

Faktenblatt zur Kommissionsinitiative 09.471 "Biometrische Ausweise"

Die Kommissionsinitiative 09.471 "Biometrische Ausweise"

(http://www.parlament.ch/d/suche/Seiten/geschaefte.aspx?gesch_id=20090471) lautet:

Eingereichter Text:

Die Staatspolitische Kommission des Nationalrates beschliesst, eine Änderung des Ausweisgesetzes auszuarbeiten, welche den anlässlich der Volksabstimmung vom 17. Mai 2009 geführten Diskussionen über die biometrischen Ausweise Rechnung trägt:

1. Die dem Bundesrat übertragene Kompetenz zur Festlegung der Ausweisarten, welche mit einem Datenchip versehen werden müssen, soll durch das Gesetz in der Weise eingeschränkt werden, dass nach wie vor nichtbiometrische Identitätskarten ausgestellt werden können.

2. Auf eine obligatorische zentrale Speicherung der Daten soll verzichtet werden. Es ist zu prüfen, ob auf die zentrale Datenbank entweder überhaupt verzichtet wird oder ob jede Bürgerin und jeder Bürger individuell verlangen darf, dass ihre bzw. seine Daten nicht zentral gespeichert werden.

Diese Kommissionsinitiative fasst die Anliegen von insgesamt fünf Parlamentarischen Initiativen (Pa.Iv.) zusammen, die vor und nach der Volksabstimmung zu diesem Thema eingereicht wurden (09.431 n Pa.Iv. Marra, SP, **Ausweisgesetz**; 09.435 n Pa.Iv. Hodgers, Grüne, **Änderung des Ausweisgesetzes**; 09.439 n Pa.Iv. Meyer Thérèse, CVP, **Allen Schweizer Staatsangehörigen auch weiterhin den Bezug einer herkömmlichen, nichtbiometrischen ID ohne Chip zusichern**; 09.440 n Pa.Iv. Fraktion SVP, **Keine zusätzlichen biometrischen Ausweise**; 09.441 n Pa.Iv. Fraktion SVP, **Biometrische Pässe ohne Datenbank**). Bevor die Staatspolitische Kommission des Nationalrates ihre Kommissionsinitiative umsetzen kann, muss sie noch die Zustimmung der Staatspolitischen Kommission des Ständerates einholen. Im Nationalrat sind zudem zwei weitere Vorstösse zur gleichen Thematik pendent: 09.3678 Motion Kiener Nellen, SP, **Keine Identitätskarte mit biometrischen Daten. Kein Abbau des Service public bei den Gemeinden** sowie 09.3949 Motion Kiener Nellen, SP, **Stopp dem Ausbau der zentralen Datenbank für Fingerabdrücke**. Diese zweite Motion wurde von 66 Nationalrätinnen und Nationalräten mitunterzeichnet.

Aufgrund der Patt-Situation bei der Volksabstimmung vom 17. Mai 2009 mit dem knappstmöglichen Abstimmungsergebnis von 49,9% NEIN zu 50,1% JA bzw. einem Stimmenunterschied von schweizweit lediglich 5504 Stimmen und einem Ständeverhältnis von 16 Kantone NEIN zu 10 Kantone JA ist die Nachbesserung des Ausweisgesetzes (AwG) und der Ausweisverordnung (VAwG) unabdingbar.

Unter anderem folgende Gründe sprechen für die Zustimmung zu dieser Kommissionsinitiative 09.471 "Biometrische Ausweise":

1. Der Kanton Thurgau wird in Kürze folgende Standesinitiative einreichen: Nicht-biometrische Identitätskarten sollen auch in Zukunft bei der Gemeinde erhältlich sein

Die Regierung des Kantons Thurgau unterstützt in ihrer Antwort vom 8.12.2009 offiziell eine von 77 von den total 130 Kantonsrätinnen und Kantonsräten des Kantons Thurgau eingereichte Motion vom 17.6.2009 und beantragt dem Kantonsparlament, diese Motion für erheblich zu erklären, damit der Kanton Thurgau eine Standesinitiative in Bern einreicht mit folgendem Text:

Der Kanton Thurgau unterbreitet der Bundesversammlung folgende Standesinitiative:

Der Bund wird aufgefordert, die folgende Übergangsbestimmung der Änderung vom 13. Juni 2008 im Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG; SR 143.1)

ersatzlos aufzuheben:

"Identitätskarten ohne Datenchip können im Inland nach dem Inkrafttreten dieser Gesetzesänderung noch während längstens zweier Jahre wie bisher in der Wohnsitzgemeinde beantragt werden; die Kantone bestimmen, ab wann Identitätskarten nur noch bei den ausstellenden Behörden beantragt werden können."

Mit diesem Vorstoss soll erreicht werden, dass auch in Zukunft die Schweizer Gemeindeverwaltungen nicht-biometrische Identitätskarten abgeben dürfen und die Bürgerinnen und Bürger nicht in ein biometrisches Erfassungszentrum reisen müssen, wenn sie nur eine nicht-biometrische Identitätskarte benötigen.

Weitere Details zu dieser Motion/Standesinitiative findet man unter:

<http://161.78.2.130/grgeko/DetailView.php?>

[SESSID=e3d0e0c547e56f7a9e8b388d38edad&om_id=100&obj_id=4243](http://161.78.2.130/grgeko/DetailView.php?SESSID=e3d0e0c547e56f7a9e8b388d38edad&om_id=100&obj_id=4243) (ist die offizielle Geschäftsdatenbank Kantonparlament Thurgau; dort rechts unten die beiden "Download"-Links anklicken)

Medienberichte darüber:

[http://www.thurgauerzeitung.ch/thurgau/kanton/IDAusgabe-Gemeinden-machen-](http://www.thurgauerzeitung.ch/thurgau/kanton/IDAusgabe-Gemeinden-machen-mobil/story/27981955)

[mobil/story/27981955](http://www.thurgauerzeitung.ch/thurgau/kanton/IDAusgabe-Gemeinden-machen-mobil/story/27981955) : "19.6.2009. ID-Ausgabe: Gemeinden machen mobil. Die Thurgauer Gemeinden kämpfen dafür, dass sie weiterhin die Identitätskarten abgeben dürfen. Sie wollen mit einer Standesinitiative das Bundesgesetz ändern."

[http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-wollen-ID-selbst-](http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-wollen-ID-selbst-abgeben/story/14533306)

[abgeben/story/14533306](http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-wollen-ID-selbst-abgeben/story/14533306) : "18.8.2009. Gemeinden wollen ID selbst abgeben. Die Thurgauer Gemeinden wollen weiterhin die ID an die Bürger abgeben können. **Ständerat Hermann Bürgi ist zuversichtlich, dass das Anliegen bei der Revision des Ausweisgesetzes aufgenommen wird.** ... Jetzt bekommen die Gegner der zentralisierten Abgabe Schützenhilfe aus Bern. Die Staatspolitische Kommission des Nationalrats (SPK-N) habe am 19. Juni eine Kommissionsinitiative angenommen, die das Ausweisgesetz in einigen Punkten ändern wolle. Damit habe das Parlament Anliegen der Bevölkerung aufgenommen, sagt der Thurgauer Ständerat Hermann Bürgi (SVP). So solle unter anderem im Ausweisgesetz ausdrücklich festgehalten werden, dass es weiterhin eine konventionelle ID geben müsse. Weiter solle der Verzicht auf die umstrittene zentrale Datenbank geprüft werden. **Wenn man das Ausweisgesetz in diesen Punkten ändere, sollte man die dezentrale Abgabe der konventionellen ID wieder aufgreifen, findet Bürgi. Allenfalls könne er sich einen entsprechenden Antrag vorstellen. Er erwarte, dass die Initiative der SPK-N von der Staatspolitischen Kommission des Ständerats unterstützt werde. Das Ja der SPK-N sei mit 18:2 Stimmen überdeutlich.**"

[http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-sollen-weiterhin-Identitaetskarten-](http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-sollen-weiterhin-Identitaetskarten-ausstellen-koennen/story/27588389)

[ausstellen-koennen/story/27588389](http://www.thurgauerzeitung.ch/thurgau/kanton/Gemeinden-sollen-weiterhin-Identitaetskarten-ausstellen-koennen/story/27588389) : "11.12.2009. Gemeinden sollen weiterhin Identitätskarten ausstellen können. Identitätskarten sollen auch in Zukunft bei den Gemeinden beantragt werden können. Der Thurgau soll eine Standesinitiative einreichen, um die gesetzliche Regelung zu ändern, wonach ID nur noch bei einer speziellen kantonalen Stelle beantragt werden können. ... In ihrer am Freitag veröffentlichten Motionsantwort stimmt die Kantonsregierung dem Begehren zu. Mit der Standesinitiative soll erreicht werden, dass die Wohnsitzgemeinden weiterhin Anträge für ID entgegennehmen können."

<http://www.tagblatt.ch/aktuell/thurgau/tb-tg/Gemeinden-sollen-ID-ausgeben;art219,1434612> :

"12.12.2009. Gemeinden sollen ID ausgeben. Der Kanton Thurgau soll sich beim Bund dafür einsetzen, dass Identitätskarten auch in Zukunft bei der Gemeinde beantragt werden können. Der Regierungsrat unterstützt einen entsprechenden Vorstoss aus dem Grossen Rat."

2. Die „Identitätskarte bei den Gemeinden belassen“ entspricht dem verfassungsmässigen Subsidiaritätsprinzip

Die „Identitätskarte bei den Gemeinden belassen“ ist wohl eines der einfachstmöglichen Anwendungsbeispiele für das (in der Schweiz vielgelobte!) verfassungsmässige Subsidiaritätsprinzip.

Aufgaben sollen bei der föderal unterstmöglichen Ebene (Bund, Kanton, Gemeinde) vollzogen werden. Bei der Bestellung und Aushändigung der Identitätskarten kann diese in den Gemeindeverwaltungen äusserst bewährte und beliebte Dienstleistung problemlos von den Gemeinden weiter ausgeführt werden. Dort kann sie am kostengünstigsten und sehr bürgernah erbracht werden (Bergkantone, grosse Kantone). Das KOMBI-Argument (Pass und Identitätskarte gleichzeitig kaufen) des Bundesamtes für Polizei sticht nicht. Eine Mehrheit der Bürgerinnen und Bürger wird immer die viel günstigere Identitätskarte ohne Chip wollen. Das KOMBI-Angebot ist nur für Bürgerinnen und Bürger, die sich Reisen ausserhalb Europas leisten (können).

Es wäre skandalös, auf dieser Grundlage unsere Bürgerinnen und Bürger zu zwingen, persönlich und auf eigene Kosten in die wenigen kantonalen Ausweiszentren reisen zu müssen, um lediglich eine Identitätskarte zu erhalten. Dieser Mehraufwand wäre für die betagte Bevölkerung, Familien mit Kindern, Menschen mit Behinderung usw. unzumutbar. In den meisten Kantonen wird es nur 1 einziges Ausweiszentrum geben, u.a. im Kanton VD mit 688'000 Einwohnern! Ein beispielloser Abbau des Service Public für eine vielgeschätzte Aufgabe, die heute und auch in Zukunft problemlos von den 375 (!) politischen Gemeinden im Kanton VD (bzw. den 2'600 Gemeinden in der ganzen Schweiz) wahrgenommen werden kann.

http://www.letemps.ch/Page/Uuid/a74fbd70-56c7-11de-b3ee-e562a179aa80/Passeport_biométrique_les_communes_blâment_la_centralisation : “12 juin 2009. Passeport biométrique: **les communes blâment la centralisation**. L'ouverture d'un seul centre, à Lausanne, pour l'établissement des nouveaux documents à partir de mars 2010 ravive le débat sur l'organisation administrative de l'Etat. Une conférence de presse et une annonce à première vue anodine ont ravivé ce jeudi l'animosité entre le canton et les communes vaudoises, que l'on cherche à pacifier depuis le début de la législature. Par la même occasion le débat sur l'organisation de l'Etat et sa présence sur le territoire a repris de plus belle. Après le oui étriqué du peuple suisse au passeport biométrique le 17 mai, Vaud vient de décider qu'un seul centre, à Lausanne, intégré au Service de la population (SPOP), délivrera le nouveau sésame à partir de mars 2010. Le même centre se chargera des cartes biométriques pour les étrangers non européens, Schengen-Dublin oblige. Cela concerne les permis B, C et L.”

3. Die (nicht-biometrische) Identitätskarte genügt für Reisen in 29 europäische Länder

Die folgenden Länder akzeptieren die (nicht-biometrische!) Schweizer Identitätskarte für die Einreise: **Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Schweden, Slowakei, Slowenien, Spanien, Tschechien, Ungarn, Vereinigtes Königreich (Grossbritannien), Zypern, Norwegen, Liechtenstein, Island, Türkei.**

(Stand Mai 2009, Quelle: Bundesamt für Polizei fedpol, Sektion Ausweisschriften)

Um sich hier klar und deutlich auszudrücken: Um in diese 29 europäischen Staaten einzureisen, brauchen Schweizer Bürgerinnen und Schweizer Bürger **keinen** Schweizer Pass (weder einen biometrischen noch einen nicht-biometrischen Pass). Sie brauchen auch **keine** biometrische Identitätskarte. Eine normale nicht-biometrische Schweizer Identitätskarte ohne Chip wird von all diesen Staaten für die Einreise akzeptiert und wird in der Schweiz (z.B. für Bank, Post, Bahnschalter usw.), in unseren 5 Nachbarstaaten und den weiteren 24 europäischen Ländern noch während Jahren gültig sein.

Auf einer solchen Grundlage den Schweizer Bürgerinnen und Bürgern ein gesetzlich garantiertes Recht zum Bezug einer nicht-biometrischen Identitätskarte zu verwehren, wäre einer freiheitlichen Demokratie unwürdig. Politik ist ein zu schnelllebiges Geschäft, als dass man sich hier auf irgendwelche mündlichen Versprechen einzelner Regierungsmitglieder (die in einigen Jahren nicht mehr im Amt sind) oder Regelungen auf Verordnungsstufe verlassen kann.

4. Die zentrale Speicherung der Daten als Haupt-Gegenargument in der Volksabstimmung vom 17.5.2009

Die vom Institut für Politikwissenschaft der Universität Genf und vom Berner Forschungsinstitut gfs durchgeführte VOX-Analyse vom 9. Juli 2009 der eidgenössischen Abstimmung vom 17. Mai 2009

bestätigte das bereits in den Abstimmungsdiskussionen und Meinungsumfragen sichtbare Bild, dass die grösste Ablehnung die Zentralisierung der Informationen und den Datenschutz betraf:

http://www.polittrends.ch/abstimmungen/abstimmungsanalysen/vox-analysen/2009-05-17_VoxD.pdf : "Bei der Ablehnung der Vorlage überwogen Befürchtungen im Zusammenhang mit dem Datenschutz."

Begleitstudie 2. Welle: April/Mai 2009 vom 05.05.09, durchgeführt vom gfs.bern:

http://www.gfsbern.ch/pub/sftrend_06_05_09-090506.pdf : "Von den gegnerischen Botschaften ist die zum Überwachungsstaat am eingängigsten; eine eindeutige Mehrheit teilt dieses Bedenken. ... Argumentativ verfügen beide Seiten über mehrheitsfähige Argumente. Auf der Ja-Seite ist das – trotz Expertenkritik – vor allem die Sicherheit der neuen Pässe, etwas eingeschränkt auch die Reisefreiheit. Auf der Nein-Seite sind es der Überwachungsstaat, die Kosten und etwas eingeschränkt die Verletzung der Privatsphäre. Bisher am meisten gewirkt haben die Folgen der Zentralisierung von Daten auf das Privatleben im Fall einer Zustimmung und die Einschränkung der Reisefreiheit bei einem Nein. Bei den unschlüssigen Personen stehen sich auch gut zwei Wochen vor dem Stichtag zwei ähnliche Erwartungen gegenüber: die Angst vor dem Überwachungsstaat auf der einen, die Befürchtungen vor Reiserestriktionen auf der anderen Seite."

Neue biometrische Pässe umstritten: Trendstudie 1. Welle: März/April 2009 vom 07.04.09, durchgeführt vom gfs.bern:

http://www.gfsbern.ch/pub/sftrend_09_04_09.pdf : "Die vorläufige Bewertung der Argumente: Das populärste Schlagwort gegen die neuen Reisepässe betrifft den „Überwachungsstaat“. 64 Prozent der Stimmberechtigten sind ganz oder eher der Meinung, mit ihrer Einführung mache man einen Schritt in diese Richtung. Damit legt eine negative Botschaft die am meisten geteilte Basis für den Abstimmungskampf. 58 Prozent der Befragten sind zudem der Meinung, die neuen Pässe seien zu teuer. Schliesslich ist auch das dritte der getesteten Nein-Argumente mit einer Zustimmungsrate von 57 Prozent mehrheitsfähig. Demnach verletzt die zentrale Speicherung biometrischer Daten die Privatsphäre. Unter dem Strich gesehen, verfügt die Nein-Seite damit über drei Botschaften, die mehrheitlich geteilt werden. Das ist auf der Ja-Seite nicht der Fall. ... Der Schluss daraus ist eindeutig. Die vorläufigen Stimmabsichten am klarsten polarisiert das Nein-Argument, wonach mit der vorgeschlagenen Einführung neuer Pässe die Privatsphäre tangiert wird. Das ist zwar nicht ein generelles Nein zu biometrischen Reisedokumenten, doch eines, das sich gegen die Zentralisierung der Informationen wendet."

5. Im Bundesbudget 2010 wurden bereits alle Ausgaben für die Erweiterung der zentralen Datenbank ISA mit Fingerabdrücken definitiv und vollumfänglich in beiden Räten gestrichen

Die im Voranschlag der Eidgenossenschaft 2010 ursprünglich vorhandenen Ausgaben für die Speicherung von Fingerabdrücken auf einer zentralen Datenbank (Investitionsausgaben von CHF 100'000 sowie Betriebskosten Informatik Sachaufwand von CHF 200'000) wurden im Dezember 2009 von beiden Kammern (Nationalrat und Ständerat) ersatzlos gestrichen.

http://www.parlament.ch/ab/frameset/d/s/4812/316392/d_s_4812_316392_316509.htm :

"Ständerat - Wintersession 2009 - Elfte Sitzung - 09.12.09-08h25

09.041 Voranschlag der Eidgenossenschaft 2010 ...

Justiz- und Polizeidepartement. 403 Bundesamt für Polizei. **Antrag der Kommission**

A2114.0001 Informatik Sachaufwand

A4100.0126 Einführung biometrischer Pass

Zustimmung zum Beschluss des Nationalrates ...

Stähelin Philipp (CEg, TG), für die Kommission: ... Bei der Position "Einführung biometrischer Pass" beispielsweise haben wir uns einander auf 100 000 bzw. 200 000 Franken angenähert. Es besteht gewissermassen nur noch eine symbolische Differenz, um den Hinweis auf die zentrale Sammlung der Fingerabdrücke und die Initiative wachzuhalten. ... Wir beantragen Ihnen deshalb, überall dem Nationalrat zu folgen. ... **Angenommen**"

Aufgrund der Materialien im Protokoll der Finanzkommission des Nationalrats (FK-N) ist klar, dass mit diesem rechtskräftigen Budgetbeschluss 2010 die Erweiterung der zentralen Datenbank um die Fingerabdrücke mit Bezug auf die sehr deutliche Annahme der Kommissionsinitiative 09.471 "Biometrische Ausweise" 2010 vorerst sistiert und einem Ausgabenmoratorium unterstellt werden muss.

6. Bis auf ganz wenige Ausnahmen verzichten alle Staaten auf eine zentrale Speicherung der biometrischen Passdaten

Nur in vier (!) anderen Ländern (Frankreich, Portugal, Niederlande und Grossbritannien) wird überhaupt eine zentrale Speicherung der biometrischen Passdaten vorgenommen. Alle anderen Staaten, so auch die Schweizer Nachbarstaaten Deutschland, Österreich und Fürstentum Liechtenstein, haben sich definitiv gegen eine zentrale Speicherung von biometrischen Daten bei der Ausweiserstellung entschieden. http://www.vaterland.li/page/lv/artikel_detail.cfm?id=35417 : **Liechtenstein:** "12.5.09. Gleichzeitig wird der **Fingerabdruck tatsächlich nur auf dem Chip gespeichert und nicht noch auf einer externen Datenbank**», so der Amtsleiter des Ausländer- und Passamts." **Und in Österreich müssen sogar die lokalen Passbehörden die biometrischen Daten nach Ausstellung des Reisedokuments löschen, d.h. es findet weder eine zentrale noch eine lokale Speicherung der Daten statt. Auch in Deutschland ist eine zentrale Datenbank mit dauerhafter Speicherung der (biometrischen und anderen) Daten deutscher Passinhaber verboten.** §16 Abs. 2 Satz 1 des deutschen Passgesetzes (http://www.gesetze-im-internet.de/bundesrecht/pa_g_1986/gesamt.pdf) verbietet es, Beantragung, Ausstellung und Ausgabe von Pässen zum Anlass zu nehmen, die dafür erforderlichen Angaben (also insbesondere die Personengrunddaten wie Name, Vorname, Geburtsdatum usw.) und die biometrischen Merkmale ausser bei den zuständigen Passbehörden zu speichern (also nur lokale Speicherung!). Der Passhersteller darf die Daten nur temporär für die Dauer der Passherstellung speichern (§16 Abs. 3 Satz 2 PassG). Die bei der Passbehörde gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des Passes an den Passbewerber zu löschen (§16 Abs. 2 Satz 3 PassG). Zudem kann in Deutschland jeder Bürger wählen, ob er eine Identitätskarte mit oder ohne biometrische Fingerabdrücke will.

Erst am 4.12.2008 hat der Europäische Gerichtshof für Menschenrechte in Strassburg in einem Gerichtsurteil (<http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843941&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>) entschieden, dass die Speicherung von DNA-Daten und Fingerabdrücken unter bestimmten Voraussetzungen gegen Artikel 8 der Europäischen Menschenrechtskonvention verstösst und die Regierung von Grossbritannien zu einer hohen Schadenersatzzahlung verurteilt.

<http://www.heise.de/newsticker/meldung/EU-Parlament-segnet-Kompromissvorschlag-zu-biometrischen-Reisepaessen-ab-198087.html> : "15.01.2009. ... **Die Mitgliedsländer können nun nicht mehr sagen, dass die Einrichtung von biometrischen Datenbanken auf Grundlage dieser EU-Verordnung notwendig ist**", so Ludfords parlamentarischer Mitarbeiter Wouter van Ballegooij gegenüber heise online. Vielfach hätten Mitgliedsstaaten beim Aufbau der Biometrie-Datenbanken auf Brüssel verwiesen. **In der neu gefassten Verordnung sei nun klargestellt, dass sie nicht zum Aufbau solcher Datenbanken ermächtigt oder auffordert.** ... Eine Grenze für die nationalen Regierungen hat kürzlich der Europäische Gerichtshof für Menschenrechte mit seiner Entscheidung gegen die britische Regierung (Marper vs. UK) gesetzt. **Darin hatte der EGMR die Speicherung von DNA-Daten und Fingerabdrücken für unverhältnismässig und unvereinbar mit dem Artikel 8 der Europäischen Menschenrechtskonvention erklärt. Etwaige nationale Gesetze zu den biometrischen Datenbanken fänden hier ihre EU-rechtliche Grenze**, erläutert van Ballegooji."

<http://www.lirak.li/index.php?src=documents&srctype=download&id=173> : "Deutscher Anwaltverein, Büro Brüssel, Dezember 2008 ... Der Europäische Gerichtshof für Menschenrechte (EGMR) hat in einem Urteil vom 4. Dezember 2008 ein Gesetz des Vereinigten Königreiches für unvereinbar mit Artikel 8 der EMRK über den Schutz der Privatsphäre erklärt. Dieses Gesetz ermächtigt die britischen Behörden DNA-Profile und Fingerabdrücke Verdächtigter unbefristet zu speichern, ungeachtet ob es zu einer Verurteilung kommt oder nicht. Es wird bei der Speicherung ausserdem nicht berücksichtigt, welche Tat einem Beschuldigten vorgeworfen wird. ... Der EGMR hatte abzuwägen, ob das Gesetz den Anforderungen des Artikels 8 EMRK entspricht und es demnach für die Sicherheit einer demokratischen Gesellschaft notwendig ist, DNA-Profile unbeschränkt zu speichern. ... Die Kammer zeigte sich beeindruckt von der Machtfülle der britischen Behörden und wies auf die Wahrscheinlichkeit einer Stigmatisierung von Unschuldigen durch ein System hin, das keinen Unterschied zwischen Kriminellen zu Unschuldigen mache. Das Vereinigte Königreich wurde aufgefordert dieser Situation abzuwehren und den Klägern Schadenersatz zu zahlen."

Lesenswert zu diesem Thema ist auch der Artikel **"Biometrischer Pass: Verstoss gegen die Menschenrechte. Das Aufbewahren von Fingerabdrücken ist nicht zulässig. Speichern von Fingerabdrücken: Strassburger Richter setzen Schranken"** vom 15.04.2009 im Konsumentenmagazin "Saldo" (unter http://www.freiheitskampagne.ch/pdf/Saldo_15042009.pdf).

7. Durch eine biometrische Datenbank würde sich die Schweiz erpressbar machen

Man kann nicht oft genug darauf hinweisen, wie gefährlich diese Biometrie-Datenbank für die Schweiz selber ist. Ausländische Staaten (speziell die USA) warten nur darauf, dass die Schweiz die biometrischen Daten aller Schweizer Bürger in einer Datenbank sammelt. Sobald diese Biometrie-Datenbank steht, werden die USA die Schweiz erpressen, um an diese Daten heranzukommen (via Datenaustausch, Onlinezugriffe usw.). Ganz einfach mit der Drohung "wenn ihr uns keine Zugriffe auf diese Datenbank gebt, führen wir für Schweizer Bürger als Strafe einfach wieder die Visa-Pflicht ein." Diese "Visapflicht-Drohung" können die USA jedes Mal neu bringen, um an zusätzliche Daten heranzukommen und die Erpressung funktioniert so laufend weiter.

Nachfolgend nur 2 Beispiele, wie es in der Praxis bereits läuft in Deutschland, Österreich und Dutzenden weiterer Länder:

Beispiel 1: Zur Erpressung von Österreich durch die USA

Am 25.3.2009 machte die österreichische Zeitung "Die Presse" ein geheimgehaltenes Treffen zwischen österreichischen Beamten (unter anderem aus dem Außen- und Innenressort) und Vertretern der USA, darunter Mitarbeiter des Außen- und Heimatschutzministeriums und FBI-Ermittler, publik:

http://diepresse.com/home/panorama/oesterreich/464415/index.do?_vl_backlink=/home/index.do : "25.03.2009. **Visa-Drohung: USA wollen Österreichs Polizeidaten. US-Heimatschutz fordert Namen, Adressen, Fingerabdrücke, DNA-Daten aus Ermittlerbeständen. Bei einer Weigerung droht Österreichern die Visapflicht.** Streng vertraulich trafen Anfang dieser Woche im zweiten Stock der Herrengasse 13, einer Dependence des Außenministeriums, hochrangige Vertreter des US-Heimatschutzministeriums österreichische Kollegen aus mehreren Ministerien. Der brisante Wunsch der USA: Österreich möge den Vereinigten Staaten **dauerhaft und online Einsicht in ihre Polizeicomputer gewähren.** Namen, Adressen, Fotos und Fingerabdrücke der darin gespeicherten Personen sollen den US-Behörden zur Verfügung stehen. ... Zwei Entwürfe für entsprechende bilaterale Abkommen liegen der "Presse" vor. Für den Fall, dass sich Österreich weigert, derartige Daten weiterzugeben, hat die US-Administration vorgesorgt: Sie droht unverblümt, für Österreicher bei der Einreise in die USA die Visumpflicht wieder einzuführen. ... Einmal über den Atlantik gesendet, findet das relativ strenge österreichische Datenschutzgesetz auf die übermittelten Daten keine Anwendung mehr. Was die Amerikaner mit den Informationen dann machen, bleibt ihnen überlassen. In Wien kündigten sie bereits an, die so gewonnenen Daten "for any lawful service" einzusetzen. ... **Nach Angaben des Heimatschutzes kooperieren bereits 25 Staaten mit den USA. Welche das sind, ist geheim.** Die Daten, die in das System gelangen, werden von den Amerikanern auch nicht auf ihre Zuverlässigkeit überprüft. Was bei Informationen von Nachrichtendiensten problematisch ist, weil es dafür keinen Rechtsschutz gibt. So wurde etwa ein in einem sensiblen Bereich tätiger Mitarbeiter des Flughafens Schwechat vom österreichischen Verfassungsschutz aufgrund nachweislich falscher Geheiminformationen für nicht vertrauenswürdig befunden und gekündigt. Problematisch ist der Datenverbund auch, weil Informationen 99 Jahre lang gespeichert werden sollen. Weil auch Suchabfragen von Namen, die gar keine Treffer ergaben, 25 Jahre im System bleiben, können reisefreudige Personen und auch Geschäftsleute nach mehreren Abfragen automatisch zu Verdächtigen werden, befürchten Datenschützer. Bei der nächsten Einreise liege für den kontrollierenden Beamten der Verdacht nahe, dass die vielen Abfragen der Vergangenheit wohl einen speziellen Grund gehabt hätten. Das System produziere so seine Verdächtigen mit der Zeit selbst. Unabhängig davon, ob zur geprüften Person etwas vorliege oder nicht."

Ein weiterer Enthüllungsartikel dazu erschien am 26.3.2009: http://diepresse.com/home/meinung/kommentare/leitartikel/464400/index.do?direct=464415&_vl_backlink=/home/panorama/oesterreich/464415/index.do&selChannel= (Artikel mit dem Titel "**Wer schützt die Bürger vor den USA? Österreich soll den US-Behörden Polizeidaten zur Verfügung stellen. Und lässt sich erpressen. Warum?**" vom 26.3.2009). Die Zeitung "Die Presse", welche diesen Skandal publik machte, ist eine überregionale, bürgerlich-konservative österreichische Tageszeitung, die zur Styria Media Group gehört (http://de.wikipedia.org/wiki/Die_Presse).

Ebenfalls am 26.3.2009 veröffentlichte die APA eine Agenturmeldung über die ersten Reaktionen einiger österreichischer Parteien. Siehe den Artikel:

http://diepresse.com/home/panorama/oesterreich/464673/index.do?direct=464415&_vl_backlink=/home/panorama/oesterreich/464415/index.do&selChannel= (Artikel mit dem Titel "**Erpressungsversuch der USA**" vom 26.03.2009). Die APA – Austria Presse Agentur ist die größte nationale Nachrichtenagentur Österreichs mit Sitz in Wien sowie der führende Informationsdienstleister des Landes (http://de.wikipedia.org/wiki/Austria_Presse_Agentur).

Unter http://www.ots.at/presseaussendung/OTS_20090326_OT0037 findet man die veröffentlichte Presse-Stellungnahme der Partei BZÖ zu diesem Skandal.

Auch die grosse österreichische Tageszeitung "Der Standard" (http://de.wikipedia.org/wiki/Der_Standard) berichtete am 26.3.2009 darüber, siehe http://derstandard.at/1237228488070/Datenschutz-Aufregung-um-US-Gier-nach-Austro-Daten?sap=2&_pid=12485182 (Artikel mit dem Titel "**Datenschutz: Aufregung um US-Gier nach Austro-Daten.**" vom 26.3.2009). Darin steht zusätzlich die Information: "**Seit dem Vorjahr können die Ermittler in Deutschland, Österreich und Luxemburg auf diese Weise auch in den elektronischen Fingerabdruckdateien ihrer Pendants stöbern.**", d.h. unter diesen drei Staaten besteht offenbar bereits in der Praxis das gegenseitige Stöbern in den Fingerabdruckdatenbanken der anderen.

Daraufhin wurden im österreichischen Parlament am 22.4.2009 zwei offizielle Anfragen an die österreichische Regierung eingereicht mit "Fragen betreffend die Weitergabe von Polizeidaten an andere Staaten im Lichte des Datenschutzes":

1. Schriftliche Anfrage von Nationalrat Harald Stefan (FPÖ) zusammen mit weiteren Abgeordneten mit 32 Fragen an die Bundesministerin für Inneres (siehe http://www.parlinkom.gv.at/PG/DE/XXIV/J/J_01743/pmh.shtml). Die Antworten vom 22.6.2009 durch die Bundesministerin für Inneres findet man unter http://www.parlinkom.gv.at/PG/DE/XXIV/AB/AB_01799/pmh.shtml
2. Schriftliche Anfrage von Nationalrat Werner Herbert (FPÖ) zusammen mit weiteren Abgeordneten mit 34 Fragen an den Bundesminister für europäische und internationale Angelegenheiten (siehe http://www.parlinkom.gv.at/PG/DE/XXIV/J/J_01745/pmh.shtml). Die Antworten vom 19.6.2009 durch den Bundesminister für europäische und internationale Angelegenheiten findet man unter http://www.parlinkom.gv.at/PG/DE/XXIV/AB/AB_01759/pmh.shtml

Die Antworten der Regierung sind in beiden Fällen mehr oder weniger faule Ausreden, um die aufgeflogene Sache kleinzureden. Die österreichische Regierung und die Regierungsparteien haben alles unternommen, um den Skandal um dieses publik gewordene Geheimtreffen soweit wie möglich herunterzuspielen. Der Skandal hat in der Zeit März bis Juni 2009 in Österreich Wellen geschlagen, scheint dann aber wieder etwas in der Versenkung verschwunden zu sein.

Beispiel 2: Zum Zugriff der USA zu Fingerabdrücken und DNA in Deutschland

<http://www.daten-speicherung.de/index.php/zugriff-der-usa-auf-deutsche-fingerabdruecke-und-dna-geplant/> : "5. Mai 2009. **Zugriff der USA auf Fingerabdrücke und DNA von Deutschen geplant.** Ohne parlamentarische Beteiligung, hinter verschlossenen Türen und im deutschen Alleingang haben Wolfgang Schäuble (CDU) und Brigitte Zypries (SPD) mit den USA ein Abkommen ausgehandelt, welches einer ungenannten Zahl US-amerikanischer Behörden (darunter US-Strafverfolger, US-Grenzbehörden und US-Geheimdienste) einen **direkten Online-Abgleich von Fingerabdrücken und DNA-Körperproben mit deutschen Datenbanken ermöglichen** soll. Außerdem sollen deutsche Behörden den USA ungefragt melden dürfen, welche Personen sie der Beteiligung an oder Planung von terroristischen Aktivitäten verdächtigen."

<http://deinedatendeinemacht.wordpress.com/2008/03/11/datenaustausch-mit-den-usa-ohne-datenschutz> : "Heute wurde ein Vertrag zwischen Deutschland und den USA unterzeichnet, der weitreichenden Datenaustausch vorsieht. Es geht dabei um folgende Daten:
Name, Geburtsdatum

Staatsangehörigkeit
Fingerabdrücke
DNA-Profile

Nicht nur die Daten von Schwerverbrechern können dabei **von 17'000 amerikanischen Behörden online abgerufen** werden, sondern jeder erkennungsdienstlich erfasste Bürger. Dies umfasst z.B. auch Asylbewerber, bei Demonstrationen erfasste Bürger oder Visumantragssteller. Die (in amerikanischen Behörden gespeicherten) **Daten deutscher Bürger unterliegen dabei keinem Datenschutz, denn das amerikanische Datenschutzgesetz bezieht sich explizit nur auf Daten von Inländern**. Zudem enthält der neu geschlossene Vertrag kaum konkrete Datenschutzbestimmungen und sieht keine unabhängige Datenschutzkontrolle vor."

Hier geht es um das "Gesetz zu dem Abkommen vom 1. Oktober 2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität". Stellvertretend ein kleiner Auszug aus der Parlamentsdebatte im Deutschen Bundestag vom 28.5.2009 (unter <http://dipbt.bundestag.de/dip21/btp/16/16224.pdf#P.24752>):

Abgeordnete Gisela Piltz (FDP): "Schon vor über einem Jahr hat die FDP-Fraktion die Bundesregierung nachdrücklich dazu aufgefordert, in Nachverhandlungen zu dem Abkommen mit den Vereinigten Staaten einzutreten, um insbesondere umfassende Datenschutzregelungen zu implementieren, eine gemeinsame Definition terroristischer Straftaten bzw. schwerwiegender Kriminalität aufzunehmen, den Zugriff auf Fingerabdruckdaten von Asylbewerbern oder Ausländern nach dem Aufenthaltsgesetz auszuschließen und den Rechtsschutz ausreichend zu gewährleisten. **Nichts davon ist in den vorgelegten Gesetzentwürfen auch nur ansatzweise angegangen worden.**"

Abgeordneter Jan Korte (DIE LINKE): "Es enthält Regelungen für den automatisierten Abruf von DNA- und Fingerabdruckdaten sowie den Austausch von Daten terrorverdächtiger Personen. **Mit diesem Abkommen sollen personenbezogenen Daten, darunter DNA-Daten, einer unbegrenzten Zahl US-amerikanischer Sicherheitsbehörden, darunter Geheimdiensten jeder Art, zugänglich gemacht werden. Via Onlinezugriff werden Datenbanken deutscher Sicherheitsbehörden für US-Geheimdienste und Sicherheitsbehörden geöffnet. Datenschutzvorkehrungen oder bürgerrechtliche Aspekte wie eine Begrenzung der zu übermittelnden Daten oder eine Begrenzung der Speicherfristen sowie eine wirkliche Zweckbindung sind hierin nicht vorgesehen.** Das Abkommen zeichnet sich vielmehr durch eine völlig haltlose Unverhältnismäßigkeit, mangelnde Bestimmtheit, unzureichende Zweckbindung, fehlende Sicherungen oder effektiven Rechtsschutz aus. So werden neben Namen und Geburtsdaten auch Identifikationsnummern und Fingerabdrücke gespeichert und ausgetauscht. Mehr noch: Über den Umweg des Abkommens sollen nunmehr nicht nur in den USA, sondern auch in der Bundesrepublik Informationen über „die Rasse oder ethnische Herkunft, politische Anschauungen, religiöse oder sonstige Überzeugungen oder die Mitgliedschaft in Gewerkschaften, die Gesundheit und das Sexualleben“ gespeichert werden. **Das ist der grundrechtspolitische Dambruch.**"

Abgeordneter Wolfgang Wieland (BÜNDNIS 90/DIE GRÜNEN): "Im März 2008 hat Herr Schäuble stolz diesen Vertrag präsentiert. ... Und so ist es auch mit diesem Abkommen, einem Abkommen übrigens, zu dem es bei seinem Bekanntwerden im März 2008 heftige Kritik von allen Seiten gab. Der Innenausschuss hat den Bundesinnenminister damals auf die Defizite und Ungereimtheiten hingewiesen, Nachverhandlungen an bestimmten Punkten verlangt und eine Information des Parlamentes gefordert. **Nichts davon hat Herr Schäuble erfüllt!**"

Die Chronologie dieser Gesetzesvorlage findet man unter <http://dipbt.bundestag.de/extrakt/ba/WP16/193/19380.html>. Im Juli 2009 entschied der deutsche Bundesrat, dass die Bundesregierung mit den USA Nachverhandlungen aufnehmen muss mit dem Ziel der Festlegung verbindlicher Begriffsdefinitionen sowie der Verbesserung des Datenschutzniveaus, weil der aktuelle Gesetzesentwurf in vielfacher Hinsicht (Verletzung Persönlichkeitsschutz, Datenschutz usw.) ungenügend ist (siehe <http://dipbt.bundestag.de/dip21/brd/2009/0637-09B.pdf>). Wolfgang Schäuble ist somit mit seinem Versuch (vorerst zumindest) gescheitert, das ganze Abkommen hinter dem Rücken des Parlaments still und leise durchzubringen und die Grundrechte der deutschen Bürger an die USA zu verkaufen.

Auch die Schweizer Regierung ist drauf und dran, den gleichen Fehler zu begehen:

<http://www.drsl.ch/www/de/drs1/sendungen/samstagsrundschau/142094.schweiz-soll-heikle-daten-mit-der-eu-austauschen.html> : "14.9.2009. **Schweiz soll heikle Daten mit der EU austauschen.** Grundsätzlich ist der Bundesrat daran interessiert, beim europäischen DNA-Datenaustausch mitzumachen. Dies bestätigte Eva Zwahlen vom Bundesamt für Polizei gegenüber Schweizer Radio DRS. Der Bundesrat ist am Austausch sensibler Daten mit anderen europäischen Ländern interessiert und prüft eine Unterzeichnung des sogenannten Vertrags von Prüm, bei dem 14 EU-Staaten mitmachen. Der Vertrag ermöglicht den Polizeibehörden **grenzüberschreitend Zugriff auf die gesamten DNA- und Fingerabdruck-Daten der Mitgliedstaaten.** ... Schengen greift weniger weit. Der Vertrag von Prüm geht weiter als der Vertrag von Schengen, bei dem die Schweiz bereits mitmacht. Mit Schengen werden nur Fahndungsdaten ausgetauscht. Beim Vertrag von Prüm geht es um **die gesamten Datenbanken mit DNA-Profilen und Fingerabdrücken.** ... Mit dem Vertrag von Prüm könnten Polizisten **aus 14 EU-Staaten diese sensiblen Daten abrufen.**"

Der beste Datenschutz in der Schweiz nützt nichts, wenn ausländische Behörden Zugriff auf diese Daten erhalten. Was diese mit den abgerufenen Daten auf der anderen Seite der Landesgrenzen machen, kann niemand mehr kontrollieren. Im schlimmsten Fall unterliegen diese Daten dort gar keinem Datenschutz mehr, wie im Fall der USA, denn das amerikanische Datenschutzgesetz bezieht sich explizit nur auf Daten von Inländern. Zudem: Wer wird in Zukunft sonst noch alles Zugang zu den privaten Daten auf solchen zentralen Datenbanken erhalten? Wir haben keine Ahnung, wer in zehn Jahren die Herrschaftshoheit in den diversen Staaten haben wird. Wer meint, er habe ja nichts zu verbergen: Unter falschem Regime reicht es, eine abweichende Meinung zu haben, "die die Staatssicherheit gefährdet". In vielen Staaten gilt leider: "Es ist gefährlich, Recht zu haben, wenn die Regierung Unrecht hat."

Doch es gibt für Regierungen, Geheimdienste und Verbrechenorganisationen diverse weitere Möglichkeiten, wie man an die wertvollen biometrischen Daten von unschuldigen Bürgern anderer Staaten herankommen kann, denn:

8. Biometrische Daten von Unschuldigen sind u.a. für Visumsfälscher sehr wertvoll

<http://www.tagesspiegel.de/zeitung/Die-Dritte-Seite;art705,2004254> : "11.2.2007. Fälschungssicher, Missbrauch ausgeschlossen: die Worte des Staates bei der Einführung des elektronischen Ausweises. Er hat unrecht. Lukas Grunwald wollte sich irren. Er wollte, dass sein Experiment fehlschlug. Dann werde alles gut, hoffte er. Aber Lukas Grunwalds Versuch gelang. Es dauerte exakt 4,80 Sekunden. Den Ablauf hat er protokolliert, auf die Hundertstelsekunde in einer Datei auf seinem Rechner gespeichert. ... „Dass es so einfach ist, hätte ich nicht gedacht“, sagt er zu seinem Kollegen Christian Böttger, der neben ihm im Büro seiner Computerfirma steht. Die beiden haben in einer unscheinbaren Hildesheimer Wohnstraße etwas vollbracht, was nach Angaben der Bundesregierung eigentlich unmöglich ist: die Daten eines deutschen Reisepasses aus der Innentasche eines Sakkos zu stehlen, ohne den Pass zu sehen und ohne ihn zu berühren. Christian Böttger, 46, trägt einen Bart und einen Dokortitel der Physik. Für gewöhnlich lässt er sich nicht leicht aus der Ruhe bringen, aber nun ist er nervös; als er den Pass aus der Anzugjacke holen will, verhakt er sich im Futter. „Jeder Datendieb kann das nachmachen“, sagte er. ... Grunwald **kann sich nicht vorstellen, dass ein Schwarzmarkt für biometrische Daten lange auf sich warten lässt. Ein Grund: Ausländer, die ein Visum für die Bundesrepublik beantragen, werden "biometrisch identifiziert": Foto und Fingerabdruck werden mit den Datenbanken der Polizei abgeglichen. Biometrische Daten von Unschuldigen werden für Visumsfälscher da schnell wertvoll.**"

9. Gefahr von Hackerattacken auf die Bundesverwaltung und andere behördliche Datenbanken

http://www.parlament.ch/ab/frameset/d/n/4812/314116/d_n_4812_314116_314136.htm?DisplayTextOid=314137 : "Kiener Nellen Margret (S, BE): ... Dieser wichtigen Kommissionsinitiative haben wir in diesem Rat letzte Woche mit einer grossen Mehrheit Folge gegeben. ... Es geht um eine Prüfung der Erweiterung dieser Datenbank, nachdem die Bundesverwaltung gerade in den letzten Monaten von einer noch nie dagewesenen Hackerattacke betroffen war - eine Hackerattacke, vor der der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte im Vorfeld der Abstimmung zur Biometrie sehr gewarnt hatte.

Nun ist es möglich, auch diesen Bedenken noch Rechnung zu tragen."

<http://www.20min.ch/news/schweiz/story/13257549> : "26.10.2009. **Hackerangriff. Virenattacke auf das Aussendepartement.** Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) von Bundesrätin Micheline Calmy-Rey ist Ziel einer Virenattacke geworden. ... Es habe sich um eine sehr professionelle Virenattacke mit einer besonderen Software gehandelt, sagte EDA-Sprecher Georg Farago am Montag gegenüber der Nachrichtenagentur SDA. Damit hätten gezielt Informationen beschafft werden sollen. Die Schadsoftware war äusserst gut versteckt und verursachte praktisch keine wahrnehmbaren Störungen in der IT-Infrastruktur. Der Angriff wurde am vergangenen Donnerstag, 22. Oktober entdeckt. ... Neben dem Informatikdienstleister des EDA sind auch das Bundesamt für Informatik und Technologie (BIT) sowie die Melde- und Analysestelle Informationssicherung (Melani) des Bundes daran beteiligt. Die Informatiker sind seit Freitag ununterbrochen im Einsatz. Wie die Virensoftware auf die Computer gelangen konnten und ob bestimmte Abteilungen Ziel der Attacke waren, wollte Farago nicht sagen. Ebenso wenig äusserte sich der EDA-Sprecher über die mögliche Herkunft der Virenattacke. ... Bereits am Freitag hatte eine Störung die Computer des Eidgenössischen Departements des Innern (EDI), des Eidgenössischen Finanzdepartements (EFD) und des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) lahm gelegt. Es gebe aber keinen Zusammenhang zur Attacke auf das EDA, sagte Karolina Kohout, stellvertretende Pressesprecherin des BIT, gegenüber 20 Minuten Online. ... Das EDA war zusammen mit dem Staatssekretariat für Wirtschaft (Seco) bereits Ende 2007 Opfer eines Hacker-Angriffs geworden. Mitarbeiter des EDA und des Seco hatten in zwei Wellen über 500 E-Mails erhalten, die auf einen vermeintlichen Fotowettbewerb hinwiesen. Klickten die Mitarbeiter dort auf ein Foto, um ihre Stimme für den Wettbewerb abzugeben, luden sie einen Trojaner herunter, der Spionageprogramme nachlädt und ausführt. Das schädliche Programm wurde damals von den gängigen Virencannern nicht erkannt."

<http://www.20min.ch/news/schweiz/story/31676245> : "21.05.08. **Bundesbeamte tappen in die Hackerfalle.** Womöglich ein ausländischer Geheimdienst steckt hinter einer grossangelegten Hackerattacke auf das EDA und das SECO von Ende letzten Jahres. Getarnt war die Aktion als Fotowettbewerb. Jetzt ermittelt die Bundeskriminalpolizei. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) und das Staatssekretariat für Wirtschaft (SECO) haben den Angriff bestätigt, wie Radio DRS berichtet. Die Bundeskriminalpolizei macht wegen Verdachts auf Spionage polizeiliche Vorabklärungen. ... Noch ist nicht klar, ob bei dem Angriff geheime Daten geklaut wurden. Brisant ist, dass die Aktion zwei Bundesstellen traf, die unter anderem bei der Exportkontrolle für Waffen über sensible Daten verfügen. Das Vorgehen der unbekanntenen Täter war so raffiniert wie professionell. Mit E-Mails und gefälschten Internetseiten wurde ein Fotowettbewerb vorgegaukelt. **Mehrere Angestellte der Bundesverwaltung taptten blind in die Hackerfalle. Sie installierten so eine Software, die Computer und Netzwerk ausspioniert.** Die Verantwortlichen sind beunruhigt. «Was die Professionalität der Täter anbelangt, die den Fokus auf ganz bestimmte Teile der Bundesverwaltung legten, und die ganze technische Infrastruktur die aufgebaut werden musste - unter diesen Gesichtspunkten ist dies ein einzigartiger Fall», sagt Marc Henauer von der Nationalen Koordinationsstelle zur Bekämpfung der Internetkriminalität (MELANI) auf Radio DRS. Das SECO war nach Angaben seiner Sprecherin Rita Baldegger vom Hacker-Angriff «praktisch nicht betroffen». Nur rund ein halbes Dutzend Mitarbeitende hätten die betreffenden E-Mails geöffnet. ... Die E-Mail-Nachrichten waren personalisiert, das heisst mit der korrekten Anrede des Empfängers versehen. Der gefälschte Absender war eine Bundesstelle, die auf einen Fotowettbewerb hinwies. Um daran teilzunehmen, wurde man dazu aufgefordert, einen in der E-Mail enthaltenen Link anzuklicken. Tat man dies, so öffnete sich im Web-Browser eine täuschend ähnliche Kopie der Website besagter Bundesstelle. Unter der Rubrik Fotowettbewerb wurden verschiedene Fotos gezeigt. Durch Anklicken konnte man dem Foto seiner Wahl die Stimme geben. Dadurch lud man sich eine Screensaver-Datei auf den Computer, die Malware enthielt. Die Art des Angriffs lässt gemäss MELANI auf eine professionelle und mit einigen finanziellen und technischen Ressourcen ausgestattete Täterschaft schliessen. Die eingesetzte Malware sei vorerst durch keine gängige Antiviren-Software erkannt worden. Gezielte Spionage via Internet bleibe von grosser Aktualität, heisst es im MELANI-Bericht. Diese basiere auf politischen, militärischen und wirtschaftlichen Interessen. Bei den Angreifern könne es sich um staatlich unterstützte oder auch um einzelne oder organisierte Akteure handeln. Im Visier seien Regierungssysteme, insbesondere Informationen zu Verteidigungs- und Aussenpolitik."

<http://wiso.zdf.de/ZDFde/inhalt/9/0,1872,7510025,00.html> : "2.2.2009. **Fingerabdruckscanner ist unsicher. Reisepass: Hacker können Schwachstellen ausnutzen.** Mehr Sicherheit - das war das Argument für den elektronisch lesbaren Reisepass. Auf einem Chip sind zum Passfoto auch zwei Fingerabdrücke

gespeichert. **Doch die Übertragungstechnik ist nicht sicher, Hackern bieten sich Angriffsmöglichkeiten, und auch der Bundesdatenschutzbeauftragte ist besorgt.** Eine Situation, mit der jeder Bundesbürger konfrontiert ist: Beim Antrag für den neuen Reisepass müssen alle Deutschen ihren Fingerabdruck abgeben. Gunnar Porada hat diese Prozedur hinter sich und entdeckt: Die Daten sind nicht ausreichend geschützt. Der Computer-Sicherheitsexperte, der professionell Unternehmen auf Schwachstellen in ihren Netzwerken überprüft, **könnte ohne großen Aufwand in den Behördenrechner eindringen, die Fingerabdrücke mitlesen und manipulieren.** Kriminellen bieten sich dadurch ungeahnte Möglichkeiten: "Letztlich hebeln wir damit die Sicherheit aus, die wir uns eigentlich mehr erhoffen durch die Fingerabdrücke", sagt Porada: "Wenn ich selber ein Schwerekrimineller wäre, könnte ich meine Fingerabdrücke im Reisepass von einer mir ähnlich aussehenden Person eintragen. Dann könnte ich mit seinen Daten reisen, ich würde seinen Namen und Identität annehmen, würde somit an allen Grenzposten vorbeikommen." ... **Sicherheitslücken in Behördenrechnern seien, wie bei allen Computern, nicht die Ausnahme,** erklärt Gunnar Porada."

Und so weiter... Man könnte mit zusätzlichen Beispielen solcher (erfolgreichen) Hackerattacken stundenlang weiterfahren. Einige weitere Musterchen (allein aus den Jahren 2008 und 2009), wo Hacker geheime Daten von Regierungsdatenbanken klauen konnten (z.B. **"Hacker knacken das teuerste Waffenprojekt der USA auf dem Pentagon-Computer"** oder **"Ein chilenischer Hacker hat sich Zugang zu über sechs Millionen Daten seiner Regierung verschafft"** oder **"Jobbörse Monster werden bei einem Hackerangriff 4,5 Millionen Datensätze ihrer Kunden gestohlen inklusive Nutzer-IDs und Passwörter, E-Mail-Adressen, Namen und Telefonnummern"** usw.), findet man unter <http://www.freiheitskampagne.ch/rfid-datenbanken-sind-besonders-gefährdet/>

10. Gefahr durch Diebstahl und Weiterverkauf der biometrischen Daten durch eigene Mitarbeiter

Auch Beispiele solcher Fälle gibt es bereits genug, z.B. bei Bankkontodaten:

<http://www.blick.ch/news/wirtschaft/daten-dieb-ich-wurde-von-agenten-verschleppt-136361> : "22.12.2009. Datenklauer Hervé Falciani (37). Daten von 130 000 soll er der Genfer Privatbank HSBC geklaut haben, darunter 3000 Franzosen. Er soll zusammen mit seiner franko-libanesischen Geliebten Georgina Mikhael (35) versucht haben, die Ware an andere Banken zu verkaufen. Unter anderem im Februar 2008 im Libanon. Als keine Bank kaufte, soll er die Daten dem deutschen und dem französischen Geheimdienst angeboten haben."

<http://www.blick.ch/news/wirtschaft/so-plante-frankreichs-meili-seinen-coup-136118> : "18.12.2009. Der HSBC-Datendieb. So plante Falciani seinen Coup. Der Informatiker Hervé Falciani (37) klaute Kundendaten bei der britischen Privatbank HSBC in Genf. Dabei überliess er nichts dem Zufall. Der HSBC-Angestellte Hervé Falciani bereitete seinen Coup genau vor. Anders als der Wachmann Christoph Meili, dem bei der Schweizerischen Bankgesellschaft heisse Akten in die Hände fielen, schlug der Informatiker in seiner Bank bewusst zu. Mit dem Ziel, Kundendaten zu Geld zu machen."

<http://www.welt.de/wirtschaft/article5474439/Bankmitarbeiter-klaut-Daten-von-Steuersuendern.html> : "9.12.2009. Der Fall erinnert an Deutschlands Steuerstreit mit Liechtenstein. Ein Archivar der fürstlichen Liechtensteiner Bank LGT hatte dem Bundesnachrichtendienst für 4,5 Mio. Euro Kontodaten verkauft. Dies hatte 2008 zu spektakulären Ermittlungen gegen etwa 700 deutsche Steuersünder geführt."

<http://www.vaterland.li/index.cfm?ressort=wirtschaft&source=lv&id=6507> : "9.12.2009. Bankdaten in Genf geklaut. Der Kieber der Schweiz heisst «Antoine». Nun hat auch die Schweiz ihren Fall Kieber: Ähnlich wie in Liechtenstein, wo Heinrich Kieber, ein Angestellter der LGT Treuhand, Kundendaten entwendete und ins Ausland verschacherte, soll ein Beschäftigter der HSBC Privat Bank in Genf Tausende Kontodaten entwendet und der französischen Steuerfahndung übergeben haben."

<http://www.sueddeutsche.de/wirtschaft/775/433524/text/> : "19.2.2008. In der Affäre um Steuerhinterziehung ist der Informant des Bundesnachrichtendienstes (BND) angeblich enttarnt worden. Die amerikanische Zeitung Wall Street Journal nennt den vollen Namen eines Mannes, der sich inzwischen nach Australien abgesetzt haben soll. Dem Blatt zufolge hat der Mann einst für das Liechtensteiner Bankhaus

LGT gearbeitet und dabei Daten über Hunderte Kunden mitgenommen. In den vergangenen 18 Monaten soll der Mann seine Informationen den Steuerbehörden "auf mehreren Kontinenten" angeboten haben, unter anderem in den USA. Die Zeitung nennt als Quelle eine Person, "die mit der Sache vertraut ist". Einer der Autoren des Artikels, David Crawford, sagte bei N24, auch die US-Behörden hätten Daten gekauft und arbeiteten seit einigen Monaten damit. ... Der BND hatte dem Mann 4,2 Millionen Euro für die CD mit Kontodaten von mutmaßlichen Steuerflüchtlern gezahlt."

11. Gefahr durch simplen Datenverlust durch eigene Mitarbeiter

<http://info.kopp-verlag.de/news/der-fluch-des-fortschritts-alle-daten-ueber-kriminelle-sind-in-grossbritannien-weg.html> : "23.8.2008. In Großbritannien sind alle Daten über Kriminelle abhanden gekommen. Während man in **Deutschland über den illegalen Handel mit den Daten von Millionen unbescholtenen Bürgern** diskutiert, erlebt Großbritannien einen Super-GAU. **In London sind die Daten von 130'000 Kriminellen abhanden gekommen. Sie sind einfach weg.** Und nun hat man Panik. In Deutschland gibt es einen »Skandal« um die Weitergabe personenbezogener Daten. Das ist bekannt. Und die Politiker beschäftigen sich mit dem Fall. Wirtschaftsminister Michael Glos brachte ein vollständiges Handelsverbot von personenbezogenen Daten ins Gespräch, die Justizministerin Brigitte Zypries will die Gewinne der Datenhändler abschöpfen. Solche Vorschläge sind politischer Alltag. Was aber macht man, wenn brisante Daten nicht verkauft werden, sondern einfach verschwinden? In Großbritannien ist ein USB-Stick mit den Daten von 84'000 Häftlingen, 10'000 Schwerverbrechern und zehntausenden weiteren Daten Krimineller einfach verloren gegangen. Man hat nun Angst davor, dass zehntausende Häftlinge die Regierung auf Schadensersatz verklagen. Denn die Daten sind auf dem USB-Stick nicht verschlüsselt. Und ein jeder Finder des USB-Sticks hätte den freien Zugriff auf alle Datensätze. Da gibt es Datensätze über Sexualstraftäter, Datensätze über potentielle Terroristen und Datensätze über Personen, die observiert werden. Der britische Telegraph berichtet nun, dass der britische Steuerzahler wohl nun jedem Kriminellen, der wegen der Datenschlamperei ein Gerichtsverfahren anstrengt, Schmerzensgeld zahlen müsse, weil Rechte verletzt und die Datensicherheit grob fahrlässig gehandhabt worden sei. **Dummerweise reiht sich der peinliche Vorfall ein in eine Reihe ähnlicher Vorkommnisse. Seit 2003 werden nun mindestens 88 USB-Sticks mit geheimen oder streng vertraulichen Daten bei den Regierungsbehörden vermisst.** Nun sollten deutsche Leser nicht hochmütig über die Datenschlamperei der Briten lächeln. Denn ganz zaghaft kommen in diesen Tagen Meldungen an die Öffentlichkeit, dass es solche Datenschlampereien auch in deutschen Justizkreisen gibt, Beispiel **Rheinland-Pfalz: Dort sind persönliche Daten aus der Jugendstrafanstalt Schifferstadt auf der Straße gefunden worden.** Ein Pfortenbuch mit den Namen von mehr als 150 Anwälten, rund 200 jugendlichen Häftlingen und zahlreichen Ermittlern geriet in die falschen Hände. In dem Kalender seien Besuche von Anwälten bei ihren Mandaten vermerkt worden, heißt es. Man hatte die Unterlagen nicht korrekt entsorgt."

Und so weiter, und so weiter... Man könnte mit weiteren Beispielen auch hier stundenlang weiterfahren. Einige weitere Musterchen (allein aus den Jahren 2008 und 2009), wo Mitarbeiter des Staates geheime Daten ganz einfach irgendwo in der Öffentlichkeit verloren haben (z.B. **"Das britische Innenministerium hat jüngst einen Laptop bei Ebay verkauft inklusive vertraulicher Daten aus dem Ministerium mit unverschlüsselten Daten von 25 Millionen Kindergeldempfängern inklusive deren Bankverbindungen."** oder **"Britische Behörden verlieren Daten von 3 Millionen Führerscheinanwärtern"** oder **"Bank of Ireland verliert 31'000 Kundendatensätze"** oder **"US-amerikanische Bank of New York Mellon verliert Magnetband mit 4,5 Millionen Kundendaten"** usw.), findet man unter <http://www.freiheitskampagne.ch/rfid-datenbanken-sind-besonders-gefaehrdet/>

=> Fazit: Bei einem Verzicht auf das Obligatorium der zentralen Datenspeicherung würde das schweizerische Ausweiswesen nicht etwa geschwächt, sondern die Schweiz schützt sich im Gegenteil dadurch staatspolitisch vor dem grossen Gefahrenpotential einer solchen zentralen Datenspeicherung der biometrischen Daten ihrer eigenen Bürgerinnen und Bürger. Genauso wie dies mit Ausnahme von vier alle anderen Staaten weltweit machen, die auf diese zentrale Datenspeicherung verzichten. Von den Aufbau- und Unterhaltskosten ganz zu schweigen. Die Gefahr von Erpressungen, Hackerattacken, Datenverkauf durch Mitarbeiter, Datenverlust beim Transport usw. kann die Schweiz nur verhindern, indem sie gar keine Biometrie-Datenbank betreibt. Die simpelste Regel des Datenschutzes lautet bekanntlich: Erst gar keine Datenbank erstellen. Das beugt Hackerangriffen und Missbrauch am Effizientesten vor.