

E-Pass: Das Ende von Schengen oder Weg in den Überwachungsstaat?

Seit dem 11. September hat sich die Diskussion um die öffentliche Sicherheit verschärft. Die globale Einführung von Pässen mit biometrischen Merkmalen ist ein Ergebnis dieser Entwicklung. Und obwohl bisher mehr als 60 Staaten solche Reisedokumente einführen, ist deren Notwendigkeit bis heute nicht abschliessend geklärt. *Christian Walter*

Am 17. Mai stimmen die Schweizer Bürger über die geplante Änderung des Ausweisgesetzes ab. Dabei geht es vor allem um die Einführung des neuen «Pass 10» – auch bekannt als E- oder Biometrie-Pass. Dessen Gegner fürchten um den Verlust von Privatheit und Datenschutz und sehen in den mit der Einführung einhergehenden Massnahmen einen weiteren Schritt in Richtung Überwachungsstaat. Die Befürworter des E-Passes empfinden diese Argumente vor allem als paranoid, ein Nein an der Urne könne die Reisefreiheit gefährden und das Ende von Schengen-Dublin bedeuten. Somit mahnen beide Seiten extreme Konsequenzen an, wobei sich die Diskussion auf einer technischen und einer politischen Ebene erstreckt.

Wie stark sind die technischen Mängel des E-Passes?

Stein des Anstosses aus technischer Sicht ist vor allem der im Pass enthaltene RFID-Chip. Theoretisch ermöglicht er die Fernabfrage der in ihm gespeicherten Personendaten und schürt damit die Angst vor dauernder Überwachung, unberechtigtem Zugriff durch Dritte sowie Identitätsdiebstahl. Dies nicht zuletzt deshalb, da es immer wieder Berichte zu gefälschten und gehackten E-Pässen gibt. Erst vor kurzem demonstrierten amerikanische Wissenschaftler die Anfälligkeit von US-Passport Cards, die aus einer Entfernung von 50 Metern ausgelesen und geklont wurden. Dennoch darf man diese Meldungen auch nicht überbewerten, da E-Pass nicht gleich E-Pass ist. Nicht zuletzt auch aufgrund der Erfahrungen in anderen Ländern war man hierzulande bemüht, nicht dieselben Fehler zu begehen (siehe Tabelle).

Zwar kann ein Verlust der Personendaten, des biometrischen Fotos oder der biometrischen Fingerabdrücke nicht vollständig ausgeschlossen werden, dennoch sind die genannten Datengruppen mit Abstufungen verhältnismässig sicher. Mit Ausnahme der BAC werden

die in ihm steckenden Kryptoverfahren sogar von Mitgliedern des Chaos Computer Clubs als relativ sicher bewertet.

Die Aussagekraft von biometrischen Daten wird kritisch betrachtet

Dennoch tauchen Plausibilitätsüberlegungen an anderer Stelle auf. So zum Beispiel bei der Aussagekraft der biometrischen Daten. Verschiedene Studien des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Deutschland stellen deren Nützlichkeit in Frage. «Gemäss der BioP-II-Studie wiesen die getesteten Verfahren zwischen 3 und 23 Prozent der teilnehmenden Personen fälschlich zurück. Dabei sind Teile des Berichts noch immer unter Verschluss», so Frank Rosengart, Sprecher des Chaos Computer Clubs. Besonders betroffene Gruppen sind zum Beispiel Senioren, bei denen ein gewisser Prozentsatz einfach keine verwertbaren Fingerabdrücke mehr hat. Eine andere Problemgruppe sind Menschen, die viel mit den Händen arbeiten oder mit chemischen Substanzen in Berührung kommen. Diese Personen wären in Zukunft einer verstärkten Diskriminierung ausgesetzt, eine Gefahr, auf die auch schon das Bundesamt für Polizei hingewiesen hat. Dennoch geht das Fedpol heute davon aus, dass die Biometrie zuverlässig funktioniert. «Mit dem in E-Pässen elektronisch gespeicherten Foto und den Fingerabdrücken kann zuverlässig festgestellt werden, dass der Pass und die Person, die ihn vorweist, zusammengehören», so Guido Balmer, stellvertretender Informationschef des Eidgenössischen Justiz- und Polizeidepartements (EJPD). Somit ist der Schweizer Pass zwar kein perfektes, aber ein nach heutigem Stand der Technik sehr sicheres Dokument. Nichtsdestotrotz wird dies durch die rapide technische Entwicklung laufend in Frage gestellt, vor allem wenn man die Gültigkeitsdauer des PASSES von zehn Jahren betrachtet. In Bezug auf die

technische Entwicklung ist das eine Ewigkeit. Dabei wird gern aussen vor gelassen, dass es keine Garantie dafür gibt, dass die Antenne des RFID-Chips auch so lange funktioniert. Auch ist unklar, wer die Kosten für einen Ersatz tragen muss.

Das Ende des Schengen-Abkommens

Die Diskussion um den E-Pass beschränkt sich allerdings nicht nur auf die technische Sicherheit des Dokuments. So stellt sich auch die Frage, ob sich die Schweiz überhaupt auf den E-Pass hätte einlassen sollen. Fakt ist, dass die Schweiz im Rahmen von Schengen-Dublin jegliche EU-Rechtsfortbildung übernehmen muss, wenn sie am Rechtssystem angeschlossen bleiben will. «Da die Schengen-Staaten die Einführung biometrischer Pässe beschlossen haben, ist somit auch die Schweiz dazu verpflichtet», so Daniel Brühlmeier, Mitglied des Vereins Unser Recht. Deshalb sehen die Befürworter des E-Passes hier auch ein Risiko für die Schweiz, da aufgrund eines Neins an der Urne der Schengen-Vertrag aufgelöst werden könnte.

Die Gegner des biometrischen PASSES sehen das allerdings anders. Wohl auch nicht ganz unberechtigt, da es tatsächlich Sonderregelungen für einige Länder beim Thema E-Pass im Rahmen des Schengen-Abkommens gibt, und zwar für England, Dänemark und Irland. Auch sehen sie das Abkommen nicht gefährdet: Der Stichtag für die Einführung des E-Passes ist der 1. März 2010. Sollte dieser also abgelehnt werden, hat die Schweiz fast ein Jahr Zeit, eine Alternative zum aktuellen Vorschlag zu suchen. Erst die Nichteinhaltung dieser Frist würde die Schweiz zwingen, innerhalb von weiteren 90 Tagen eine Übergangslösung zu vereinbaren. Erst wenn bis dahin immer noch keine Lösung gefunden wurde, besteht die Gefahr eines Ausschlusses vom Schengen-Abkommen. Insofern gibt es

Unterschiede zur letzten Abstimmung in Bezug auf die Personenfreizügigkeit.

Die Gesetzesänderung geht über den E-Pass hinaus

Natürlich lässt sich die Einführung des E-Passes nicht auf die EU-Raum reduzieren. Vielmehr handelt es sich um eine globale Entwicklung. Mittlerweile haben 62 Länder einen solchen Pass eingeführt. Allen voran die USA, die mittlerweile verlangen, dass alle nach dem Oktober 2006 ausgestellten Pässe ein elektronisch gespeichertes Gesichtsbild enthalten. Somit geht es beim E-Pass nicht nur um eine Einigung mit der EU. Die internationale Entwicklung scheint momentan in die Richtung zu weisen, dass in Zukunft kein Weg mehr an der Einführung eines solchen Dokuments vorbeiführt, will ein Land seinen Bürgern Reisen ins Ausland ohne grossen Aufwand ermöglichen. Dennoch geht es bei der anstehenden Abstimmung nicht einfach um die Frage E-Pass ja oder nein. Viele der Gegner der Änderung des Ausweisgesetzes sind nämlich nicht einfach gegen den E-Pass. Ein Blick auf die Website der Freiheitskampagne genügt, um das breite Spektrum der Kritiker auszumachen. Es gibt wahrscheinlich wenige Themen, bei denen die Schweizer Demokraten auf derselben Seite stehen wie die Alternative Liste – ganz zu schweigen von SP und SVP. Viele der Mitglieder dieser schon mal als unheilig bezeichneten Allianz stören sich nicht so sehr am E-Pass als an den mit ihm verbundenen flankierenden Massnahmen: Gemeint ist die Aufnahme der Fingerabdrücke in die ISA-Datenbank (Informationssystem Ausweisschriften) sowie die Option, auch die IDs in Zukunft mit biometrischen Daten zu versehen. Beide Punkte werden nicht von der EU gefordert, sondern vom Bundesrat.

Datensammlungen können politisch umgenutzt werden

Das ISA existiert bereits seit 2003 und dokumentiert, wer welchen Ausweis mit welchen Daten erhalten hat. Zu diesem Zweck beinhaltet das ISA zurzeit die Personalien sowie das Foto des Ausweisinhabers. Diese sollen im Rahmen der Änderung des Ausweisgesetzes nun durch zwei biometrisch erfasste Fingerabdrücke ergänzt werden. Der Bund

verspricht sich davon zweierlei. Damit soll vermieden werden, dass sich jemand unter Vortäuschung einer falschen Identität (65 dokumentierte Vorfälle seit 2003 bei insgesamt 3,9 Millionen Pässen) einen zweiten Ausweis ausstellen lässt. Ausserdem sollen so verlorengegangene Reisedokumente im In- und Ausland leichter ersetzt werden können. Momentan werden etwa 13 000 Schweizer Pässe im Jahr als verloren oder gestohlen gemeldet.

Kritik an der Datenbank kommt indes nicht nur von den Gegnern des E-Passes, sondern auch vom Zürcher Datenschutzbeauftragten Bruno Baeriswyl sowie dem Eidgenössischen Datenschutzbeauftragten Hanspeter Thür. Beide äusserten sich entsprechend in der NZZ. Demnach ist die Fälschungsgefahr schon durch den direkten Vergleich der Fingerabdruckdaten mit dem Fingerabdruck der Person stark vermindert. Mehr würde auch im Schengen-Recht nicht verlangt. Ausserdem weckten zentrale Datenbanken rasch neue Bedürfnisse, etwa bei der Fahndung. Dies vor allem, da eine Rasterfahndung mithilfe der ISA-Datenbank erst durch die Zugabe der Fingerabdruckdaten möglich wird. Darüber hinaus sei so eine Datensammlung ein interessantes Ziel für Hacker. Zwar ist der Einsatz der Personendaten zu Fahndungszwecken momentan gesetzlich verboten, dennoch ist die Umnutzung eines einmal geschaffenen Instruments politisch wesentlich einfacher, als ein neues Instrument zu schaffen. Solche Befürchtungen sind dabei alles andere als unbegründet. Ähnliches geschah vor kurzem in Deutschland mit der Umnutzung der Mautdaten zu Fahndungszwecken. Und auch Datenverluste, ob durch Cyberkriminelle oder einfach durch schlampige Arbeit oder Unachtsamkeit sind mittlerweile an der Tagesordnung. Die englische Regierung dürfte hier in den letzten Jahren den eigenen Rekord öfters gebrochen haben.

Dabei geht es nicht einmal nur um das Vertrauen in die Kompetenz der eigenen Regierung oder ihrer ausführenden Organe, denn der Bundesrat ist aufgrund der aktuellen Gesetzesformulierung berechtigt, die Daten an fremde Regierungen und private Unternehmen weiterzugeben. Darüber hinaus kann ein Datenverlust auch Konsequenzen in Bereichen jenseits von Pässen und Reisen haben. Biome-



Bildquelle: Fotolia

► trische Daten erfreuen sich zurzeit grosser Beliebtheit als Sicherheitsfaktoren zum Beispiel bei Zutrittsbeschränkungen zu bestimmten Zonen, Log-ins für Computersysteme und Ähnlichem. Ein Verlust der im Pass gespeicherten Daten, sei es durch illegales Auslesen aus einem einzelnen Pass oder durch Verluste via eine Datenbank, ist gleichbedeutend mit einem Verlust für alle diese Anwendungen.

Kommt die E-ID?

Seit kurzem ist noch ein weiterer Kritikpunkt an der Änderung des Ausweisgesetzes vermehrt diskutiert worden. Besagte Änderung erlaubt nämlich theoretisch auch, die ID in Zukunft mit biometrischen Daten und RFID-Chips zu versehen. Die derzeitige Formulierung überlässt eine mögliche Einführung dem Bundesrat. Auch hier handelt es sich um eine Idee, die nichts mit Schengen zu tun hat. Das Schengen-Abkommen klammert diesen Typ Ausweis sogar explizit aus der Biometriepflicht aus. Zwar geben die Befürworter des Passes auch hier an, dass dies momentan nicht geplant sei. Dennoch verweisen die Gegner auf entsprechende Aussagen von Bundesrätin Widmer-Schlumpf und Nationalrat Roberto Schmidt. Erschwerend hinzu kommt, dass bisher auch nicht klar ist, wie die Sicherheitstechnik bei einer solchen ID aussehen würde. Selbst wenn der Schweizer E-Pass komplett

sicher wäre, ist unklar, ob das auch auf eine E-ID zutreffen würde.

Der E-Pass hat aber auch noch eine ökonomische Dimension - vielleicht nicht unbedingt in der Schweiz, aber in anderen Ländern. Mit dem E-Pass wird eine automatische Überprüfung der Person an Flughäfen und Grenzen möglich. Damit einhergehen können Verzicht oder Reduktion teuren Personals und auch der Wunsch Geld zu sparen, indem der Abwicklungsprozess schneller vonstatten geht. Ein Indikator für solche Tendenzen ist zum Beispiel Malaysia, eines der ersten Länder, das einen E-Pass einführt. So gibt es heute am Flughafen in Kuala Lumpur automatisierte Gates, bei denen der Fingerabdruck der Person mit dem im Pass gespeicherten verglichen wird.

Das biometrische Wettrüsten zahlt der Bürger

Die Einführung biometrischer Ausweise in vielen Ländern erfolgt laut offiziellen Aussagen vor allem deshalb, für mehr Sicherheit zu sorgen. Dabei ist so ein internationales System nur so stark wie sein schwächstes Glied. Es ist durchaus vorstellbar, dass sich eine entsprechend motivierte Person eine neue Identität in einem Schwellenland kaufen kann. Unter Verwendung dieses Ausweises, mit denselben biometrischen Daten jedoch unter anderem Namen, kann man dann wieder einreisen,

falls die Daten nicht zentral gespeichert werden. Somit muss ein Land allerdings alle Daten horten, um erneute Einreiseversuche unter anderem Namen zu verhindern. Da aber alle Länder solche Bedürfnisse haben, bedarf es dazu einer möglichst umfassenden Datenbank in jedem beteiligten Land. Selbst wenn also die Schweizer Datenbank vor illegalem Zugriff geschützt wäre, stellt sich die Frage, ob das auch für alle anderen Länder gilt.

Aber selbst ein System, das solche Probleme vermeidet, kommt an anderer Stelle an seine Grenzen. Vorstellbar ist nämlich auch der Erwerb eines Ausweises mitsamt einem Satz neuer biometrischer Daten. Von so einem Fall berichtete vor kurzem die japanische Zeitung Yomiuri. Eine Frau erwarb einen falschen Ausweis plus Gummifingerkuppen in Korea und reiste dann mit diesen in Japan ein. Szenarien dieser Art sollten sich wiederum mit Scannern vermeiden lassen, die Lebendgewebe identifizieren können. Dieses Hin und Her sorgt für ein Wettrüsten, bei dem das Ergebnis für den technisch unversierten Bürger unklar bleibt, er aber die Kosten tragen darf. Im übrigen kann auch der E-Pass Gefahren, die von realen Personen ausgehen, nicht verhindern. Mohammed Atta flog unter seinem Namen mit seinem Pass in die USA. Die Anschläge vom 11. September hätten wohl auch dann stattgefunden, hätte sein Pass noch seine Fingerabdrücke enthalten.

Wie sicher ist der E-Pass?		
Angriffsart	Was heisst das?	Auswirkungen auf den Pass 10
Heimliches Scannen	Kann der Pass ohne Einwilligung des Besitzers gelesen werden? Dabei gibt es zwei Abstufungen: 1. Sind die Personendaten lesbar? (Identitätsdiebstahl) 2. Hat der Pass eine eindeutige ID-Nummer? (Tracking und Hotlisting)	1. Ist der Schlüssel der Basic Access Control bekannt, kann der Pass auch in geschlossenem Zustand gelesen werden. Zugriff besteht dann auf die Personendaten und das Foto, nicht aber auf die Fingerabdrücke 2. Siehe nächster Punkt
Heimliche Überwachung	Verfügt der Pass über einen statischen Identifikator (klare Personendaten oder ID-Nummer), der jederzeit gelesen werden kann, ermöglicht er die Überwachung der Personenbewegung. Dazu reicht ein Anbringen von Scannern an strategisch wichtigen Orten, z.B. Türrahmen.	Gemäss EJPD sind die Daten immer verschlüsselt. Ausserdem generiert der Pass 10 bei jedem Lesevorgang eine neue UID. Dies sollte eine Überwachung unmöglich machen. Es sei denn, der BAC-Schlüssel ist bekannt.
Abhören	Das Lesen der Daten funktioniert nur aus kurzer Entfernung. Ist der RFID-Chip durch den Lesevorgang jedoch aktiviert, beginnt er zu senden. Hier besteht die Gefahr des Abhörens aus grösserer Entfernung. Dies ist problematisch, da eine solche Aktion leicht unbemerkt durchgeführt werden kann und die Antennentechnik sich laufend weiterentwickelt.	Gemäss EJPD ist das Risiko hier klein, auch aufgrund diverser alltäglich vorkommender Störquellen wie Computer oder Mobiltelefone. Die technische Entwicklung schreitet jedoch voran. Ausserdem findet die Übertragung verschlüsselt statt, ein Mitschnitt wäre jedoch möglich.
Kryptoschwächen: Basic Access Control (BAC)	Wie sicher ist der Schlüssel? Aus den Personendaten in der MRZ (Machine Readable Zone) wird nach optischem Scan ein Schlüssel errechnet. Wird der RFID-Chip damit bedient, beginnt er Personendaten inklusive Foto zu senden.	Gemäss EJPD kommt dieses Verfahren nur dann zur Anwendung, wenn keine EAC (siehe nächster Punkt) möglich ist. Der BAC-Schlüssel des Passes 10 ist sicherer als in anderen Ländern (höhere Entropie). Die Übertragung kann jedoch mitgeschnitten werden. Ob der Schlüssel dann später via Brute-Force-Attacke zu brechen ist, wird kontrovers diskutiert.
Kryptoschwächen: Extended Access Control (EAC)	Wie sicher ist der Schlüssel? Die EAC hat einen höheren Grad an Entropie.	Befindet sich der Scanner in einem Land, das berechtigt ist, auf die biometrischen Daten zuzugreifen, wird gleich zu Anfang eine hochsichere Verbindung im Sinne der EAC aufgebaut. Diese sollte gemäss EJPD nicht zu knacken sein. Ausserdem wird der Zugriff auf die biometrischen Fingerabdruckdaten nur mit einem Schlüssel frei, den die Schweizer Behörden der überprüfenden Behörde zur Verfügung stellen müssen. Dazu müssen die oben genannten Verfahren funktionieren. Das Problem hier ist vor allem die globale Infrastruktur, da jeder Scanner online sein muss, weil die Zertifikate nur kurze Zeit gültig sein sollen.
Klonen	Hier gibt es zwei Ansatzpunkte: 1. Sind die Daten echt? 2. Ist der Container (Reisepass) echt?	1. Die Daten sind signiert, um ihre Echtheit zu garantieren. 2. Die Echtheit des Containers wird via Chip Authentication sichergestellt, dabei kommt ein Public-/Private-Key-Verfahren zum Einsatz.