelle Gesetzgebungsvorhaben übergreifendes Gewicht. Wir mussten uns schon in der Vergangenheit daran gewöhnen, dass die immer stärkere Technisierung und Elektronisierung - sowohl der Behördenkommunikationen als auch der Ermittlungen als solche - und auch der immer weiter gehende Zugriff der Sicherheitsbehörden auch auf private, und andere nicht-polizeiliche Datenbestände zu einer Zunahme von Vernetzungen geführt hat und zu der Einführung von immer mächtigeren Werkzeugen bei der Ermittlung. Mithin dazu, dass ganz alltägliche Datenspuren in immer größerem Umfang zum Nachvollziehen von Verhalten zunächst im Verdachtsfall, perspektivisch aber auch zur Kontrolle und Überwachung, Anwendung finden können. Wenn Sie eine datenschutzpolitische Einschätzung dieser Tendenz und des Gesetzentwurfs wünschen, dann ist der Gesetzentwurf einmal mehr nicht der definitive Schritt in den bürgerrechtlichen Umgang. Aber er ist einer von vielen kleinen Schritten hin zu einer Gesellschaft, die sich ein Sicherheitsrecht leistet, das ganz alltägliche Spuren und Verhaltensweisen des täglichen Lebens über lange Zeit verfügbar macht für sicherheitsbehördliche Zwecke. Das ist, wenn man so will, der Einstieg in die Vorratsdatenspeicherung ohne vorher bestimmte Zwecke. Natürlich hat auch das Passregister einen ganz spezifischen, einen ganz konkreten Zweck. Dieser Zweck mündet heute nach dem Passgesetz bspw. in die

Frage: Ist ein Reisepass an eine bestimmte Person ausgestellt worden und was sind da für Daten drauf und welche Qualität haben die Daten? Und wenn ein Pass gefunden wird, was macht man damit? Und ist er überhaupt authentisch oder ist es eine Fälschung? Dazu gibt es das Passregister. Wenn Sie aber einen Online-Abruf auf alle Passregisterdaten etablieren, wie das bspw. auch schon in der Stellungnahme des Bundesrates gefordert wird, wenn Sie also das Passregister zur Verfolgung von Straftaten ganz allgemein freischalten wollen, dann haben wir einen ganz anderen Charakter des Passregisters, nämlich den einer von vielen Sicherheitsdatenbanken, die aus sicherheitsrechtsfremden Datenbeständen eine Sicherheitsdatenbank machen. Diese politische Entwicklung, die andere Kollegen mit „Salamitaktik“ beschreiben, ist datenschutzpolitisch aufs Schärfste zurückzuweisen.

Vors. **Sebastian Edathy**: Dann bitte Herr Ziercke.

SV **Jörg Ziercke**: Vielleicht zunächst eine Vorbemerkung. Es geht darum, dass bei diesem Thema - wie ich das auch von den Zahlen her aufgezeigt habe - wir es mit einem internationalen Phänomen zu tun haben, wenn es um Dokumentenfälschung, um Verfälschungen, um Totalfälschung geht und fälschlich ausgestellte Ausweispapiere, um Missbrauchsfälle. Auch mittelbare Falschbeurkundung kann hier eine Rolle spielen und in Einzelfällen gibt es Phantasiedokumente. Ich habe hier eine grenzpolizeiliche Gesamtstatistik der Bundespolizei 2005, aufgelistet nach Grenzen, Stand März 2006. Ich lese Ihnen beispielhaft einiges vor. So haben wir an der Grenze zu Polen 743 Verfälschungen festgestellt, 570 Totalfälschungen, fälschlich ausgestellte 29, Missbrauch 103. Zur Schweiz 185 Verfälschungen, 264 Totalfälschungen, Missbrauch 104. Flughäfen 1.018 Verfälschungen, 618 Totalfälschungen, Missbrauch 215 usw.. Das sind die Differenzierungen. Und die Statistik soll, anders als das vorhin in einer Äußerung hier zum Ausdruck kam, im Grunde nicht darauf hindeuten, dass wir demnächst dann bei den biometrischen Pässen genau diese Fallzahlen haben. Das wäre ja völlig widersinnig. Ich habe Ihnen durch diese Fallzahlen dargestellt, dass wir jetzt ein Problem mit den konventionellen Ausweisen haben. Und ich erwarte eine erhebliche Reduzierung, wenn die Biometrie eingeführt wird. Sie haben ja eben gehört was Fälschungssicherheit angeht, was insbesondere die Verhinderung von Missbrauch angeht. Dem gegenüber gibt es Hochrechnungen, die realistisch sind aufgrund der Situation in den Staaten, die noch nicht im Schengener Informationssystem enthalten sind. Sie wissen, dass es eine Ausgleichsmaßnahme für den Wegfall der Grenzkontrollen gibt. Aktuell haben wir bei 15 Schengenstaaten einschließlich Norwegen, Island und andere rd. 14,4 Mio. ausgestellte Dokumente in der Schengenfahndung und die Hochrechnung, wenn 15 weitere dazu kommen, liegt bei etwa 20 bis 25 Mio. Dokumenten. Das ergibt sich aus den Fallzahlen, die wir aus diesen Beitrittsländern jetzt schon kennen.

BE **Jan Korte**: Ich habe nur eine Nachfrage: Bezieht sich das denn auf deutsche Pässe die Zahlen, die Sie eben genannt haben, denn darum geht es hier ja.

SV **Jörg Ziercke**: Ich habe Ihnen doch dargestellt, dass wir es in Deutschland mit einem internationalen, mit einem globalen Phänomen der grenzüberschreitenden Terrorismusbekämpfung und der Organisierten Kriminalität zu tun haben. Ich kann Ihnen auch die Zahlen für Deutschland natürlich nennen - wenn ich sie hier so schnell finde - dann haben wir Inlandsfeststellungen: 228 Verfälschungen, Totalfälschungen 213, fälschlich ausgestellte 56. Das ist jetzt aber nur das Jahr 2004, in das ich gerade hineingegriffen habe. Nur, das bringt mir letztlich in der Erkenntnis nicht viel, weil wir eben ein Land sind, durch das Millionen von Touristen reisen, in das Menschen kommen, die hier zur Arbeit kommen, aber eben auch um kriminelle Handlungen zu begehen. Deshalb ist es für die Grenzkontrollbehörden völlig unerheblich, ob das der Ausweis eines Österreichers, eines Schweizers oder eines Deutschen ist. Es geht hier - und das zeigen auch die Beschlüsse auf EU-Ebene, die Beschlüsse der Vereinten Nationen sogar - es geht um ein Phänomen, das insgesamt - und das ist meine Position jetzt - zur Kriminalitätsbekämpfung einen Beitrag leisten soll.

Vors. **Sebastian Edathy**: Vielen Dank. Dann hat jetzt für die Fraktion BÜNDNIS 90/DIE GRÜNEN das Wort der Kollegen Wolfgang Wieland.

BE **Wolfgang Wieland**: Ich habe eine Frage an Herrn Ziercke und will es noch mal versuchen und hoffe, Sie haben noch die Geduld, evtl. zu verstehen, worauf der Kollege Korte und auch ich hinauswollen. Herr Hilbrans sprach vom deutschen Pass als einem Spitzenprodukt. So ist er uns auch seinerzeit mal geschildert, ich will nicht sagen, „verkauft“ worden, nämlich fälschungssicher und maschinenlesbar. Wir erinnern uns, dass es vorher durchaus noch üblich war, dass terroristische Kreise ihre Papiere mit Jupiterlampe selber fälschten. Das es eine Reihe von Prozessen gegen Ausweisgebern gab, die als Unterstützer verurteilt wurden, weil sie ihre Ausweise zur Verfügung gestellt hatten und terroristischen Tätern, die damit unterwegs waren. Die Frage, die Ihnen auch schon gestellt worden war, Herr Ziercke: Gibt es denn so etwas heute auch? Gibt es auch nur einen verfälschten Bundespersonalausweis? Nur dann gäbe es auch einen Sinn, ihn zu verbessern. Angeblich zu verbessern mit biometrischen Maßnahmen, von denen ich hier nun hören muss, dass sie so gefährlich sind, dass ich mir gleich so ein Container um den Pass am besten mache, und die Haltbarkeit 5 Jahre ist. Die Frage ist: Wird denn irgend etwas besser und sicherer oder wird durch diese Maßnahme nicht nur eine Risikomaximierung hier erteilt? Also, ist unser Pass ein Spitzenprodukt oder wird er fortlaufend gefälscht? Was macht es denn für einen Sinn, dass der Bundesbürger nun einen biometrischen Pass hat, und die die einreisen und sei es der Schweizer, der ihn nicht hat, und der US-Amerikaner auch nicht, und die die möglicherweise aus kritischen Staaten einreisen, erst recht nicht. Hier werden im Grunde die EU-Bürgerinnen und Bürger, die in dem Zusammenhang gar nicht die auffälligsten sind, zu einer Maßnahme verpflichtet und bei denen man es möglicherweise gerne hätte, lassen sich dadurch natürlich nicht verpflichten. Mit der dann noch geschilderten absurden Konsequenz „Insellösung“ - das ist also noch nicht mal das, was Otto Schily uns immer sagte - brauchen wir diese beiden Fingerabdrücke, um in Zukunft in die USA zu reisen. Nun höre ich hier, was ich bisher nur vom Schreibmaschinenschreiben kannte. Es gibt

ein Zwei-Finger- und ein Zehn-Fingersystem, und die USA wollen jetzt ein Zehn-Finger-System. Also, klipp und klar gefragt: Gibt es eigentlich überhaupt Probleme mit den bundesdeutschen Ausweispapieren? Das eine Menge verloren geht und das eine Menge geklaut wird, das ist jetzt so - ist mir vor Weihnachten auch passiert, man wollte offenbar mein Geld, und hat mir jede Menge Plastikkarten bei der Gelegenheit mit geklaut - doch das hört doch in Zukunft nicht auf. Dann haben Sie hier die biometrischen Pässe in der Zahl mit drin. Was soll das eigentlich beweisen? Zweite Frage an Herrn Pfitzmann und auch an Herrn Schabhüser. Dieses zur Verfügung stellen an Drittstaaten, das ganze hat doch nur einen Sinn, wenn der Pass dort gelesen wird, wo ich mit ihm einreise. Immer nur mich dann hier wieder zu kontrollieren, wenn ich zurückkomme von der Reise, - denke ich - trägt das ganze nicht. D.h. im System ist angelegt, dass an sehr viele Drittstaaten die entsprechende Möglichkeit, das zu lesen - das ist ja zunächst ein legales Lesen - zur Verfügung gestellt wird. Ist es denn irgendwie kontrollierbar, ob diese Staaten dann möglicherweise auch andere Informationen rausziehen, die dort in diesem Chip sind, und ist irgendwie kontrollierbar, ob und wie diese Staaten die Merkmale, Daten weitergeben bzw. - das ist ja auch geplant von der Bundesregierung - hieraus so etwas wie einen Exportartikel zu machen, im Rahmen dieser Hightec-Strategie. Ein früherer Bundesinnenminister hat das ja auch als Lebensaufgabe, das nun globalisiert zu vertreiben. D.h., wenn er so erfolgreich ist wie bisher, natürlich zu verkaufen, er verschenkt es nicht, das ist auch völlig legitim, dass er beim Verkauf hilft, aber Endpunkt wird doch dann immer sein, dass sehr umfassend diese Lesemöglichkeiten bestehen auch in so genannten Schurkenstaaten, auch in Diktaturen oder wo auch immer. Gibt es irgendwelche erkennbaren Sicherungsmechanismen, dass ich in Zukunft sicher sein kann, dass ein Staat, in den ich möglicherweise aus politischen Gründen - oder wie auch immer - einreise, keine Missbrauchsmöglichkeit für diese Daten hat.

Vors. **Sebastian Edathy**: Angesprochen sind Prof. Pfitzmann, Dr. Schabhüser und Herr Ziercke. Zunächst Herr Pfitzmann, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Schauen wir mal kurz in die Präsentationen, in den Teil, den ich Ihnen aus Zeitgründen nicht präsentieren konnte. Zunächst mal muss man zu der Extended Access Control sagen, dass die dann wirksam ist, wenn es so etwas gibt wie einen Weltstaat, in dem sich alle Leute an alle Regeln halten. Das wäre jetzt der Punkt 3. Wenn wir die PKI, diese Public Key Infrastruktur, auf der die Extended Access Control basiert, überall haben, es kein „Klonen“ von Lesegeräten gibt und keine „Schurkenstaaten“, dann ist das Problem gelöst. Aber ich denke, wenn Sie keine „Schurkenstaaten“ mehr haben, dann haben Sie viele Probleme gleich mal gelöst. Man muss dazu sagen, um Ihre Frage noch genauer zu beantworten, gibt es irgendwelche Sicherheitsmechanismen, die an der Stelle überhaupt schützen können? Geht das prinzipiell überhaupt? Und die Antwort lautet: nein. Es geht nicht, ganz egal wie sich das BSI Mühe gibt, denn Sie geben einem „Schurkenstaat“ Ihren Pass zum Lesen. Dort wird Ihr Name gelesen, Ihr Geburtsdatum, Ihr Bild, alles was da optisch erkennbar ist. Und selbstverständlich wird Ihnen ein „Schurkenstaat“ dort auch ein

Fingerabdrucklesegerät hinstellen und sagen: Bitte legen Sie auch Ihren Finger auf dieses Lesegerät. Ganz egal, ob wir dann den Datenabgleich mit dem Fingerabdruck im Pass machen können. Man wird im „Schurkenstaat“ - Schlagwort „Organisierte Kriminalität“, fremde Geheimdienste - selbstverständlich den Fingerabdruck bei Grenzübertritt erfassen. Und das zu vergleichen damit, dass Sie vielleicht in einem „Schurkenstaat“ ein Glas anfassen und dort auch Ihren Fingerabdruck hinterlassen, ist mit Verlaub gesagt, absolut lächerlich. Es ist ein riesiger Unterschied, ob etwas halbautomatisiert ist oder vollautomatisiert erfasst werden kann, massenhaft oder ob da im Einzelfall irgendein „Schlapphut“ jetzt schauen muss oder jemand von der Polizei, wer hat welches Glas angefasst, hoffentlich haben die Leute jetzt nicht die Namensschilder und die Gläser vertauscht. Diese Sachen zu vergleichen ist absolut weltfremd. Es geht an der Stelle ganz deutlich um eine neue Qualität.

Vors. **Sebastian Edathy**: Vielen Dank.

Zwischenrufe (nicht rekonstruierbar)
SV **Prof. Dr. Andreas Pfitzmann**: Dieser „Schurkenstaat“ hat jetzt bei jedem Grenzübertritt von Fremden einen weiteren Datensatz mit biometrischen Merkmalen, Fingerabdruck, Name, Geburtsdatum usw. Was er jetzt machen kann damit ist bspw., wenn er zusammenarbeitet mit Kriminellen hier, dass er die Datenbank, die im Ausland gewonnen wurde, selbstverständlich auch hier im Inland nutzt, um falsche Spuren zu legen. Und jetzt habe ich nicht gesagt, dass der Fingerabdruck das einzige Ermittlungsmerkmal wäre, das hat Herr Ziercke betont, habe ich aber nicht gesagt. Ich habe gesagt: Es ist ein Mittel, um zu ermitteln. Soweit ich polizeiliche Arbeit kenne, auch ein wichtiges Mittel. Und deswegen wird es an der Stelle die polizeiliche Ermittlung zunächst mal nicht stützen, sondern in die Irre leiten. Ich hoffe, dass mit dem entsprechenden Aufwand dann die Polizei aus diesem Irrweg nach gewisser Zeit wieder herausfindet. Aber dieses Ganze zu verkaufen, wir fangen auf die Art Kriminelle, wir steigern Sicherheit, ist einfach - Entschuldigung - abstrus.

Vors. **Sebastian Edathy**: Herr Binninger hat noch eine konkrete Nachfrage an den Sachverständigen.

BE **Clemens Binninger**: Nur eine kurze Zwischenfrage, Herr Pfitzmann. Mir leuchtet nicht ein, wenn Sie sagen, ein „Schurkenstaat“ wird alle Daten, die er aus dem biometrischen Pass gewinnen kann, vor allem den Fingerabdruck nehmen, um mit diesen Daten dann im Inland zu handeln, um falsche Spuren zu produzieren. Das könnte er doch einfacher haben. Da könnte er doch quasi 100 Einwohner seines eigenen Landes nehmen, von denen die Fingerabdrücke abnehmen und diese Fingerabdrücke dann nach Deutschland versenden oder verkaufen. Wozu, für all das, was Sie beschrieben haben, leuchtet mir nicht ein, wozu braucht er dazu den biometrischen Pass? All das, was an Missbrauch von Ihnen beschrieben wird, und was ich dem „Schurkenstaat“ nicht einmal abstreiten will, ist doch alles heute schon möglich.

Abnehmen des Fingerabdrucks, Registrierung der Personalien, was hat das mit dem biometrischen Pass zu tun?

SV **Prof. Dr. Andreas Pfitzmann**: Der Punkt ist: Mit dem biometrischen Pass hat es insoweit etwas zu tun, dass Grenzkontrollpunkte entstehen, wo Bürger damit rechnen, hier wird mir der Fingerabdruck abgenommen. Und ein Staat, der das tut, ist nicht einfach deswegen - weil er es tut - ein „Schurkenstaat". Das ist die große Änderung. D.h. also, diese Daten kommen selbstverständlich an alle Staaten, damit auch an „Schurkenstaaten". Der zweite Punkt ist: Selbstverständlich können Sie heute, wenn Sie meinen Fingerabdruck haben wolle, jetzt gucken, hier steht das Schild, hier steht das Glas, ich werde nachher gehen, ohne das Glas abzuwaschen. Wenn das ganze einen Wert haben soll für die Organisierte Kriminalität, dann doch nicht den Wert, irgendeinen Fingerabdruck am Tatort zu hinterlassen, sondern wenn ich eine Datenbank habe, wenn ich viele Datensätze habe, dann kann ich den Fingerabdruck desjenigen am Tatort lassen, der entweder kein Alibi hat, in der Nähe war oder fachlich irgendwo in der Nähe ist. D.h., je größer meine Auswahl wird - und durch die Computer unterstützt, wird die Erfassung drastisch größer - desto zielgerichteter kann ich die Polizei in die Irre führen und selbstverständlich gibt es für diese Sachen einen Markt. Es wäre naiv zu glauben, dass es da keinen Markt gibt.

Vors. **Sebastian Edathy**: Vielen Dank. Dann als nächster Sachverständiger zur Beantwortung der Fragen von Herrn Wieland, bitte Herr Schabhüser.

SV **Dr. Gerhard Schabhüser**: Vielleicht muss ich es noch ein bisschen zu Recht rücken an dieser Stelle. Natürlich, Herr Pfitzmann, Sie haben Recht, wenn ein „Schurkenstaat" Daten entgegennehmen will, auch andere Staaten, nicht nur „Schurkenstaaten", nehmen an der Grenze Fingerabdrücke. Das ist heute in den USA schon der Fall, man hinterlässt dort seine Fingerabdrücke und die können dann mit den Datenbanken machen was sie wollen. Das ist nicht in unserer Steuermöglichkeit. Durch die Einführung des Extended Access Control steht aber das Lesen aus den Daten des deutschen Passes unter der Kontrolle der ausstellenden Nation, also in diesem Fall unter der Kontrolle Deutschlands. Da muss es ein Abkommen geben irgendeiner Natur, die technischen Möglichkeiten sind geschaffen, wo dann vereinbart wird: Jawohl, du Land Nr. X darfst das Auslesen. Und das Auslesen soll technisch so geregelt werden, dass der Extended Access Control-Mechnismus immer noch hier in Deutschland ist und im Zweifelsfall, wenn Verdacht besteht, dass damit Unfug betrieben wird, abgeschaltet wird. So ist es technisch vorgesehen. Es ändert nichts daran, Herr Pfitzmann, natürlich, die USA nehmen auch so die Fingerabdrücke und haben die in einer Datenbank. Das ist durch dieses Thema nicht zu adressieren. Aber die Kontrolle der in EU-Pässen hinterlegten Fingerabdrücke bleibt eben bei der ausstellenden Nation. Und das ist technisch sichergestellt, soweit können wir da gehen.

Vors. **Sebastian Edathy**: Herr Ziercke, bitte.

SV **Jörg Ziercke**: Zunächst einmal, ich habe hier übrigens einen amerikanischen Pass. Wenn Interesse besteht, weil eben bestritten worden ist, dass die Amerikaner diesen Pass eingeführt haben. Was man unterscheiden muss, ob das nur Gesichtsbiometrie oder Fingerabdruckbiometrie ist. Da gibt es unterschiedliche Zeiten, wann das eingeführt werden soll. Zunächst einmal zu den Statistiken, die ich hier vorgetragen habe. Ich kann ja nichts für diese Zahlen, da werden Sie mir sicherlich Recht geben. Und ich habe auch deutlich gemacht, dass das ganze Thema aus der Sicht des BKA ein internationales, ein globales Thema ist. Ich kann heute Organisierte Kriminalität in Deutschland nicht ohne Blick über die Grenzen bekämpfen. Und ich sage Ihnen mal die Daten - weil das eben vielleicht etwas irrtümlich rübergekommen ist - wer eigentlich wann was macht. Das Einführungsdatum für den biometrischen Pass, Belgien: 2004, Thailand: 2005, Schweden: 2005, Norwegen: 2005, Australien: 2005, Neuseeland: 2005, Japan: 2006, so geht es der Reihe nach weiter. Ich habe hier insgesamt 20 EU-Staaten, 6 Staaten, die nicht zur EU gehören und 7 Staaten wie Thailand, Australien, Neuseeland, Japan, Singapur, USA und Hongkong, in denen der biometrische Pass eingeführt wird. Ich kann nur sagen, das sind für mich die entscheidenden Staaten, mit denen wir unmittelbar auch was die Bekämpfung des Terrorismus und der Organisierten Kriminalität angeht, Bezüge haben. In Deutschland selbst - ich habe hier noch mal die Zahlen überschlagen in den letzten 2½ Jahren - haben wir einen hohen Standard, das ist ja hier auch festgestellt worden, was den deutschen Pass angeht, was die Qualität angeht. Wir haben aber Verfälschungen. Wir haben über 100 Verfälschungen von deutschen Reisepässen und Ausweisen, was nur in Deutschland aufgefallen ist. Ich habe nicht die Zahlen der Auffälligkeit im Ausland, die müsste ich dann über Interpol in besonderer Weise erheben.

Vors. **Sebastian Edathy**: Frau Kollegin Stokar, Sie können sich gerne zu Wort melden, wir sind nämlich am Ende der Berichterstatterrunde, d.h., es besteht jetzt die Möglichkeit auch für weitere Kolleginnen und Kollegen Fragen zu stellen. Bereits gemeldet haben sich der Kollege Benneter und Herr Kollege Binninger und Frau Stokar und Herr Korte. Also, Herr Kollege Benneter, bitte.

Abg. **Klaus Uwe Benneter**: Ich habe eine Frage an Herrn Schaar. Herr Schaar, wir haben ja bisher schon im Passgesetz die Möglichkeit, dass Daten übermittelt werden können. Wenn ich das richtig sehe, steht im bisherigen Passgesetz, es ist ja keine Form vorgeschrieben bzw. auch keine Form ausgeschlossen, wie diese Daten übermittelt werden können. So ein Amtshilfeverfahren gibt es auch heute über diese Verkehrsordnungswidrigkeiten hinaus. Worin besteht Ihre Befürchtung, was jetzt die Datensicherheit angeht bei diesem Online-Verfahren? Das ist die eine Frage, die zweite Frage ist: Warum können die biometrischen Gesichtszüge nicht auch so wie die Fingerabdrücke, also in der gleichen verschärften Form, gespeichert werden, sondern - wenn ich Sie richtig verstanden habe - gibt es bei den biometrischen Gesichtszügen einen anderen Standard als bei den Fingerabdrücken. Warum wird da ein Unterschied gemacht, und wodurch ist der gerechtfertigt? Eine Frage noch an Herrn Ziercke: Ihre Zahlen zu den Fälschungen, die können doch eigentlich ein korrektes Bild erst dann

ergeben, wenn man weiß, wie viel Dokumente insgesamt geprüft wurden, und wie viel davon gefälscht waren. Also, wenn ich 700 Fälschungen festgestellt habe, und es sind mir 702 Pässe vorgelegt worden, dann ist das sicherlich was anderes, als wenn ich 700.000 vorgelegt bekommen und geprüft habe und dann eben nur 700 gefälscht waren. Das wäre es erst mal.

Vors. **Sebastian Edathy**: Bitte Herr Schaar und Herr Ziercke.

SV **Peter Schaar**: Zur ersten Frage, Herr Benneter: Die Datensicherheit bei Online-Verfahren wird deshalb ein Stück schwieriger herzustellen sein, weil ein Online-Verfahren die Öffnung der entsprechenden Datenbanken für Dritte voraussetzt, denn sonst kann man diese Daten natürlich nicht abrufen. Das bedeutet, dass eine Schnittstelle zu dem Datenbanksystem eingeführt werden muss, sonst können die Daten von der Polizei nicht aus den lokalen Passregistern abgerufen werden. Dieses ist ein Risiko deshalb, weil diese Schnittstelle ggf. auch von unberechtigten Dritten in Anspruch genommen werden kann. Das ist ein generelles Problem bei Online-Verfahren. Zum Thema der datenschutzrechtlichen Qualität hatte ich ja vorhin schon Stellung genommen, das will ich jetzt nicht wiederholen. Aber der Sicherheitsaspekt ist darin zu sehen, dass hier eine Öffnung eines Datenbestandes nach außen erforderlich ist, damit die berechtigten Dritten Daten abrufen können. Wenn sie das dann tun, dann werden diese Daten über ein Netz transportiert. Dieses Netz ist ein zusätzlicher Angriffspunkt für Hacker oder sonstige Personen, die sich für die Daten interessieren. Beides kann man absichern, das will ich hier nicht leugnen, aber es ist eine gewaltige Herausforderung, weil diese Pass- und Personalausweisregister, nach meinem Kenntnisstand, technisch nicht bundesweit standardisiert sind, so dass dann eine Vielzahl verschiedener Abrufmöglichkeiten mit unterschiedlichen technischen Spezifikationen eingerichtet werden müsste-, aber natürlich nach gemeinsamen Standards im Hinblick auf die Schnittstellen.
Der unterschiedliche Zugriffsschutz für Gesichtsbilder und für Fingerabdrücke wird damit begründet, dass das Gesichtsbild ohnehin in der optischen lesbaren Zone des Passes vorhanden ist und insofern weniger sensibel sei. Natürlich wäre es denkbar, auch hier einen verstärkten Schutz einzuführen. Dieser verstärkte Schutz hätte dann allerdings zur Konsequenz, dass nur noch sehr wenige ausländische Stellen diese Bilder lesen könnten. Der ICAO-Standard sieht im Übrigen auch vor, dass diese Basic Access Control für das Gesichtsbild anzuwenden ist und nicht diese Extended Access Control, so dass ein Pass, der mit einer Extended Access Control auch für die Gesichtsbilder versehen würde, nicht ICAO-konform wäre. Selbst wenn man als Datenschützer dafür eintreten würde, das Gesichtsbild genauso gut zu sichern wie den Fingerabdruck, würde eine solche Lösung auf praktische Probleme stoßen.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Ziercke, bitte.

SV **Jörg Ziercke**: Vielleicht noch zwei Vorbemerkungen, möglicherweise ist das noch nicht ganz klar geworden. Die Zahlen, die ich Ihnen genannt habe - gerade was die

Zahlen in Deutschland angeht, aber auch im Ausland - sind auf der einen Seite abhängig von den Kontrollen, das ist völlig klar. Und sie sind davon abhängig, dass man bei Kontrollen auch den Missbrauch erkennt. D.h., wir gehen davon aus, dass, was wir hier an Zahlenmaterial haben - auch abhängig von der Kontrollintensität - letztlich nur die „Spitze des Eisberges“ ist. Der Missbrauch wird eigentlich dadurch in besonderer Weise deutlich, wenn man einmal die Unterscheidung zur Verfälschung oder Totalfälschung nimmt. Dann ist der Missbrauch etwas, wo es um einen echten Pass geht. Der echte Pass wird nur durch eine andere Person - dieser Person gehört dieser Pass nicht - verwendet. Um diesen Missbrauch zu erkennen, dazu helfen biometrische Systeme, wie man sich vorstellen kann in erheblicher Weise, d.h., das ist der Zusammenhang zwischen dem was wir erkennen können und was wir nicht erkennen können. Darum unterscheide ich zwischen Verfälschung, zwischen Totalfälschung und zwischen Missbrauch. Die Anzahl der Kontrollen - um das noch mal auf den Punkt zu bringen - ist abhängig von der Kontrollintensität. Die liegt sicherlich in Größenordnungen, die erheblich über dem liegen, was wir wirklich festgestellt haben. Auch die Frage nach der Qualität der dann festgestellten Personen; was waren das für Personen, in welchen Netzwerken - Terrorismus, Organisierte Kriminalität - waren es Einbrecher, waren es Räuber, waren es Banden, die aus dem Ausland zu uns gekommen sind oder sind es Gefährder, die wir da festgestellt haben, können wir deswegen Reisewege feststellen, kann die beobachtende Fahndung dadurch unterstützt werden, sind es Leute, die zu Logistik, zur Rekrutierung, zur Vorbereitung nach Deutschland kommen oder die durch Deutschland durchreisen - all das kann man auch mit dem Missbrauch echter Ausweispapiere machen. Dieses zu erkennen, das ist für mich ein ganz wichtiger Aspekt der Biometrie in Ausweisen.

Vors. **Sebastian Edathy**: Vielen Dank, dann als nächster Kollege Binninger.

BE **Clemens Binninger**: Ich habe eine Frage an Herrn Ziercke noch mal und an Herrn Schabhüser, die ist zweigeteilt, mit zwei unterschiedlichen Aspekten. Sie bezieht sich aber auf die gleiche Bestimmung im Passgesetz, und zwar das Passregister. Im heutigen Passgesetz hat das Passregister auch im zukünftigen Jahr, weil wir es im Moment noch nicht ändern, aber diskutieren, die Funktion anhand der Daten, die bei der Passbehörde gespeichert sind, die Identität des Passinhabers und die Echtheit des Dokuments zweifelsfrei feststellen zu können. Jetzt diskutieren wir darüber, dass wir zumindest dezentral dann bei allen Passbehörden auch alle Daten, die im Pass sind konsequenterweise, wenn es um die Echtheitsüberprüfung geht, auch bei der Passbehörde speichern sollten. Es reicht, wenn ich hier eine ganze Reihe von Sorgen höre als Sachverständiger was das Thema „Klonen“, Haltbarkeit des Chips und was auch immer angeht. Deshalb die erste Frage: Wäre es von daher nicht zwingend geboten, nicht nur als Verwaltungsprinzip, sondern auch aus Gründen der Sicherheit für den Passinhaber, dass logischerweise im Passregister alle Daten, die im Pass vorhanden sind, auch bei der Passbehörde dezentral vorhanden sind. Zweiter Teil der Frage: Unterstellt, das wäre so und es geht um eine weitere Nutzung der Daten, so wie es heute beim Strafverfahren schon diskutiert wurde, will ich auf einen Fall abheben,

und da speziell Herrn Ziercke um eine Einschätzung bitten. Wenn wir heute bei einem schweren Verbrechen, einem Sexualmord, eine anonyme Täterspur am Tatort finden und diese anonyme Täterspur in der Datenbank des BKA nicht vorliegt, führt es immer wieder mal dazu - ich hatte so ein tragisches Ereignis selber bei mir im Wahlkreis, dass Massenspeichelproben genommen werden unter einer Zahl von ca. 1.000 Männern, im Alter zwischen 14 und 64 - wäre im gleichen Fall, eine dezentrale Speicherung bei der Passbehörde nicht nur hilfreich für die Aufklärung solcher Verbrechen, schon sogar der leichtere Eingriff, sozusagen als eben Massen-DNA-Tests durchzuführen.

Vors. **Sebastian Edathy**: Herr Dr. Schabhüser und Herr Ziercke, bitte.

SV **Dr. Gerhard Schabhüser**: Ich denke, für mich ist eher die erste Frage, Haltbarkeit des Chips oder Doppelung bzw. Redundanz. Eine Redundanz durch eine dezentrale Speicherung dürfte nicht zur Absicherung des Systems insgesamt zu bevorzugen sein. Natürlich, jede Redundanz ermöglicht im Nachgang zu kontrollieren, ob irgendetwas schiefgegangen ist oder nicht. Da kann man sich aber auch andere Wege vorstellen. Da sehe ich nicht die zwingende Notwendigkeit der Speicherung Es hilft, wenn man noch mal nachgucken kann. Das ist aber kein zentrales Element, weil der Prozess - wie Herr Schaar schon gesagt hat - ein verlässlicher ist, den wir heute so aufgestellt haben. Man kann es machen, man muss es an dieser Stelle nicht machen. Die andere Frage sehe ich eher kriminalistischer Natur.

Vors**. Sebastian Edathy**: Dazu dann bitte Herr Ziercke.

SV **Jörg Ziercke**: Das Beispiel, das Sie gewählt haben, kann natürlich so passieren, das ist klar. Voraussetzung ist dabei aber natürlich bei dezentraler Speicherung, dass es einen Bezug geben kann zwischen dem Tatort und den möglichen Passbehörden, d.h. im Umfeld. Ähnlich ist es bei Massenspeichelproben, bei DNA, dass man einen bestimmten Bereich, aus dem lt. Prognosen der Tatverdächtige kommen könnte, hat, um diese Massenspeichelproben durchzuführen. Auch da ist im Grunde logisch, dass die DNA im Vergleich zum Fingerabdruck - würde ich auf den ersten Blick einmal sagen - der stärkere Eingriff ist. Das kann durchaus so sein. Wenn man die Fingerabdrücke hätte - aber das wäre die Voraussetzung, dass man sie recherchierbar haben müsste, dann dezentral -, dann wäre das eine leichte Möglichkeit, wenn es eine solche Spur gibt bei einem solchen Tatort - wobei, noch einmal, es geht nur um zwei Finger, die möglicherweise noch vorhanden sein können, wahrscheinlich nur einer dann - da ist ein grundsätzliches Problem, das muss man auch sehen, da hätte man diese Möglichkeit. Gleichwohl es ist eine Möglichkeit, ob Sie tatsächlich realistisch ist in der Praxis, was Häufigkeit angeht, das müsste man sich noch genauer ansehen. Dies kann ich so auch nicht beantworten.

Vors. **Sebastian Edathy**: Frau Stokar, bitte.

Abg. **Silke Stokar von Neuforn**: Ich habe erst mal eine Frage an Herrn Schaar. Der Vertrag von Prüm, der berühmte, der regelt ja bisher die Weitergabe u.a. auch der Fingerabdruckdaten, soll aber erweitert oder überführt werden in europäisches Recht, d.h., es werden andere Staaten mit einbezogen, und es ist ja auch bekannt, dass zwar nicht der Vertrag von Prüm ausgedehnt werden soll auf die USA, aber die Inhalte dieses Vertrages. Meine Frage: Wenn der Polizei ein Online-Zugriff erlaubt wird auf Fingerabdrücke, die in Einwohnermeldedaten enthalten sind, wird das dann mit erfasst? Sie verlassen dann ja den Zuständigkeitsbereich der Kommunen und die Verfahrenshoheit, wie mit den Fingerabdrücken umgegangen wird, liegt dann ja im polizeilichen Ermessen. Also besteht rechtlich die Möglichkeit, dass alle Fingerabdrücke aller Bundesbürger dann ab dem 14. Lebensjahr europaweit und transatlantisch zur Verfügung gestellt werden. Das, was Herr Schäuble in letzter Zeit geäußert hat, lässt ja in die Richtung denken. Meine zweite Frage, die geht eher an Herrn Ziercke: Ich verstehe nicht, wenn der Fingerabdruck international von so großer Bedeutung ist, warum setzen Sie sich eigentlich nicht dafür ein, dass wir das auch in unsere Einreisebestimmungen aufnehmen. Für mich ist das eine Frage der Gerechtigkeit. Warum muss ich meine Fingerabdrücke im Pass haben, wenn ich in die USA reise. Sie mögen nur hier einen US-Pass zeigen, aber bisher ist es ja nicht so, dass die Bürgerinnen und Bürger der USA, die nach Europa oder nach Deutschland reisen, die gleichen Bedingungen haben, d.h. dann auch bitte schön, hier ihren Fingerabdruck hinterlassen müssen. Das ist für mich eine Frage der Gewichtung von Sicherheit aus dem Blickwinkel des BKA. Ich habe noch eine Frage, die sich auch an Herrn Ziercke richtet: Wenn wir denn zukünftig die absolut fälschungssicheren Reisepässe haben, wie lösen Sie eigentlich das Problem? Sie brauchen doch für Ihre verdeckten Ermittler und auch für die Geheimdienste gefälschte Reisepässe. Muss ich zukünftig damit rechnen, dass Sie Identitäten real existierender Bürgerinnen und Bürger nutzen, weil das anders technisch kaum noch möglich sein wird? Und letzte Frage: Wie sieht es mit der Reisefreiheit der Bürgerinnen und Bürger aus, die über keine lesbaren Fingerabdrücke verfügen, das sollen ja immerhin 3 % der Bevölkerung sein. Oder aber - das sind Zahlen, die wir aus Skandinavien kennen, nach dem dort das Asylverfahren die Fingerabdrücke eingeführt worden sind - also dort soll es bereits im ersten Jahr über 100 mutwillige Zerstörungen der eigenen Fingerkuppen gegeben haben, um nicht als Mehrfachasylbewerber erkannt zu werden. Auch mit diesem Phänomen müssen wir rechnen. Und ich habe eine letzte Frage an Herrn Ziercke: Wenn in diesen neuen Ausweisen zukünftig, selbstverständlich versehentlich, diese Funkantenne kaputtgehen soll, das soll ja schon durch einfaches Knicken und Knacken möglich sein, kommt das dann alles in die Statistik Ihrer Verfälschung von Ausweisen, und wie sehen Sie da die Beweislast?

Vors. **Sebastian Edathy**: Herr Schaar, bitte.

SV **Peter Schaar**: Zum Thema „Datentransfer“ nach dem Prümer Vertrag und ggf. Einbeziehung der USA: Der Prümer Vertrag, der in der Tat jetzt in europäisches Recht

überführt werden soll nach der Auffassung der deutschen Ratspräsidentschaft, bezieht sich auch auf die Fingerabdruckdaten. Allerdings nur auf die Fingerabdruckdaten aus polizeilichen Sammlungen, also erkennungsdienstlichen Sammlungen, und würde so, wie der Vertrag jetzt formuliert ist, jedenfalls nicht solche Fingerabdruckssammlungen umfassen, wie sie im Zusammenhang mit dem Passregister diskutiert werden. Außerdem gibt es eine Sicherung im Prümer Vertrag, d.h. es werden nicht die Identitätsdaten des Fingerabdruckinhabers übermittelt, sondern nur die Tatsache, dass der Fingerabdruck übereinstimmt, und dann muss man in einem normalen Rechtsverfahren nachfragen bei dem entsprechenden Staat, um wen es sich handelt. Im Anschluss daran wird die Identität entweder preisgegeben oder nicht. Gleichwohl kann ich hier nicht Entwarnung geben und zwar deshalb nicht, weil auch dieses „Hit/No-Hit-System“ ggf. durch umfangreiche Fingerabdrucksammlungen unterlaufen werden könnte. Stellen wir uns z.B. vor, die USA würden beteiligt an einem entsprechenden Vertragswerk, das muss dann nicht der Prümer Vertrag sein, sondern ein vergleichbares Instrument, wo auch nach dem „Hit/No-Hit-Verfahren“ Daten ausgetauscht würden. Da die USA von sämtlichen Personen, die in die USA einreisen, die Fingerabdruckdaten erheben, würden sie also diese Daten zur Identifizierung heranziehen können und könnten theoretisch dann abgleichen, wie viele dieser Personen in einer Fingerabdruckdatei der europäischen Staaten enthalten sind. D.h., man könnte das also praktisch durchaus koppeln, d.h. dann würde die USA aufgrund ihrer Einreisedaten, die sie über die Fluggesellschaften bekommen und bei der Einreise selbst erheben, diese Zuordnung vornehmen können und damit abfragen können, ob in europäischen Ländern diese Person in polizeilichen Sammlungen erfasst ist. Das könnte für die Risikoabschätzung der US-Behörden von erheblicher Bedeutung sein. D.h., obwohl man ein „Hit/No-Hit-Verfahren“ vereinbaren würde, hätte man faktisch die Übermittlung der personenbezogenen Daten, weil die US-Stellen ja wissen, wen sie da vor sich haben, so dass dieses Problem - glaube ich - falls man tatsächlich solchem Abkommen näher treten würde, sehr sorgfältig betrachtet werden müsste. Ich habe deshalb nicht den Eindruck, dass das „Hit/No-Hit-Verfahren“ in einem solchen Fall den erhofften Schutz gewährleisten würde. Gestatten Sie mir noch ganz kurz einen Hinweis auf das, was in US-Pässen gespeichert ist. Es gibt erste biometrische Pässe der USA, nur es gibt dort keine Pässe, in denen der Fingerabdruck gespeichert ist. Zweitens, es gibt keine Personalausweispflicht in den USA, und es gibt entsprechend auch keine Personalausweise. Es ist schwer vorstellbar, dass die US-Behörden in Zukunft von dieser Linie abweichen werden. Die Bush-Administration hat das mal angedacht, kurz nach dem 11. September, den Plan aber sehr schnell wieder fallenlassen, so dass letztlich der Fingerabdruck ein mehr oder minder europäisches biometrisches Merkmal ist, das für die Reisepässe verwendet wird. Herr Ziercke hat ja da Zahlen genannt. Er hat bestimmt genau die Zahl der Länder, in denen der Fingerabdruck außerhalb Europas benutzt wird. Vielleicht kann er mir da helfen, ich habe Thailand gehört, aber es waren wirklich nicht sehr viele Länder, die diesen Weg bisher gegangen sind. Ich glaube, ein, zwei arabische Staaten noch - das ist ein europäischer Alleingang, der hier gewählt wird, der insofern auch bei der Einreise nach Europa dazu führt, dass europäische Bürgerinnen und Bürger stärker kontrolliert werden als die amerikanischen

Bürger bspw., die nach Europa einreisen. Nun kann man natürlich sagen: Wir kennen ja den Reziprozitätsgrundsatz, wie er auch in Brasilien praktiziert wird zum großen Ärger der US-Behörden. Dort werden die Amerikaner dann entsprechend quasi erkennungsdienstlich behandelt. Ich als Datenschützer bin kein Fan einer solchen Verfahrensweise, kann es aber durchaus bei internationalen Beziehungen nachvollziehen, dass es auf nationaler Ebene manchmal zu solchen Forderungen kommt.

Vors. **Sebastian Edathy**: Vielen Dank, dann Herr Ziercke, bitte.

SV **Jörg Ziercke**: Ich hatte vier Fragenkomplexe. Einmal, was die internationale Bedeutung des Fingerabdrucks insgesamt angeht, das ist unbestritten in der Kriminalitätsbekämpfung, dass dies eine Säule ist. Die zweite Säule ist inzwischen die Speichelprobe. Das ist im Grunde die DNA-Spur geworden. Und für den Fingerabdruck spricht im Grunde, nachdem das Gesichtsbild durch die ICAO-Empfehlung auf europäischer Ebene eingeführt worden ist, dass eine hohe Praxistauglichkeit vorliegt, weil die dazu entwickelten Abnahme- und Erkennungssysteme im Grunde vorhanden sind. Und da man auf EU-Ebene der Meinung ist, dass dies eine hohe Verifikationssicherheit hat, wenn man zwei Merkmale hat, und dass man auch eine Flexibilität der Kontrolle hat, da wo es nicht so klar ist mit dem Gesichtsbild oder das Bild schon etwas älter ist, da hilft eben der Fingerabdruck im Vergleich. Insofern sind das ganz praktische Überlegungen. Die zweite Frage: Absolut fälschungssichere Reisepässe, Legende von verdeckten Ermittlern. Da bitte ich um Verständnis, aber das kann ich in öffentlicher Sitzung nicht machen. Da müssen wir uns noch mal gemeinsam verabreden, wenn Sie das wissen wollen. Das Dritte: Keine lesbaren Fingerabdrücke, 3 %, das weiß ich so nicht, aber es gibt da klare Regelungen, z.B., wenn das so sein sollte bei den Zeigefingern eben auf andere Finger auszuweichen. Das ist ganz genau bestimmt. Wenn es tatsächlich so sein sollte - den Fall kenne ich nun nicht -, dass ein Mensch gar keine Fingerabdrücke hat, dann würde ein Pass ausgestellt werden ohne Fingerabdrücke. Auch diese Regelung gibt es. Aber das ist absolut der Ausnahmefall. Was das „Knicken und Knacken“ angeht, da habe ich gerade gehört, das soll 10fach nach ISO-Normen getestet worden sein. Man soll 10.000 Biegungen wohl durchgeführt haben, man hat Klimatests gemacht, alles Mögliche. Die das von der technischen Seite zu verantworten haben, sind jedenfalls der Meinung, dass es relativ „knick- und knacksicher“ sein soll, relativ.

Vors. **Sebastian Edathy**: Herr Kollege Korte, bitte.

BE **Jan Korte**: Ich hätte an Herrn Ziercke zwei Fragen. Zum einen, in der „Süddeutschen“ vom 21. April 2007 hat der Herr Heribert Prantl, wie ich finde, in nachdenkenswerter Weise aufgezählt, was mit dem Ausländerzentralregister alles möglich ist und ob das nicht eigentlich das Vorbild ist für ein Bundesmelderegister und daraus den Schluss gezogen, inwieweit das jetzige Vorhaben - also dezentrale Pass- und Melderegister - nicht die Grundlage dafür sein könnten. Da würde ich gern von

Ihnen wissen, wie Sie das einschätzen. Zum Zweiten würde ich noch mal nachfragen: Sie haben eben in Ihrem vorhergehenden Beitrag von rd. 100 Verfälschungen von deutschen Pässen gesprochen, also was Ihnen an Erkenntnissen vorliegen. Können Sie vielleicht noch mal sagen, was das für Verfälschungen sind? Ist da einfach eine Ecke abgebrochen, oder sind es nachweisliche Verfälschungen, die dann für eine kriminelle Handlung benutzt werden? Eine dritte Frage an Herrn Schaar: Ich würde gern noch mal wissen, am Ende Ihrer Stellungnahme haben Sie davon gesprochen, dass es für die Politik vor allem nötig wäre, einmal eine wirkliche Evaluierung sämtlicher Neuerungen vorzunehmen. Das wäre wünschenswert. Ich würde von Ihnen gerne wissen, wie so etwas konkret aussehen könnte, damit man natürlich keine Evaluierung macht wie beim Terrorismusbekämpfungsgesetz, wo das Innenministerium sein eigenes Gesetz evaluiert und dann überraschenderweise herauskommt, dass das ganz gut ist. Wie könnte eine wirkliche unabhängige Evaluierung aussehen? Letzte Frage, vielleicht noch mal an die, die sich hier vor allem technisch geäußert haben, vielleicht an Herrn Pfitzmann und Herrn Schabhüser: Ganz konkret, wie stelle ich mir das vor, wenn ein Chip defekt ist, aus welchen Gründen auch immer, der Pass aber trotzdem noch gültig ist. Was ist denn dann?

Vors. **Sebastian Edathy**: Dann zunächst zur letzten Frage Herr Prof. Pfitzmann und Herr Dr. Schabhüser, bitte.

SV **Prof. Dr. Andreas Pfitzmann**: Wenn ein Chip kaputt ist, dann haben Sie einen Pass, der einfach unserem bisherigen Pass in der Funktionalität zum verwechseln ähnlich ist. Da steht Ihr Name, da steht Ihr Geburtsdatum, da ist das Bild, und das war es. Möglicherweise werden Sie dann bei der Grenzkontrolle etwas genauer ins Visier genommen. Sei es, dass der Staat, in den Sie einreisen wollen, vielleicht nicht weiß, ob das noch ein gültiger deutscher Pass ist. Es könnte sein, da bleiben Sie erst mal ein paar Stunden, bis das geklärt ist. Ich weiß es nicht. Ich hoffe, das ist gut abgesprochen. Und selbstverständlich könnte man sich auch fragen, mit dem Knicken und Knacken - also, es gibt vielleicht noch andere Methoden, um den Chip dazu zu kriegen, aufzugeben. Also, wenn die Bevölkerung nicht mitspielt, dann wird das, was Sie jetzt als die Ausnahme beschreiben, was, wenn die Techniker ordentlich gearbeitet haben, bei „good will“ der Bevölkerung auch die Ausnahme wäre, schnell der Regelfall werden. Und dann ist die Frage okay, was nützt es.

Vors. **Sebastian Edathy**: Herr Dr. Schabhüser, bitte.

SV **Dr. Gerhard Schabhüser**: Herr Pfitzmann hat das schon richtig dargestellt. Wenn ein Chip kaputt ist, ist der Pass immer noch ein gültiges Reisedokument, aber natürlich ist durch das Zeichen vorne auf dem Pass erkennbar, dass es sich um einen ePass handelt. Und das ist wie heute, wenn ein viermal in der Waschmaschine gewesener Pass an einer Grenzkontrolle ist, dann ist er etwas auffälliger als ein vollfunktionsfähiger Pass. Und das kann dann zu einer sorgfältigeren Inspektion führen.

Zwischenrufe (nicht rekonstruierbar)

SV **Dr. Gerhard Schabhüser**: (….) Wenn Sie den gewaschen haben, ja, das wissen Sie vorher, aber es kann ja auch ein Pass von allein kaputt gehen, und dann stehen Sie vor einer Grenze, und Sie werden als „Knicker, Knacker“ oder „Heimlichwäscher“ angesehen.

Vors. **Sebastian Edathy**: Es gibt eine Nachfrage von der Abg. Silke Stokar von Neuforn an Herrn Dr. Schabhüser.

Abg. **Silke Stokar von Neuforn**: Ich möchte jetzt eine ernsthafte Nachfrage stellen. Ich habe konkret eine Anfrage eines Geschäftsreisenden in die USA gehabt. Er hat mit seinem derzeitigen Chip im Reisepass - und zwar bemerkt er es nicht zu Hause - bei einer Reise in die USA folgende Situation gehabt: Der Grenzbeamte sagte ihm: Ihr Chip ist kaputt, damit kriegen Sie in Amerika Schwierigkeiten, lassen Sie sich sofort einen Ersatzpass ausstellen. Und der war dann noch teurer als der Ursprungspass. Meine Frage: Ihnen werden doch Zahlen vorliegen, wir haben doch schon einige Reisepässe mit Chips auf dem Markt, die auch schon genutzt werden. Wie viele von den Chips dieser superneuen Reisepässe sind denn schon durch „Kaputtsein“ aufgefallen? Die Zahlen würde ich gerne wissen. Wenn nicht mit „Knicken“ und „Knacken“ - das ist mir schon klar, da es sich um Daten handelt - dann kann man mit elektromagnetischen Verfahren - einige haben mir gesagt, die Mikrowelle reicht - ohne Waschmaschine - wie man das früher gemacht hat - durchaus eingreifen in die Funktionsfähigkeit dieses Chips. Und wenn der Chip sowieso nur nach Expertenmeinung nur 5 Jahre hält, oft kaputt geht, dann stellt sich doch die Frage, ob die Bürgerinnen und Bürger, wenn eine ganze Familie reisen will, wirklich bereit sind, ein paar hundert Euro alle 3, 4, 5 Jahre für Reisepässe für die Familie auszugeben. Das sind doch ganz konkrete Folgen, die mit diesem angeblich so sicheren Pass auf uns zukommen werden.

Vors. **Sebastian Edathy**: Herr Dr. Schabhüser.

SV **Dr. Gerhard Schabhüser**: Zu einem Punkt kann ich Stellung nehmen, zu den anderen wahrscheinlich nicht, weil das nicht mein Themenfeld ist. Zur Haltbarkeit des Chips habe ich eben nicht geantwortet. Herr Busch hat es dargestellt, seine Zutrittskontrollkarte von vor 10 Jahren ist ihm in der Vergangenheit dreimal kaputt gegangen. Das, was in den Pässen heute eingesetzt wird, da gibt es Verträge mit der Bundesdruckerei, Passproduzent heute. Ob er das ewig ist, wird sich dann zeigen. Dass die Haltbarkeit gewährleistet ist, ist, soweit ich weiß, von der Bundesdruckerei garantiert.

Zwischenrufe (nicht rekonstruierbar)

SV **Dr. Gerhard Schabhüser**: Jetzt kommt der nächste Punkt. Den Vertrag kenne ich nicht, den habe ich nicht gelesen, das ist BMI-Thema. Die nächste Frage, wie viel

wirklich kaputt gegangen sind und welche Szenarien da aufgetreten sind, da muss ich mich entschuldigen, ich bin als IT-Fachmann hier platziert und nicht als Grenzkontrollkandidat oder für diplomatische Verwicklungen. Sorry.

Vors. **Sebastian Edathy**: Also, zu dem was Frau Stokar von Neuforn wissen will, kann da einer der anderen Sachverständigen etwas dazu sagen? Das scheint nicht der Fall zu sein, dann bitte ich jetzt Herrn Schaar und Herrn Ziercke zu den weiteren Fragen des Kollegen Korte Stellung zu nehmen.

SV **Peter Schaar**: An mich ist die Frage gerichtet worden nach der Evaluation. Eine Vorabevaluation hat ja in diesem Bereich, zumindest durch den TAB-Bericht stattgefunden. Und es hat jetzt auch endlich eine Befassung hier gegeben. Allerdings hat man die Entscheidung auf europäischer Ebene im Wesentlichen ohne eine entsprechende Evaluation getroffen, so dass man da sicher in Zukunft manchen Fehler vermeiden könnte, indem man da vorab auch die entsprechenden Pro und Kontra intensiver diskutiert. Entscheidender ist sicherlich die Frage: Wie erfolgreich war denn eine entsprechende Maßnahme, wie jetzt z.B. die Einführung der biometrischen Pässe. Und dazu bedarf es dann eben auch einer periodischen Bewertung. Das kann man dadurch erreichen, indem man das Gesetz erst mal befristet und eine Evaluationsklausel in das Gesetz aufnimmt. Man kann auch unabhängig von einer Befristung eine solche Evaluationsklausel ins Gesetz schreiben. In einer solchen Evaluationsklausel sollte man - das zeigt die Erfahrung des Terrorismus-bekämpfungsgesetzes - doch etwas präzisere Angaben aufnehmen, wie denn die Evaluation vorzunehmen ist. Dazu gehört einmal die Festlegung der wesentlichen Kriterien, nach denen evaluiert wird. Dabei geht es dann nicht nur um ein bloßes Zahlenwerk, sondern auch um die Frage der Grundrechtsrelevanz von bestimmten Maßnahmen. Dann geht es um die Frage: Wer evaluiert? Da, denke ich, ist es sinnvoll, dass man hier auf eine unabhängige Evaluation setzt. In den USA bspw. - ich habe es vorhin beiläufig erwähnt - gibt es ein „Government Accounting Office“, das solche Evaluationen durchführt und durchaus nicht immer mit vorhersehbaren Ergebnissen für die US-Regierung, teilweise mit kritischen oder vernichtenden Urteilen über bestimmte Maßnahmen, z.B. zuletzt über das Einreiseregime der Vereinigten Staaten. Da ist ein sehr dicker Bericht vorgelegt worden, der doch viele sehr kritische Fragen nicht nur stellt, sondern auch beantwortet in der Weise, dass es doch teilweise ein ziemlich ungeeignetes Verfahren ist, das dort installiert wurde. Wenn man den Maßstab ‚höhere Sicherheit’ anlegt, dann gehört dazu auch die Frage, wie wird das ganze zurückgekoppelt ins parlamentarische Verfahren? Ich denke, hier muss es natürlich immer eine Verfahrensherrschaft des Parlaments geben, wenn es sich um eine Maßnahme handelt, die auf gesetzlicher Grundlage geregelt oder eingeführt wurde. Hier gibt es bestimmte Ansätze im Terrorismusbekämpfungsgesetz, die ich begrüße. Dies könnte man sicherlich aber noch ausbauen. Das wäre sicherlich der Weg, wie man zu einer verbesserten Kontrolle von getroffenen Maßnahmen gelangt. Ich meine aber auch, dass derjenige, der Grundrechte einschränkt, letztlich auch rechenschaftspflichtig ist. Dieser Rechenschaftspflicht muss sowohl im Vorfeld einer Entscheidung, als auch

im Nachhinein nachgekommen werden. Deshalb wäre eine generelle entsprechende Vorgehensweise sicherlich sehr hilfreich.

Vors. **Sebastian Edathy**: Herr Ziercke, bitte.

SV **Jörg Ziercke**: Die erste Frage zum Bundesmelderegister - so wie ich Sie verstanden habe. Mir ist nicht bekannt, dass die Bundesregierung derartiges anstrebt. Das BKA strebt nicht nach dieser Aufgabe, Punkt 1. Punkt 2: Zur Frage der Verfälschung, die Sie angesprochen haben, möchte ich noch mal vorausschicken: Ich habe Ihnen dargestellt, in welchen europäischen Staaten - die Übersicht steht hier auch zur Verfügung, wenn Sie das gerne wollen - wie jetzt der Weg des biometrischen Passes und Ausweispapiers gegangen wird vor dem Hintergrund der Bedeutung, die die Dokumentenkriminalität aus meiner Sicht auch in Europa hat; dies ist das eigentliche Problem. Und ich kann diese Frage - ich gehe gleich auf Ihre Frage näher ein - aber überhaupt nicht isoliert für Deutschland diskutieren, um das ganz deutlich zu sagen. Das macht nämlich auch keinen Sinn. Zu Ihrer Frage, was das für Fälle sind. Ich würde sie Ihnen gern beantworten, ich kann es Ihnen aber so nicht sagen. Sicher ist nur, es geht nicht um das Abschneiden zum Ungültigmachen eines Passes, um diesen dann in der Statistik als Verfälschung zu registrieren. Das ist mit Sicherheit nicht der Fall. Ihre Frage jetzt, Frau Abgeordnete, zur Haltbarkeit. Ich glaube, das ist noch zu früh. Bisher lesen die USA die Pässe aus. Ich habe hier eine Zahl, aber die ist letztlich nicht belastbar: Von den 3 Mio. in Deutschland ausgegebenen Pässen hat es in 33 Fällen Probleme gegeben. Die Belgier gehen davon aus, das kann bis zu einem Prozent vielleicht sein, so die Information, die ich im Moment habe von dieser Ebene.

Vors. **Sebastian Edathy**: Vielen Dank. Herr Kollege Hofmann.

BE **Frank Hofmann (Volkach)**: Eine kurze Nachfrage: Sie sprechen hier von Dokumenten. Was verstehen Sie denn unter Dokument im Sinne dieser Statistik? Das ist ja wohl wesentlich mehr als nur der ePass.

SV **Jörg Ziercke**: Das ist der Ausweis, es ist der Pass. Es gibt auch andere Dokumente, aber das habe ich hier differenziert in meinen Zahlen, diese Fälle habe ich hier nicht genannt. Es gibt darüber hinaus bei Visa Probleme, bei Aufenthaltstiteln, aber diese Zahlen habe ich hier gar nicht genannt. Ich habe, bezogen auf deutsche Dokumente, nur die Fälle genannt für Ausweispapiere und für Pässe, die Gesamtstatistik umfasst alle Dokumente und das im Zusammenhang mit Totalfälschung, Verfälschung und mit Missbrauch.

BE **Frank Hofmann (Volkach)**: Sie haben die Dokumente Personalausweis und Pass gemeint.

SV **Jörg Ziercke**: Die habe ich gemeint, und es gibt aber darüber hinaus eine ganze Anzahl anderer Verfälschungen, die sich insbesondere auf Visa beziehen. Ich habe von etwa 100 Passverfälschungen in den letzten 2 ½ Jahren gesprochen.

Vors. **Sebastian Edathy**: Es gibt eine weitere Wortmeldung des Kollegen Klaus Uwe Benneter.

Abg. **Klaus Uwe Benneter**: Herr Schaar, noch mal, das bisherige Passregister, da sagt die Kommentarliteratur dazu, dass die Zulässigkeitsvoraussetzung deshalb besonders streng sei bei der Datenübermittlung aus diesem Register auf Ersuchen anderer Behörden, weil eben das Passregister kein Auskunftsregister sei und deshalb für Datenübermittlungen nur in äußerst begrenztem Umfang zur Verfügung stehen soll. Dies sei ein gravierender Unterschied zum Melderegister, in welchem die gesetzlich festgelegten Daten erfasst und gespeichert werden machen Melderegister nach Maßgabe auch weitergegeben werden können. Zum einen: Worin liegt dieser offensichtlich ganz maßgebliche Unterschied zwischen Passregister und Melderegister? Und zum anderen habe ich Sie so verstanden, dass Sie die modernen Informations- und Kommunikationstechnologie hier nicht außen vor lassen wollen. Wo Sie Bedenken haben, ist das Online-Verfahren, d.h. der Direktzugriff der ersuchenden Behörde ohne Einschaltung der bereitstellenden Behörde.

Vors. **Sebastian Edathy**: Herr Schaar, bitte.

SV **Peter Schaar**: Sie haben völlig zu Recht auf diese unterschiedlichen Aufgaben der verschiedenen Register hingewiesen. Diese Aufgaben sind gesetzlich festgeschrieben. D.h., es ist erstmal eine Regelung des einfachen Rechts, die hier differenziert. Theoretisch kann man das Recht auch ändern: Man kann sagen, das Passregister wird auch zu einer Art Melderegister, das könnte man ins Gesetz hineinschreiben. Ob das allerdings angemessen wäre, im Hinblick darauf, wenn in Zukunft dann auch die biometrischen Daten generell abrufbar wären, das ist eine andere Frage. D.h., die müsste man noch mal gesondert beantworten, und insbesondere im Hinblick auf die Fingerabdruckdaten habe ich da schon meine Zweifel, dass eine solche Regelung verfassungsrechtlich einwandfrei ausgestaltet werden könnte. Das Passregister dient ausschließlich der Gewährleistung des Passwesens, bei dem es im wesentlichen um die Identitätsfeststellung geht. Das Melderegister dient - auch das ist datenschutzrechtlich ggf. noch mal zu diskutieren - als allgemeiner Informationsbestand für vielfältige öffentliche und nichtöffentliche Stellen. Insofern muss man immer fragen, welche Daten werden für welche Zwecke wem zur Verfügung gestellt. Und gerade bei einem solchen allgemeinen Register muss ich das auf unsensible Daten beschränken. Biometrische Angaben sind immer auch sensible Angaben, und zwar aus einem Grund, der hier bisher nicht allzu intensiv diskutiert worden ist. Ich meine die Frage der so genannten Zusatzinformationen. Das gilt sowohl für die Gesichtsbilder als auch für die Fingerabdrücke. Es gibt verschiedene Zusatzerkenntnisse, die jeder von uns aus einem Gesichtsbild ziehen kann. Wenn man das jetzt standardisiert und automatisiert, dann ist

damit z.B. eine Selektion des farbigen Anteils der Bevölkerung möglich. Es ist möglich, Personen mit bestimmten Gesichtszügen zu selektieren. D.h. es handelt sich dabei im Regelfall um sensible Informationen, die eben bisher nicht Ziel einer Abfrage sind, es aber sein könnten. Insofern ist ein Abruf biometrischer Daten völlig anders zu bewerten als ein Abruf von Adressdaten aus dem Melderegister. Deshalb meine ich auch, dass es bei der bisherigen Praxis bleiben sollte, und ich sehe eigentlich auch nicht, dass die Bundesregierung hier den anderen Weg einschlagen möchte, das Passregister zu einem allgemeinen Auskunftssystem umzubauen. Aber wie gesagt, wenn diese Forderung kommt, ich habe dies im politischen Raum ja auch schon gehört, dann muss darüber diskutiert werden. Ich würde dem sehr skeptisch gegenüberstehen.

Vors. **Sebastian Edathy**: Herr Hofmann, bitte.

BE **Frank Hofmann (Volkach)**: Ich möchte noch mal Herrn Schaar ansprechen und Herrn Schabhüser, und zwar zu der Frage mit den Drittstaaten. Welche Voraussetzungen müssen denn erfüllt sein, damit Drittstaaten die Fingerabdrücke auslesen können, also technisch mit Lesegeräten auslesen können und auch rechtlich auslesen dürfen. Das ist die eine Frage, die ich stellen wollte. Der zweite Bereich geht mehr um die Bewegungsprofile von Personen. Und da die Frage an Herrn Schabhüser: Ist es möglich mit Hilfe des ePass-Chips in deutschen Reisepässen, Bewegungsprofile von Personen zu erstellen? Wenn ja, wie ist es möglich, falls man es hier sagen kann. Wenn nein, wie wird das ganze verhindert? Und dann wollte ich Sie auch noch mal fragen: Wir haben jetzt gesprochen über einen Feldtest, initialisiert zur Erfassung von Fingerabdrücken, ich glaube in fast 30 Passbehörden. Wie haben sich denn die betroffenen Bürger zu der Erfassung der Fingerabdrücke geäußert, weil ja auch die Frage wegen der möglichen ablehnenden Haltung der Bevölkerung aufgetaucht ist. Und im Übrigen wollte ich auch noch fragen - in die Runde vielleicht am besten - gibt es Studien, oder wer kennt Studien, die eine ablehnende Haltung der Bevölkerung zu biometrischen Verfahren dokumentieren, national oder international? Gibt es da irgendetwas auf dem Markt? Danke.

Vors. **Sebastian Edathy**: Das ist die letzte Frage von Herrn Hofmann, kann da jemand etwa dazu sagen? Gibt es Studien zur Akzeptanz der Einführung biometrischer Verfahren? Ist nicht bekannt, oder? Herr Dr. Schabhüser hat sich gemeldet und Herr Prof. Busch.

SV **Prof. Dr. Christoph Busch**: Ich würde ganz allgemein darauf antworten. Die Akzeptanz ist überall da groß, wo ein Vorteil für den Bürger erkennbar ist. Ich nenne zwei Beispiele. Das eine Beispiel hatte ich auch in meiner Stellungnahme schon angedeutet. Es wurde vor nicht allzu langer Zeit in einer Bank in der Schweiz ein biometrisches Zugangskontrollsystem eingeführt, das ein tokenbasiertes System ersetzt. Das ist für die Mitarbeiter in dieser Bank sehr komfortabel. Die Mitarbeiter sind dort sehr zufrieden. In ähnlicher Art, kann man sagen, sind auch die Personen, die bei dem SmartGate-Versuch in Australien an der Pilotierung teilgenommen haben, sehr

zufrieden. Das ist zumindest das Ergebnis der Umfrage, die dort erstellt wurde. Der zweite Aspekt, den hatte ich in meiner Stellungnahme zu der Drucksache 16/3406 erwähnt. Er ist in der bisherigen Diskussion nicht im Vordergrund gewesen. Ich kann mir durchaus vorstellen, dass man, wenn man für nichthoheitliche Anwendungen die Biometrie vielleicht in einer anderen Ausprägungsform - beispielsweise templatebasiert - in den elektronischen Personalausweis einführen würde, für den Bürger ein unmittelbarer Vorteil entsteht. Ich nehme jetzt mal das Szenario Online-Banking. Wenn ich die bisherige Absicherung über PIN und TAN realisiere und dabei ein Transaktionslimit habe - wo auch immer das bei meiner Bank liegt - und ich nachweisen kann, ich habe jetzt hier einen elektronischen Pesonalausweis, und ich in einer höheren Stufe nachweisen kann, ich habe einen elektronischen Personalausweis und eine biometrische Charakteristik, die ich präsentiere, und in einer noch höheren Stufe vielleicht eine nicht-flüchtige biometrische Charakteristik, die ich präsentiere, dann steigert sich mit jeder Stufe mein Verfügungsrahmen, d.h., ich habe einen Vorteil dadurch. Ich glaube, das wäre dann ein Weg, bei dem man einen unmittelbar erkennbaren Vorteil für den Bürger einräumen könnte. Er ist nicht verpflichtet, das zu nutzen. Er kann nach wie vor zum Schalter gehen und sich dort das Geld holen oder zum ATM-Automaten.

Vors. **Sebastian Edathy**: Also, wenn die Kollegin Stokar und Kollege Korte noch Anmerkungsbedarf haben, dann bitte ich um entsprechende Wortmeldung. Ansonsten hat jetzt zunächst Herr Dr. Schabhüser das Wort zur Frage „Akzeptanz“, aber auch zu den übrigen an ihn gerichteten Fragen des Kollegen Hofmann.

SV **Dr. Gerhard Schabhüser**: Zunächst zum Thema „Akzeptanz“. Herr Busch hat schon SmartGate erwähnt. Positive Rückmeldung gibt es überall dort, wo ein positiver Effekt zu erwarten ist. Zurückkommend auf den Feldtest, der adressiert worden ist: Es ist so, dass in 28 Behörden derzeit die Fingerabdruckausgabe getestet wird. Der Beginn des Feldtextes war am 1.3.2007. Er soll am 30.6.2007 beendet sein. Wir haben Fragebögen für die Sachbearbeiter erstellt, wozu derzeit Rückmeldungen schon eingegangen sind, wo die Akzeptanzfrage gestellt wurde. Die Rückläufer sind folgendermaßen: Also, Akzeptanz der Fingerabdruckerfassung und -speicherung seitens der Antragsteller, also Speicherung im Chip. Die Stimmung ist insgesamt gut bis positiv. 61 Prozent der Bearbeiter schätzten die Akzeptanz bei den Bürgern mit „gut“ ein, 21 Prozent schätzten die Akzeptanz mit „sehr gut“ ein, 18 Prozent schätzten die Akzeptanz der Bürger mit „weniger gut“ ein. (….)

Zwischenrufe (nicht rekonstruierbar)

Vors. **Sebastian Edathy**: Herr Dr. Schabhüser hat das Wort und der Kollege Korte hat es jetzt nicht.

SV **Dr. Gerhard Schabhüser**: Ich gebe eine Rückmeldung aus dem Test zurück. Es ist eine Fragestellung, die erstellt worden ist. Die drei anderen Fragen, Voraussetzung für

Drittstaaten zum Auslesen von Fingerabdruckdaten technisch - ich hatte das eben erläutert: Das Verfahren ist so, dass nur autorisierte Leser lesen können. Autorisierte Leser werden von einer Zertifizierungsstelle in Deutschland mit einem Zertifikat versehen über eine zweistufige Public Key Infrastruktur, technische Details, da möchte ich jetzt nicht darauf eingehen. Und über diesen Pfad werden Leser freigeschaltet. Das setzt zuvor ein Mandat voraus, dass diese Freischaltung erfolgt. Das ist ein politischer Prozess, zu dem ich nichts sagen kann. Der zweite Punkt war: Bewegungsprofile von Personen mit ePässen erstellen. Das zielt ein bisschen auf die RFID-Technologie auf unterster Ebene ab. Da wird normalerweise eine Unique-ID vergeben und über diese ID könnte man Profile erstellen, wenn man die Zuordnung entsprechend platziert hat. Das ist aber in den Pässen so nicht realisiert. Die in den RFID-Chips typischerweise feste Unique-ID ist in diesem Fall durch eine zufallserzeugte ersetzt, so dass jedes Mal beim Lesen eine andere Zahl platziert wird und aus diesem Grund die Unique-ID so nicht funktioniert. Das ist der zweite technische Punkt gewesen.

Vors. **Sebastian Edathy**: Danke. Dann Herr Schaar, bitte.

SV **Peter Schaar**: Zum Thema „Zugangsmöglichkeit zu Fingerabdrücken“. Da gibt es bisher keine besonderen rechtlichen Regelungen, auch nicht in dem Gesetzentwurf. Und ich denke, dass es sicherlich sinnvoll wäre, hier eine gesetzliche Festlegung vorzunehmen, unter welchen Voraussetzungen an Drittstaaten die erforderlichen Schlüssel für den Zugriff auf die Fingerabdruckdaten weitergegeben werden. Wir sind uns, glaube ich, hier unter den Sachverständigen alle einig, dass es zwischen der Sensibilität der Fingerabdruckdaten und der Gesichtsbilddaten einen erheblichen Unterschied gibt. Dementsprechend wäre es im Sinne des Grundrechtschutzes der Passinhaber, wenn der Gesetzgeber selbst regeln würde, welchen Staaten - nicht enumerativ aufgezählt, aber unter welchen Voraussetzungen - dieser Schlüssel zur Verfügung gestellt wird, um auszuschließen, dass Staaten, die kein angemessenes Datenschutzniveau haben, die Fingerabdruckdaten auslesen könnten. Dieses wäre durchaus ohne weiteres ins Gesetz zu formulieren, jedenfalls leichter, als etwa eine Regelung zur Online-Durchsuchung zu finden, die verfassungsrechtlichen Vorgaben entspricht. Z.B. könnte man sagen, sofern in den Staaten bestimmte Voraussetzungen gegeben sind, wenn also dort ein angemessenes Datenschutzniveau in Bezug auf diese Daten und ihre Zweckbindung erreicht wird und wenn die Fingerabdruckdaten nicht in zentralen Dateien landen, wird diesen Staaten der Leseschlüssel zur Verfügung gestellt. Das könnte man ohne weiteres in das Gesetz hineinschreiben. Ich denke, das macht schon Sinn, um einen wirksamen Grundrechtschutz zu verwirklichen. Insofern bringt eine Anhörung auch neue Anregungen.

Vors. **Sebastian Edathy**: Eine Nachfrage zunächst vom Kollegen Hofmann. Wenn noch Fragen offen sind, wird auch Frau Philipp noch etwas fragen.

BE **Frank Hofmann (Volkach)**: Wir haben es jetzt nicht im Gesetz drin. Es gibt im Moment keine Regelung, die es dem deutschen Staat erlauben würde, dann dass diese

Pässe in anderen Drittstaaten gelesen werden. Klar gibt es Regierungsabkommen oder irgendetwas anderes. Es gibt also keine Möglichkeit, d.h. das ganze kann nur passieren in Europa.

SV **Peter Schaar**: Das habe ich nicht gesagt. Ich habe nur ausgeführt, es gibt keine Regelung. Man muss ja unterscheiden zwischen dem, was im internationalen Reiseverkehr verpflichtend vorgegeben ist und dem, was optional ist. Der ICAO-Standard bezieht sich, was das Pflichtprogramm anbelangt, ausschließlich auf das Gesichtsbild und beinhaltet Angaben zur Basic Access Control. D.h., das Gesichtsbild kann überall gelesen werden durch Geräte, die entsprechend technisch ausgestattet sind. Angesichts der höheren Sensibilität der Fingerabdrücke wäre es aber angemessen, die entsprechenden Berechtigungen an eine gesetzliche Voraussetzung zu binden. Und dieses würde sicherlich bedeuten, dass man dann eine entsprechende Norm in das Gesetz aufnimmt, die genau die Kriterien festlegt, unter denen dieser Schlüssel weitergegeben wird und vielleicht auch ein Verfahren, wie das Vorliegen, das Vorhandensein dieser entsprechenden Kriterien festgestellt werden kann. Welche Staaten diesen Voraussetzungen genügen, muss ja der Gesetzgeber nicht selber festlegen, das kann ja das Bundesinnenministerium ggf. tun. Es ist im Sinne der Transparenz, dass die Liste der Staaten, in denen der Fingerabdruck ausgelesen werden kann, öffentlich bekannt gemacht wird, etwa auf einer Web-Seite. Das wäre ohne weiteres möglich, und das wäre übrigens auch sinnvoll im Sinne einer Nachvollziehbarkeit für den Betroffenen, dass nicht etwa ein Staat zu Unrecht behauptet, er dürfte die Daten auslesen. Dann würde genau das passieren, was hier als Szenario von Herrn Prof. Pfitzmann angedeutet wurde, dass das überhaupt gar nicht zum Auslesen verwendet wird. Ohne Veröffentlichung habe ich überhaupt gar keine Chance, dieses zu kontrollieren. Ein solches Verfahren würde auch die Datenschutzkontrolle sehr erleichtern.
Wenn ich zu den anderen Punkten noch etwas sagen dürfte, würde ich das jetzt hier auch noch machen. Zum Thema „Bewegungsprofile“: Das ist eine sehr allgemeine Frage, letztlich nur zu beantworten im Hinblick auf die Kontrolldichte, die tatsächlich besteht. Bisher ist es praktisch nicht möglich, Bewegungsprofile mit den ePässen anzulegen, weil es keine Lesegeräte gibt. Wenn überall an den Grenzen Lesegeräte sind, kann man feststellen, ob jemand einreist oder ausreist. Das kann man heute aber auch feststellen, d.h., es ist kein zusätzliches Bewegungsprofil. Wenn sich allerdings in unseren Personalausweisen auch Biometrie-Chips befinden und diese biometrischen Angaben auch zur innerstaatlichen Identitätskontrolle verwendet werden, dann ist es möglich, an Kontrollstellen bei bestimmten Ereignissen die Identitätsfeststellungen zu beschleunigen, indem man ggf. die Pässe oder Personalausweise automatisiert kontrolliert und auch die Verifikation anhand des Fingerabdrucks - wahrscheinlich nicht des Gesichtsbildes - vornimmt. Das würde dann bedeuten, dass dann die Kontrolldichte steigt. Wenn die Kontrolldichte zunimmt, werden auch Bewegungsprofile einfacher. Die dritte Phase wäre die Kombination der biometrischen Merkmale, die jetzt im Rahmen der Pässe oder auch später bei Personalausweisen erhoben werden, mit Kontrollmaßnahmen, die im Rahmen der Videoüberwachung durchgeführt werden. Das

ist rechtlich bisher nicht zulässig, aber technisch wird es zunehmend möglich. Herr Ziercke und ich waren vor einiger Zeit bei der Wissenschaftspressekonferenz in Bonn. Dort wurde genau über diese Frage gesprochen. Und ich halte es für ziemlich wahrscheinlich, dass die Möglichkeiten zur elektronischen Gesichtsbilderkennung bei Videoüberwachung deutlich zunehmen werden. Man wird niemals zu einer 100%igen Erkennungsleistung kommen, das halte ich für völlig ausgeschlossen, aber man wird sicherlich eine Qualitätssteigerung erreichen. Wenn das tatsächlich eingetreten sein wird, und ich denke, das ist allerdings noch eine Frage von einigen Jahren, dann wäre es möglich, diese Angaben - bestimmte technische Infrastruktur und rechtliche Regelungen vorausgesetzt - auch für die Erstellung von Bewegungsprofilen zu nutzen. Ich will hier niemandem unterstellen, dass er das anstrebt, aber die Logik von Entwicklung spricht dafür, dass Daten, die einmal da sind, technische Infrastrukturen, die da sind, technische Möglichkeiten, die da sind, bei entsprechender allgemeiner Gefahreneinschätzung eben auch genutzt werden. Mir erscheint es nicht ausgeschlossen und im Gegenteil sogar als wahrscheinlich, dass solche Forderungen zumindest irgendwann mal hochkommen werden. Bisher sind sie jedenfalls noch nicht da.
Zu internationalen Erfahrungen: Es gibt einen ganz großen ‚Feldversuch', der durchgeführt wird, seit einiger Zeit in den Vereinigten Staaten über die Akzeptanz von biometrischen Merkmalen bei in die USA einreisenden Personen. Dieses ist keine Erfolgsstory, d.h. die Akzeptanz - wenn man es an der Anzahl der Einreisenden bemisst - ist nicht so sonderlich groß bisher. Das kann sich natürlich ändern, wenn an jeder Grenze biometrische Merkmale erhoben werden. Dann überlegt man sich vielleicht, ob man es nicht doch akzeptiert, auch wenn man bisher ansonsten Vorbehalte dagegen hat.

Vors. **Sebastian Edathy**: Weitere Wortmeldungen sehe ich nicht. Oder doch, Herr Kollege Tauss?

Abg. **Jörg Tauss**: Ich wollte den Prof. Pfitzmann fragen. Mich würde es einfach interessieren, ich sage das als Forschungskollege, ich halte die ganze Frage „Gesichtserkennung" zum Teil technisch für eine Fehlentwicklung. Ich hielte es für intelligenter, Herr Präsident des Bundeskriminalamtes, wenn wir uns nicht darauf verwenden, wer könnte möglicherweise so aussehen wie ein Tourist, sondern die Möglichkeiten, die wir technisch hätten, nützen, um rauszukriegen, wer Sprengstoff am Leib hat, und den sofort identifizierbar machen mit technischen Systemen. Und da die Anstrengungen reinrichten. Die Frage ist nach Technik der datensparsamen Implementierungen der bisherigen Sicherheitssysteme und zwar unter dem Gesichtspunkt auch dessen, was Art. 29, die Arbeitsgruppe entsprechend dargestellt hat. Also, ganz konkret, Implementierung des ePasses, Stand der Technik, auch unter dem Gesichtspunkt der Datensparsamkeiten. Datensparsamkeiten ist übrigens auch etwas, was wir als Stand der Technik im Datenschutzrecht verankern wollen.

Vors. **Sebastian Edathy**: Das war jetzt eine Frage, Herr Tauss, die sich richtete an Prof. Pfitzmann? Dann bitte ich Herrn Prof. Pfitzmann um eine möglichst effiziente Beantwortung der Frage.

SV **Prof. Dr. Andreas Pfitzmann**: Okay. Der große Fortschritt wäre, wenn die biometrische Messung nicht stattfinden würde in einem fremden Gerät, also einem Gerät, was ich vor Ort vorfinde, dem ich dann möglicherweise zwar traue, wenn da der Bundesadler draufklebt, aber weniger traue, wenn da der Bundesadler fehlt. Wenn diese biometrische Messung gemacht werden könnte in einem Gerät, was mein Gerät ist, und es gibt Entwicklungen im Bereich Trusted Computing, Geräte soweit zu kapseln, dass Manipulationen durch denjenigen, der das Gerät physisch hat, erkannt werden. Es ist noch ein weiter Weg, bis das effizient geht. Aber wenn man in eine Richtung geht, dann wäre eine Richtung datensparsam und datenschutzverträglich, wo die biometrische Messung im Hoheitsbereich des Vermessenen durchgeführt wird. Und das, was dieses Gerät verlässt, ist eben nicht mehr die biometrische Messung, sondern eine digitale Signatur, dass das alles stimmt mit den entsprechenden Zertifikaten. Dort sollte man langfristig hin. Diese Sache kurzfristig einzuführen - denke ich - geht technisch nicht. Aber das weist die Forschungsrichtung. Danke schön.

Vors. **Sebastian Edathy**: Vielen Dank, Herr Prof. Pfitzmann. Weitere Wortmeldungen liegen nicht vor. Ich darf mich herzlich bedanken, insbesondere bei den Sachverständigen, dass Sie uns hier im Ausschuss Rede und Antwort gestanden haben, und wünsche noch einen erfolgreichen weiteren Arbeitstag bzw. eine gute Heimreise. Die Sitzung ist geschlossen.

Ende der Sitzung: 17.00 Uhr