# Gesichtsbuch in Staatshand

## Der elektronische Personalausweis als biometrisches Erfassungsinstrument

Seit November 2010 ist der Personalausweis der Bundesrepublik Deutschland „elektronisch“ und heißt drum ePA oder, nach Regierungs-Neusprech, nPA, weil „neu“ offenbar positiver konnotiert ist als „elektronisch“. Nun dürfen die Untertanen gar nicht mehr lächeln, wenn sie Ausweisfotos machen: Sowohl Pass als auch Personalausweis brauchen jetzt „biometrische“ Bilder. Diese landen in einem RFID-Chip und beim Meldeamt -- und dann?

Vorneweg: Um die beim ePA auch neue Auslesbarkeit digitaler Daten im Ausweis per Funk („RFID“) geht es uns hier nicht. Dazu gab es schon einen Artikel in RHZ 2/06, und es scheint auch, als sei die Obrigkeit an solchen Tricks zunächst vor allem interessiert, weil der Ausweis ohne Kontakte robuster ist. Jedenfalls sind vorläufig keine Pläne bekannt, ePA-Portale zu bauen, die nach dem Muster der Mautbrücken einfach alle durchgehenden Identitäten erfassen. Die Sorte RFID-Chip, die im ePA verbaut ist, macht sowas auch nicht gerade einfach. Wenn also RFID-basiertes Bewegungsprofiling kommen sollte, dann nicht bald und nur als Kollateralnutzen.

Aber natürlich ist auch der offizielle Grund, bessere (Fälschungs-) Sicherheit nämlich, nicht stichhaltig -- die Hauptlücken hier lagen schon bisher eher im administrativen Bereich, und das wird sicher nicht besser, wenn mehr komplizierter Computerwahnsinn im Spiel ist. Die EU-Vorgaben wiederum hat die Berliner Regierung wesentlich selbst diktiert, sie können also auch nicht als Motivation herhalten.

Nein, im Vordergrund stehen zwei Gründe. Der harmlosere läuft unter dem Großtitel Industriepolitik (um hässliche Wörter wie sicherheits-industrieller Komplex oder Korruption zu vermeiden) -- der Industriezweig, der „Sicherheitslösungen“ verkaufen will, ähnelt inzwischen insoweit der Waffenindustrie, als er die politischen Entscheidungen seiner Kunden ganz wesentlich beeinflusst. Die Technologie hinter dem ePA soll Exportschlager werden, seine bundesweite Einführung ist kräftige Subvention und kostenlose Werbung in einem. Da in Produktdenke mehr Features mehr Markterfolg versprechen, ist sekundär, ob all der in das System reingebastelte Kram nötig oder auch nur verträglich mit Menschenrechten ist.

Während solche Nummern in entwickelten Demokratien nur Achselzucken auslösen dürften, ist der andere Grund sinistrer: Es geht um eine erkennungsdienstliche Behandlung der Gesamtbevölkerung. Dieses gewaltige Kontrollprojekt hat am Schluss nicht ganz geklappt, weil die Erfassung der Fingerabdrücke in der gesetzgeberischen Zielgeraden „optional“ wurde -- dank an die an der damaligen Datenschutz-Empörung Beteiligten -- und mithin wohl niemand, der/die noch ganz bei Trost ist, die große ED-Behandlung auf sich nehmen wird. Doch die Entwicklung der Technologie wurde natürlich trotzdem subventioniert, andernorts besteht ja Nachfrage. Sowieso kann ja noch kommen, was noch nicht ist.

Zur Einordnung der Totalerfassung „biometrischer“ Fotos ist eine Rückschau auf das Projekt „Fotofahndung“ nützlich, das das BKA 2006/07 im Hauptbahnhof von Mainz laufen hatte. Dabei sollten Testsysteme einer Handvoll Hersteller aus dem Strom der BahnhofsnutzerInnen per Kamera bestimmte Gesichter herausfinden. Das Projekt wurde später öffentlich als mehr oder minder gescheitert abgeschrieben. Dieses Ergebnis stand indes nach ähnlichen Versuchen an anderen Orten im Wesentlichen von vorneherein fest. Ebenso klar war bereits zu Beginn, wie die Erkennungs- und Irrtumsraten zu verbessern gewesen wären: Besseres „Enrollment“, also mehr Daten von den zu erkennenden Personen. Mit ein paar Dutzend Fotos pro Person, aus verschiedenen Positionen und vielleicht mit verschiedener Beleuchtung, hätten die Rechner ein erheblich besseres Bild abgegeben.

Stattdessen war Bedingung des BKA: Ihr müsst auskommen mit -- Überraschung -- einem „biometrischen“ Passbild, beschrieben in enger Analogie zur Verordung über den ePA. Eigentliches Ergebnis des Fotofahndungs-Versuchs ist also mitnichten die alte Erkenntnis, dass Gesichtserkennung *so* nicht funktioniert, sondern megabyteweise Trainingsdaten für die Industrie, die damit funktionierende Anwendungen von Gesichtserkennung entwickeln kann.

Ein paar Beispiele für solche Systeme:

- „optimierte“ Videoüberwachung: Die armen Überwacher sitzen nicht selten vor Dutzenden von Monitoren. Es wäre doch nützlich, wenn sie blaue Rahmen für Verkehrssünder im Sichtfeld bekommen könnten, rote bei linken Zecken und grüne bei LadendiebInnen. Die erhebliche Fehlerrate stört dabei nicht wirklich, eine Hilfe ist sowas fast in jedem Fall.
- Unterstützung für die BFE: Die „Beweis- und Festnahmeeinheiten“ der polizeilichen Prügelabteilungen könnten ein Gerät haben, das sie auf ein Gesicht richten und das ihnen dann ein paar Hypothesen sagt, wer es sein könnte, samt zugehörigen Auszügen aus diversen Polizeidatenbanken. Auch wenn dabei ein paar Dutzend Namen rauskommen: Nach dem Datenbankabgleich sollten sich die „interessanten“ Fälle schnell finden -- ein Glück, dass Vermummung in diesem Land ja schon illegal ist.
- „weiche“ Bewegungsprofile: Aus im Einzelnen unsicheren Daten kann durch Korrelation mit anderen ein scharfes Bild werden. So könnten etwa Kameras einen beständigen Strom von erkannten Personen liefern. 90% dieser Erkennungen können unsinnnig sein, und 60% der Personen, die durchlaufen, nicht erkannt werden. Wenn mensch aber weiß, wo bestimmte Mobiltelefone sind, wer irgendwo mit der EC-Karte bezahlt hat oder eigentlich in der Schule sein sollte und dann die Daten ausreichend vieler Kameras mit einfachen Regelanwendungen kombiniert („in 50 Minuten kommt keineR von Westerland nach Köln-Deutz“), können sich für einzelne „Zielpersonen“ durchaus reizvolle Datensätze ergeben.

Anwendungen dieser Art sind in §15 des Personalausweisgesetzes ganz offensichtlich berücksichtigt: PA-Daten dürfen z.B. zur „Fahndung oder Aufenthaltsfeststellung“ verwendet werden. Das Personalausweisregister -- geführt von den Meldebehörden -- speichert dazu auch schon die Fotos (und übrigens auch die Unterschrift). §24 und §25 des Gesetzes genehmigen Behörden quasi freien Zugriff auf diese Daten, im Wesentlichen auf einer no-questions-asked-Basis und im Zweifel auch im Direktzugriff.

## Keine Hilfe

Die Verfahren zum Abgleich biometrischer Daten und damit auch zur Gesichtserkennung machen Fehler. Das gilt für die Implementation in unser aller Hirnen, und noch weit mehr für das, was mit heutigen Algorithmen und einem lausigen statischen Bild hinzubekommen ist. So wie wahrscheinlich jedeR schon mal ein „Hast du mich jetzt echt nicht erkannt?!“-Erlebnis ebenso hatte wie eine „Oh Verzeihung, ich habe Sie verwechselt“-Situation, können auch Rechner beim Erkennen zwei Sorten von Fehler machen: Sie können eineN GesuchteN verpassen, oder es kann Alarm geben bei einer Person, die nicht gesucht wird. Weil der Kram zwischen Medikamententests und Websuchen überall auftaucht, hier noch Jargon: Die Wahrscheinlichkeit, einen Gesuchten auch zu finden, heißt Sensitivität, die Wahrscheinlichkeit, für nicht Gesuchte auch keinen Alarm zu geben, Spezifität.

Auch wer noch kein solches System gebaut hat, wird sich vorstellen können, dass ein „schärferes“ System (das weniger Gesuchte verpasst, also eine hohe Sensitivität hat) normalerweise eine niedrigere Spezifität hat, also eher mal einen falschen Alarm gibt -- und umgekehrt. Dabei sind Fehler nicht immer schlimm: Zwar ist eine Fotofahndung, die ständig Alarm gibt, unbrauchbar. Wenn sie hingegen nur 10% der Gesuchten findet, aber nie „Unschuldige“ anschwärzt, mag sie durchaus attraktiv erscheinen.

Dennoch ist eine Maßnahme gegen die ED-Behandlung light (unterhalb des eigentlich wünschenswerten all-out-Kampfs dagegen), mehr „Rauschen“ in die Eingabedaten zu bringen, die Obrigkeit also zu zwingen, „großzügiger“ zu vergleichen, damit die Sensitivität nicht komplett vor die Hunde geht. Das aber macht ihnen die Spezifität kaputt, und ihre Fahndungscomputer kommen aus dem Piepsen gar nicht mehr raus -- arme Polizei, arme Hersteller.

„Rauschen“ heißt in dem Zusammenhang: Wer sonst keinen Bart trägt, trägt für den Personalausweis einen (so er/sie ausreichend Bartwachstum hat) , ein dezenter Kajal ist nicht verboten, auch von Frisuren können die Algorithmen nicht immer gut abstrahieren. Ganz drastisch wird es, wenn mensch es schafft, Augabstand und Position der Nasenspitze jedenfalls auf dem Bild etwas „off“ zu kriegen. Es schadet natürlich auch nichts, übernächtigt und etwas ausgehungert zum Fotografieren zu gehen (oder ausgeschlafen und wohlgenährt für professionelle PartygängerInnen). Und dann bleibt der Kamerazoom ganz drinnen -- je weitwinkliger die Optik ist, desto weiter weicht die Perspektive vom typisch großen Zoom der Überwachungskamera ab, und auch das irritiert den Rechner.

Schließlich kann mensch im Zeitalter der digitalen Fotografie ja auch das Bild im eigenen Rechner vorverarbeiten. Dazu muss mensch zunächst wissen, dass das Bild 35 auf 45 mm messen muss sowie zwischen Scheitel und Kinn 32 bis 36 mm liegen müssen. Mit einem Bildbearbeitungsprogramm (wir empfehlen den Gimp, verfügbar auf http://www.gimp.org) und den Fotodruckdiensten in der Drogerie nebenan lassen sich diese Bedingungen recht bequem erfüllen.

Auf das meist angebotene Format 15x10 cm passen z.B. bequem sechs Passbilder. Zwecks einfacher Rechnung arbeitet mensch in einem Bild im Format 1000 mal 1500 Pixel. Im Portrait müssen dann zwischen Scheitel und Kinn ca. 340 Pixel liegen (im Gimp hilft Werkzeuge/Maßband, um den Skalierungsfaktor auszurechen; den Faktor könnt ihr im Skalierungsdialog eingeben, wenn ihr als Einheit Prozent auswählt). Die Einzelbilder, die ihr in die große Druckvorlage einfügt, müssen danach logischerweise 350 mal 450 Pixel groß sein.

Soweit wir wissen, gibt es kein Gesetz dagegen, eine Gesichtshälfte um ein paar Pixel zu schrumpfen, Filter wie iWarp (dezent!) anzuwenden oder Mitesser wegzuretuschieren. Im Netz gibt es zahlreiche Anleitungen für kreative Bildverbesserung. Klar ist aber, dass ihr noch gut erkennbar sein müsst. Das ist das Gesetz, und außerdem würdet ihr natürlich den doofen Ausweis nicht bekommen, wenn nicht Menschen erkennen würden, wer die Person auf dem Foto ist.

## Die nIdentität

Neben dem Foto befindet sich auf dem Chip auch etwas, das im Gesetz „elektronischer Identitätsnachweis“ heißt und einem privaten Schlüssel bei PGP entspricht. Der ePA hat demnach auch eine Passphrase (aber für Doofe: „Geheimnummer“), und es gibt auch ein „Sperrkennwort“, das mit Glück etwas wie PGPs Rückrufzertifikat, ebenfalls für Doofe, sein könnte. Nur ist der Schlüssel natürlich nicht richtig geheim, weil er ja staatlich generiert ist und es mit dem Teufel zugehen müsste, wenn da nicht irgendwo Nachschlüssel rumliegen würden.

Deshalb ist es gut, dass die Funktion extra eingeschaltet werden muss, und klar: KeinE aufrechteR LinkeR wird das tun. Dienste, die auf dem Mist aufbauen, könnt ihr dann nicht nutzen, aber deren BetreiberInnen muss ohnehin gesagt werden, dass sie PGP unterstützen sollen -- das funktioniert genauso gut und kommt ohne potenziellen Nachschlüssel der Obrigkeit aus.

Ein Boykott der Nutzer-Krypto auf dem ePA ist um so wichtiger, als eine denkbare Motivation für ihre Präsenz auf dem Chip ein fieser Plan sein könnte, die Kryptografie der Untertanen zu „regulieren“, sprich PGP (und vieles andere) zu verbieten. Das ist nicht absurd, sondern war z.B. in Frankreich jahrelang Praxis: Was der Staat nicht knacken kann, war dem Citoyen verboten. Solche Ansinnen scheiterten in der BRD immer am Einspruch von Siemens und Freunden, denen klar war, dass ohne wirksame Verschlüsselungsmethoden im Netz kaum Geld zu verdienen sein würde.

Da nun der Staat selbst kryptografische Verfahren anbietet, die fraglos gegen nichtstaatliche Angreifer mindestens so sicher sind wie das, was derzeit Banken und Co den meisten ihrer KundInnen bieten, könnten sich Bedenken dieser Art legen. *Wenn* also die ePA-Krypto und der staatlich abgesegnete E-Mail-Dienst DE-Mail ein Erfolg werden, gehen wir jede Wette ein, dass der Law-and-Order-Chor bei der nächst passenden Paketbombe für ein Verbot von Verschlüsselungssoftware ohne Hintertür heulen wird. Je nach der Zahl der Menschen, denen ihr PGP weggenommen werden muss, könnten sie damit auch durchkommen.

Im Übrigen schadet es qua Gesetz dem Ausweis nicht, wenn der Chip kaputt ist. Nur: legt ihn nicht in den

Mikrowellenherd. Der Chip geht zwar kaputt dabei, aber aller Wahrscheinlichkeit nach so spektakulär, dass ihr gleich wieder zur Ausweisbehörde müsst und die Bundesdruckerei subventionieren dürft. Schonendere Geräte dürften bald käuflich zu erwerben sein; Anleitungen für RFID-Zapper (z.B. auf der Basis von Einwegkameras) gibts im Netz.

Datenschutzgruppe der Roten Hilfe Heidelberg

Kontakt und Artikel-Archiv: http://datenschmutz.de

PGP Fingerprint: a3d8 4454 2e04 6860 0a38 a35e d1ea ecce f2bd 132a