Biometrie und Datenschutz – Der vermessene Mensch

Peter Schaar (Hrsg.)

Tagungsband

zum Symposium
des Bundesbeauftragten
für den Datenschutz und
die Informationsfreiheit
am 27. Juni 2006 in Berlin

Herausgeber: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 20 01 12, 53131 Bonn

Hausanschrift: Husarenstraße 30, 53117 Bonn
Telefon 02 28 - 8 19 95-0, Telefax 02 28 - 8 19 95-550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

Gesamtherstellung: Das Druckhaus Bernd Brümmer, 53347 Alfter/Bonn

Inhaltsverzeichnis

Vorwort

Die Anschläge vom 11. September 2001 in New York und vom 11. März 2004 in Madrid haben vielfältige Reaktionen provoziert. Dazu gehört auch der verstärkte Einsatz biometrischer Systeme, vor allem in Reisedokumenten. Entwicklungen, die bis dahin ohne größere öffentliche Beachtung vonstatten gingen einen enormen Schwung erhalten und sind in den Fokus der Öffentlichkeit gelangt. In der Folgezeit wurden – nicht zuletzt durch die Bereitstellung von öffentlichen Geldern – erhebliche Fortschritte im technischen Bereich der Biometrie gemacht. Dazu zählen nicht nur die Entwicklungen im Bereich der Gesichts- und Stimmerkennung, sondern u.a. auch bei der DNA-Analyse und bei der Iris-Erkennung und bei der Auswertung von individuellen Bewegungs- bzw. Verhaltensmustern.

Die Frage, ob und unter welchen Bedingungen biometrische Verfahren zur Identifizierung von Personen eingesetzt werden dürfen, berührt verschiedene Rechtsgebiete. So hat die Europäische Kommission seit 2003 die Arbeiten an einem europäischen Visa-Informationssystem (VIS) vorangetrieben, in dem neben den alphanumerischen Daten aus einem Antrag auf Erteilung eines Visums bei einer Auslandsdienststelle eines Mitgliedstaates auch biometrische Merkmale (digitalisiertes Gesichtsbild, Fingerabdrücke) gespeichert werden sollen. In diese Datenbank sollen künftig jährlich die Daten von etwa 20 Millionen Visa-Antragsteller gespeichert werden. Der Europäische Rat hat durch die „Verordnung (EG) Nr. 2252/2004 vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten“ die Aufnahme des Gesichtsbildes sowie von Fingerabdrücken in elektronischer Form in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten verbindlich vorgeschrieben. Seit November 2005 enthalten daher die neu ausgestellten deutschen Reisepässe einen RFID-Chip, in dem zunächst – neben den bereits in den konventionellen Pässen gespeicherten alphanumerischen Angaben über den Passinhaber- dessen Gesichtsbild in digitalisierter Form gespeichert wird. Ab November 2007 ist zudem geplant, dort zusätzlich die Daten von Fingerabdrücken zu speichern. Nach den Planungen der Bundesregierung soll auch der Personalausweis künftig einen Chip mit biometrischen Daten erhalten.

Der Verabschiedung der europäischen Pass-Verordnung ((EG) Nr. 2252/2004) ist keine ausreichende öffentliche Diskussion vorausgegangen . Angesichts der weiteren Planungen zur Einführung biometrischer Merkmale sowohl im öffentlichen wie im nicht-öffentlichen Bereich ist es jedoch notwendig, derartige Verfahren auf fundierter wissenschaftlicher Basis breit zu diskutieren. Als Beitrag zu dieser Diskussi-

on habe ich am 27. Juni 2006 in der Staatsbibliothek zu Berlin ein Symposium mit dem Titel „Biometrie und Datenschutz – Der vermessene Mensch“ veranstaltet. Der vorliegende Tagungsband dokumentiert die dort gehaltenen wissenschaftlichen Beiträge sowie die anschließende politische Diskussion. Besonders gefreut hat mich dabei, dass sich nicht nur Wissenschaftler aus dem rechtswissenschaftlichen Bereich, sondern auch aus dem rechtsphilosophischen und dem technischen Bereich bereit erklärt haben, dem Symposium zum Erfolg zu verhelfen. Die Vortragstexte wurden für diesen Tagungsband von den Vortragenden teilweise überarbeitet und gehen daher mitunter über die mündlich behandelte Thematik hinaus. Wie auch bei meinem ersten Symposium hatten sich darüber hinaus namhafte Bundestagsabgeordnete bereit erklärt, die Ergebnisse der Vorträge in einer Podiumsdiskussion politisch aufzuarbeiten.

Allen, die zum Erfolg des Symposiums beigetragen haben, möchte ich auf diesem Wege noch einmal meinen Dank aussprechen. Der Dank richtet sich dabei nicht nur an diejenigen, die durch Referate und Diskussionsbeiträge inhaltlich interveniert haben, sondern auch an all diejenigen, die im Hintergrund für einen reibungslosen Ablauf der Veranstaltung gesorgt haben.

Bonn, Oktober 2006

Peter Schaar

Eröffnung

Peter Schaar

Ich möchte Sie zum 2. Symposium des Bundesbeauftragten für den Datenschutz Willkommen heißen. Wir als Datenschützer begreifen uns als Bestandteil der Öffentlichkeit. Wir tragen zur Meinungsbildung bei. Wir hoffen allerdings auch, dass wir mit dem Symposium ein wenig zur Fortbildung beitragen.

Heute geht es um das Thema „Der vermessende Mensch", um die Biometrie. Wir wollen uns heute von unterschiedlichen Seiten diesem Thema nähern, auch im Sinne einer politischen Positionsbestimmung. Wir werden, wie schon bei dem letzten Symposium zum Großen Lauschangriff, Vertreter und Vertreterinnen von Politik und von Wissenschaft zusammenführen, um dann über die politischen Konsequenzen zu diskutieren. Allen Expertinnen und Experten, wie auch den anwesenden Vertretern der Medien ein herzliches Willkommen.

Ganz herzlich bedanken möchte ich mich auch bei der Berliner Staatsbibliothek und der Stiftung Preußischer Kulturbesitz, die uns hier kooperativ geholfen haben, dieses Symposium durchzuführen. Wir beabsichtigen, über das Symposium einen Tagungsband zu erstellen. Auf jeden Fall werden die Beiträge und auch die Diskussionen entsprechend dokumentiert und verfügbar gemacht, damit auch diejenigen, die sich nicht in diesem Raum befinden, die Chance haben, von den Erkenntnissen zu profitieren. Zudem freue ich mich auch noch sehr, dass ein Team von Studenten der Deutschen Film- und Fernsehakademie hier anwesend ist und eine Aufzeichnung für eine Abschlussarbeit macht.

Der Titel des Symposiums ist bewusst doppeldeutig gewählt: „Biometrie und Datenschutz - Der vermessene Mensch". Die Tatsache, dass man es jetzt mit biometrischen Merkmalen zu tun hat, ist terminologisch neu, aber nicht wirklich, wenn es um die Frage geht, welche Erkenntnisse man von anderen Menschen hat. *„Bios"* bedeutet das Leben und *„Metron"* das Maß. Also letztlich geht es hier um die Lehre von der Anwendung mathematischer Methoden zur zahlenmäßigen Erfassung, Planung und Auswertung von Experimenten in Biologie, Medizin und Landwirtschaft. Das sagt zumindest der Duden. Das Online-Lexikon Wikipedia macht es ein bisschen einfacher: Vermessung qualitativer Merkmale von Lebewesen unter Anwen-

dung statistischer Verfahren. Ja, insofern denke ich ist „Der vermessene Mensch“ auch wörtlich zu nehmen, wenn wir uns mit Biometrie befassen. Es geht also nicht nur um bildliche Darstellungen, also um diese sehr klassischen biometrischen Methoden, mit denen wir es immer schon zu tun haben, sondern es geht um die Messung der erfassten Merkmale.

Wenn man sich über die Vorteile und die Anwendungsbereiche biometrischer Methoden Gedanken macht, dann muss man auch fragen: Gehen von diesen Methoden auch Gefährdungen für den Betroffenen aus ? Es wird Sie nicht überraschen, dass gerade der Datenschutzbeauftragte sich mit dem Aspekt des Datenschutzes - also des Rechts auf informationelle Selbstbestimmung – auseinandersetzt. Wir erwarten uns von den Redebeiträgen auch hier neue Erkenntnisse. Schon heute wissen wir, dass diese biometrischen Merkmale häufig nicht nur die gewünschten Informationen beinhalten, die dazu beitragen sollen, den Einzelnen zu identifizieren, sondern Überschussdaten oder Überschussinformationen. Also z.B., dass sich aus dem Gesichtsabbild bestimmte Informationen über die Lebensumstände der betroffenen Personen ablesen lassen - das ist zwar banal. Aber vielleicht wird dies in Zukunft auch automatisierbar. Das könnte dann schon sehr viel problematischer sein. Dasselbe gilt im Prinzip für sämtliche biometrischen Merkmale. Diese Zusatzinformationen beziehen sich auf die Persönlichkeit des Einzelnen, auf seinen Gesundheitszustand, seine ethnische Herkunft und insofern enthalten diese Überschussinformationen immer auch sensible Daten. Daher ist die Frage gestattet, in welchen Bereichen und in welchen Einsatzumgebungen können biometrische Verfahren überhaupt verwendet werden.

Aber es ist nicht das einzige Risiko, mit dem wir es zu tun haben. Ich will sie hier nur stichwortartig erwähnen, denn ich denke, diese werden in den folgenden Vorträgen noch vertieft. Wichtig ist, dass biometrische Daten ggf. zu Überwachungszwecken verwendet werden könnten, nicht nur zur Identifikation in der definierten Einsatzumgebung. Ein Bild, das für ein Zugangskontrollsystem gemacht wird, könnte auch verwendet werden für eine Überwachungsanlage mit Videotechnik. Biometrische Merkmale könnten missbraucht werden, indem man Informationen oder eben diese Merkmalsausprägungen sich verschafft und das biometrische Merkmal nachbildet, z.B. eine Silikonfingerkuppe mit einem echten falschen Fingerabdruck. Bei solchen Verfahren stellt sich natürlich die Frage, wie kann ich denn beweisen - wenn dann die Biometrie anscheinend den sicheren Beweis für dass ich es war, der dieses Merkmal irgendwo abgegeben oder verwendet hat -, dass ich es eben doch nicht war, sondern ein Dritter, der dieses biometrische Merkmal gefälscht oder gestohlen hat. Die Frage, wie zuverlässig diese biometrischen Merkmale sind, ist natürlich auch gestattet. Was passiert z.B., wenn ich bei einer Biometrie gestützten Grenzkon-

trolle nicht erkannt werde ? Muss ich mich dann zusätzlich rechtfertigen ? Höchstwahrscheinlich ja, d.h., ich gerate ggf. unter Verdacht. Schließlich im Sinne derjenigen, die solche Verfahren einführen wollen: Wie sicher sind die Verfahren denn wirklich ? Hier muss man sich ganz nüchtern Rechenschaft ablegen und ich hatte in der Vergangenheit das Gefühl, dass das nicht immer angemessen geschehen ist. Auch und gerade im Zusammenhang mit der Einführung der biometrischen Merkmale in den Pässen, die ja von der EU in einem ziemlichen Hau-Ruck-Verfahren beschlossen worden ist.

Ich denke, ich spreche auch für meine Kolleginnen und Kollegen, die ich hier zahlreich vertreten sehe, wenn ich darauf hinweise, dass wir nicht den Anspruch haben, Technologie zu verhindern oder sinnvolle Verfahren aufzuhalten. Aber wir haben den Anspruch Verfahren datenschutzgerecht zu gestalten, und deshalb hat der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder schon vor Jahren Handlungsempfehlungen zum datenschutzgerechten Einsatz von biometrischen Verfahren ausgearbeitet. Aus meiner Sicht sind diese Empfehlungen nach wie vor aktuell. Ich möchte hier nur einen einzigen Punkt erwähnen, der für mich von erheblicher Bedeutung ist: Die Unterscheidung von verifikationsorientierten Verfahren von Verfahren, die die Identifizierung zum Ziel haben. Technisch besteht der Unterschied nicht etwa in der Frage, wie wird das biometrische Merkmal erkannt. Die Frage ist vielmehr, wird 1:1 verglichen, d.h. stimmt die Person, die z.B. eine Chipkarte oder einen Ausweis vorlegt, auf dem ein biometrisches Merkmal gespeichert ist, mit dem Ausweisinhaber überein. Das ist Verifikation. Bei der Identifikation im weiteren Sinne geht es darum, dass man anhand des biometrischen Merkmales die richtige Person aus einer Datenbank heraus identifiziert (1:n-Vergleich). Unter Datenschutzgesichtspunkten ist diese Unterscheidung von Bedeutung, weil diese 1:n-Vergleiche im Prinzip immer Datenbanken mit biometrische Merkmalen voraussetzen. Solche Datenbanken bedeuten aber, dass diese Daten sich nicht unter voller Kontrolle des Betroffenen befinden. Und dieses wiederum beinhaltet Risiken für den Missbrauch oder eine weitergehende Verwendung dieser Informationen in nicht datenschutzgerechter Weise. Deshalb hat ja auch der Deutsche Bundestag bei der Grundsatzentscheidung im Rahmen der Anti-Terrorismus-Gesetzgebung 2002 beschlossen, Zentraldateien zu untersagen. Es geht allerdings nicht nur um Zentraldateien, auch sonstige regionale oder dezentrale Dateien können dasselbe Problem mit sich bringen, denn diese Dateien könnten ja auch verknüpft werden. Es kommt bei heutigen Technologien eben nicht mehr in erster Linie darauf an, wo das Merkmal physikalisch gespeichert ist. Deshalb sagen wir als Datenschützer, auf die Gestaltung des Gesamtsystems ist besonderer Wert zu legen.

Meine sehr verehrten Damen und Herren, wir haben es zu tun mit einem sehr aktuellen Thema - nicht nur die Pässe sind ein Stichwort hier, sondern auch die biometriegestützten Personalausweise -, deren Einführung mit einiger zeitlicher Verzögerung geplant ist. Aber auch im Bereich der Privatwirtschaft werden biometriegestützte Systeme z.B. bei der Zugangskontrolle, aber auch beim Bezahlen im Supermarkt um die Ecke eingesetzt, oder entsprechende Tests finden statt. Wir sind hier bei einem sehr aktuellen Thema, und ich freue mich darüber, dass sich so hochkarätige Teilnehmer aus der Wissenschaft bereit gefunden haben, uns hier Erleuchtung zu bringen.

Herzlich begrüßen möchte ich die drei Referenten. Es handelt sich allesamt um Professores mit jeweils unterschiedlichem Hintergrund. Ganz herzlich begrüße ich als erstes Herrn Prof. Dr. Strasser von der Karl-Franzens-Universität in Graz. Er hat bei einer Veranstaltung in der Schweiz einen sehr interessanten Vortrag über Verbrecherphysiognomien gehalten, der mich so beeindruckt hat, dass ich gesagt habe, den Mann müssen wir hier auch mal zu einem Symposium holen. Es ist mir eine Freude, ihm als Erstes das Wort zu geben, danach wird dann Herr Prof. Dr. Christoph Busch vom Fraunhofer Institut Graphische Datenverarbeitung in Darmstadt, eher den technologischen Hintergrund darstellen, und abschließend hören wir dann den sehr verehrten Herrn Prof. Rossnagel, wohlbekannt aus vielfältigen Veröffentlichungen im Datenschutz. Nicht nur rechtliche Fragen, dass ist ja seine eigentliche Profession, sondern auch die verfassungsgerechte, verfassungsverträgliche Gestaltung von Technologien ist sein Anliegen.

Es wird im Anschluss an die Vorträge die Gelegenheit gegeben, Rückfragen zu stellen. Auch im Rahmen der Podiumsdiskussion ist eine Publikumsrunde vorgesehen.

Herr Strasser, Sie haben das Wort.

Biometrie – ein Schritt in die Überwachungsdemokratie?

*Peter Strasser**

1. Die Antiquiertheit der Kontrollutopien

Da ich mich im Folgenden nolens volens auch ein wenig als Zukunftsseher betätigen werde, will ich gleich eingangs etwas über Glanz und Elend dieser Art von Profession sagen. Im 20. Jahrhundert hat es eine Reihe von Utopien gegeben, deren Autoren sich anheischig machten, die Strukturen der Gesellschaften von morgen, die heute teilweise schon wieder von gestern sind, herauszuarbeiten. 1984, die berühmte Utopie von George Orwell aus dem Jahre 1949, die wie viele andere düster und negativ war, müsste bereits vor mehr als 20 Jahren Wirklichkeit geworden sein.

Orwell, so könnte man sagen, ist ein Visionär des modernen Totalitarismus, mit seinen hyperbrutalen Methoden der Konditionierung und Einschüchterung von Menschen. In seinem Repertoire finden wir die exzessive Folter und die totale Kontrolle, nicht nur des Körpers, sondern auch des Geistes. Liest man Orwell, so denkt man an die Diktaturen des Faschismus und Stalinismus. Der ordentliche gesellschaftliche Betrieb scheint nur möglich unter der Voraussetzung, dass das Individuum verschwindet und durch eine kollektivierte, anonyme, gestanzte Massenpersönlichkeit ersetzt wird. In diesem Punkt gleichen sich, bei aller Unterschiedlichkeit im Detail, Orwells *1984*, Aldous Huxleys *Brave New World* (1932) und Ray Bradburys *Fahrenheit 451* (1953).

Einzig die Utopie von Burrhus Frederick Skinner, dem Erfinder des Konzepts der operanten Konditionierung und der Lerntheorie, ist vom Autor eindeutig positiv gemeint. Sie trägt im Original den Titel *Walden Two* (deutsch Futurum Zwei), wohl

* Peter Strasser ist Professor für Philosophie und Rechtsphilosophie am Institut für Rechtsphilosophie, Rechtssoziologie und Rechtsinformatik der Karl-Franzens-Universität Graz.

auch, um sich von den naiven Vorstellungen des 19. Jahrhunderts im Anschluss an Rousseau zu distanzieren. Denn ein Geistesverwandter Rousseaus, Henry David Thoreau, veröffentlichte 1854 einen Bericht über sein einfaches Leben im Wald unter dem Titel *Walden*. Skinners *Utopie*, 1948 erschienen, zeichnet eine Gesellschaft ganz unter der guten Herrschaft von Technokraten, welche die Menschen nach den Prinzipien der Lerntheorie erziehen.

Wichtig für die Idee des Buches ist die Kritik an der Demokratie, die als irrationale Herrschaft des Mehrheitsprinzips und des Laientums barsch abgelehnt wird. Sie sei das Schlimmste, die Diktatur des Dilettantentums. Jede funktionierende, florierende und der menschlichen Natur umfassend gerecht werdende Gesellschaft müsste demgegenüber eine Expertokratie sein, die es zuwege bringt, ihre Mitglieder laufend so zu konditionieren, dass schließlich ihre individuellen Bedürfnisse mit den Erfordernissen des Kollektivs harmonieren.

Kein Wunder, dass viele Kommentatoren in Skinners Gemeinwesen eine schreckliche Entartung wissenschaftlicher Kontrollmöglichkeiten sehen wollten. Am meisten wird die Freiheit des Einzelnen ja dadurch bedroht, dass er die Kontrolle, die über ihn ausgeübt werden soll, internalisiert, bejaht und sie schließlich zwanghaft, gleichsam wie eine Maschine, über sich selbst ausübt. Es ist unstatthaft, sagen die Kritiker zu Recht, gegen die Autonomie mit der Optimierung des Glücks im Sinne des Benthamschen Grundsatzes *The greatest happiness for the greatest number* zu argumentieren.

Mir scheint, dass alle genannten Utopien (oder „Dystopien“) Ängste und Hoffnungen ihrer Zeit widerspiegeln, die für die heutige Situation in den Demokratien des Westens kaum noch von Bedeutung sind. Das heißt jedoch nicht, dass die in diesen Werken zum Ausdruck kommende Furcht oder Hoffnung, die Gesellschaft der Zukunft könnte eine Gesellschaft umfassender Überwachung und Kontrolle werden, heute völlig unberechtigt wäre. Was die Autoren der ersten Hälfte des 20. Jahrhunderts jedoch nur unzulänglich oder gar nicht verstanden haben, war, dass der Kontrolltypus, der wirklich Zukunft hat, sich im Medium der Demokratie selbst wird entfalten müssen.

Ich will also im Folgenden Hinweise darauf geben, warum wir uns möglicherweise auf dem Wege hin zu einer Überwachungsdemokratie befinden und welche Rolle in diesem Kontext die Biometrie spielen könnte. Dabei wäre ich nicht ungehalten, wenn meinen Überlegungen das gleiche Schicksal beschieden wäre wie den erwähnten Utopien – nämlich durch die reale Entwicklung unserer Demokratien obsolet zu werden.

2. Liberaler und gesamtheitlicher Kontrollansatz

Werfen wir zunächst einen kurzen Blick in die Geschichte des Kontrolldenkens. Da finden sich schon immer einige Tendenzen und Lehren nebeneinander, manche praktisch erfolgreich, manche aber auch mehr Phantasie, mehr Wunschtraum als Realität.

Kontrolle durch die Ausübung physischer Gewalt ist eines der ältesten Modelle, das eine Reihe von Funktionen erfüllt, unter denen die Abschreckung des Einzelnen durch Leidzufügung sowie die Abschreckung der Allgemeinheit durch Furcht, also die Spezial- und Generalprävention, hervorstechen. Man sollte aber nicht übersehen, dass die Ausübung physischer Gewalt zu Kontrollzwecken immer auch den Sinn hat, die Macht desjenigen öffentlich zu demonstrieren, der diese Art von Gewalt systematisch auszuüben imstande ist.

Das ist ein Punkt, der heute wieder eine gewisse Aktualität in Anspruch nehmen darf. Je unsichtbarer nämlich die staatlichen Kontrollverfahren werden, umso stärker mag sich auch das Bedürfnis regen, weithin sichtbare Manifestationen dafür zu haben, dass der Staat effektiv kontrolliert und dabei machtvoll genug ist, seinen Bürgern Sicherheit zu gewähren gegenüber den vielfältigen Feinden von Recht und Ordnung. Die USA werden zurzeit mit guten Gründen dafür kritisiert, dass sie im Kampf gegen Kriminalität und Terror zu Mitteln wie der Todesstrafe, der Folter und menschenrechtswidrigen Internierungen greifen. Dabei darf man aber den – wie man sagen könnte – Sicherheits*mehrwert* nicht übersehen, den solche Methoden bei der eigenen Bevölkerung erbringen, die von der Arbeit der Sicherheitsdienste immer nur wenig erfährt. Deshalb wird eine Politik, die es sich leisten kann, Terrorverdächtige ohne Anklage jahrelang in Verhörlagern ohne Rechtsbeistand festzuhalten, bis zu einem gewissen Grad als Ausdruck eines starken Staates gutgeheißen, zumindest „klammheimlich".

Neben der physischen Gewalt, die auf Ordnungsstörungen reagiert, um sie generalpräventiv einzudämmen, sind seit langer Zeit andere Kontrollformen bekannt. Ausspähen, Absichten erkunden, Daten sammeln, um die so erhaltenen Informationen zur Verfolgung, Auffindung oder Gefügigmachung von Subjekten einsetzen zu können: das sind einige altbewährte Methoden der Polizei und Geheimdienste. Dabei sind gewisse, höchst wirksame Techniken wie die Daktyloskopie erst seit dem 20. Jahrhundert breitflächig im Einsatz. Frankreich, wo das komplizierte Körpervermessungsverfahren der Bertillonage eingeführt war, entschloss sich 1914, Fingerab-

drücke als Mittel der Personenidentifizierung allgemein zu etablieren; Großbritannien hatte sich bereits Anfang des Jahrhunderts dazu entschlossen.

Die Daktyloskopie ist ein biometrisches Verfahren, das ein Merkmal misst und speichert, welches die – man könnte sagen – öffentliche Oberfläche des Menschen definiert, ähnlich wie das Gesicht, für das auch niemand ernsthaft beanspruchen wird, es nur im Geheimen mit sich führen zu wollen. Doch Vorsicht ist am Platz. Denn zumindest was das Gesicht betrifft, ist die Situation heute nicht mehr eindeutig. Zu befürchten steht, dass unter Umständen aus gewissen biometrischen Anzeichen, beispielsweise aus der Beschaffenheit der Iris, auf gewisse Verhaltensgewohnheiten, namentlich auf Alkohol- und Drogengenuss, geschlossen wird. Wie dem auch sei, im Ursprung steht die Daktyloskopie für eine Kontrollmethode, die sich eines äußeren Merkmals des Menschen zu Zwecken der Identifizierbarkeit bedient, ohne ihn dabei in ein Netz von Identifikationen einbinden oder in seine psychologische Tiefe eindringen zu wollen. Weder soll sein Leben überwacht, noch sein Charakter aufgedeckt werden. Ein solches Kontrollverfahren passt gut zu unserem Verständnis jener Freizügigkeit, die liberale Demokratien ihren Bürgern zusichern.

Ganz im Gegensatz dazu kennt die Geschichte des Kontrolldenkens eine Phantasie, die davon träumt, den Menschen auf eine umfassende Weise in den Griff zu bekommen. Das Kontrollziel ist klar: Schon im Ansatz sollen asoziale Neigungen des Individuums dingfest gemacht werden, damit dieses einer entsprechenden Korrekturmaßnahme zugeführt oder, im Falle der Unkorrigierbarkeit, weggeschlossen werden kann. Die Geschichte der Physiognomik, also der vermeintlichen Erkennung des Charakters aus Merkmalen des Gesichts, ist teils skurril, teils erschreckend. Johann Kaspar Lavater war im 18. Jahrhundert so ein Gesichterleser. Seine *Physiognomischen Fragmente* (1775–1778) versah er mit dem Untertitel „…zur Beförderung der Menschenkenntnis und Menschenliebe“.

Das zeigt vor allem, dass, wenn erst die Liebe von den staatlichen Kontrollorganen ausgeht, man sich vor der Liebe in Acht nehmen muss. Lavater empfahl seine Physiognomik den Verhörbeamten und Richtern mit der Bemerkung, sie dürften fortan guten Gewissens auf einsatzintensive und dabei wenig liebevolle Verhörmethoden wie die Folter verzichten. Denn das Laster und das mit dem Laster einhergehende Verbrechen könne der Kundige dem Lasterhaften schon vom Gesicht und manchmal buchstäblich von der Nasenspitze ablesen. Auf analoge Weise werden die Verfechter der Phrenologie, allen voran ihr Begründer, der deutsche Arzt Franz Josef Gall (1758–1828), Laster und Verbrechen durch Betasten der Schädeldecke aufspüren und zu Fall bringen wollen.

In dieser Sichtweise sind rechtsstaatliche Umständlichkeiten wie Verteidiger, Beweismittelverfahren, Geschworenengerichte und eine nicht an „Heilung“ oder Abschließung orientierte Strafjustiz antiquiert. Kein Geringerer als der Begründer der modernen Kriminologie, Cesare Lombroso, wird im letzten Drittel des 19. Jahrhunderts versuchen, den gesamtheitlichen Kontrollansatz auf eine umfassende empirische Basis zu stellen, um zu beweisen, dass es einen „geborenen Verbrecher“ gibt. Und erst die Renaissance dieses Ansatzes bei den Nationalsozialisten zu Zwecken der Rassenhygiene und Selektion minderwertigen Menschenmaterials wird den Lombrosianismus endgültig desavouieren.[1]

Was rechtfertigt es dann, ihn überhaupt noch zu erwähnen? Weil es ganz und gar nicht ausgeschlossen ist, dass wir in naher Zukunft uns sozialen Zuständen annähern, in denen der gesamtheitliche Kontrollansatz wieder an Attraktivität gewinnt, freilich in einer Form, die sich von ihren Ursprüngen und den darin dominanten Phantasien zumindest äußerlich weit entfernt hat. Niemand wird mehr wie Lavater begeistert und lyrisch im Gesicht eines Menschen lesen, niemand mehr durch Schädelabtastungen auf den Charakter schließen, auch niemand mehr durch Körpervermessungen einen natürlichen Verbrechenshang nachweisen wollen.

Doch wenn gegenwärtig wieder in verstärktem Maße Kriminalitätsforschung als biologische Forschung betrieben wird, dann erfährt darin die alte Lehre vom Menschen, den seine Natur zur Asozialität bestimmt, eine Neuauflage. Nun könnte man diesen Trend in der so genannten Psychopathieforschung als eine kriminologische Besonderheit auf sich beruhen lassen. Doch das wäre meines Erachtens ein Fehler. Denn dass man den Psychopathen, also Menschen, die zur Herausbildung eines Gewissens schwerer in der Lage sind als der Durchschnitt, nun wieder tief ins Gehirn hineinschaut, um dort die genetisch determinierten, neurologischen Tiefenursachen asozialer Neigungen zu entdecken – dieser eigentümliche Erkenntnisdrang ist Teil eines Welt- und Menschenbildes, für welches mittlerweile der Name „Naturalismus“ steht.[2]

Das naturalistische Menschenbild fordert – im Gegensatz zum humanistischen –, dass der Mensch als eine Biomaschine betrachtet werde. Für die Individualität dieser Maschine ist die jeweilige DNA zuständig, die auch über die Besonderheiten der

---

1 Stephen Jay Gould, Der falsch vermessene Mensch, Franfurt a. M. 1988. Peter Strasser, Verbrechermenschen. Zur kriminalwissenschaftlichen Erzeugung des Bösen, Orig. 1984; Neuausgabe Frankfurt a. M. 2005, Kap. II („Der Mythos als Wissenschaft“), 41 ff. .

2 Vgl. „Das neue Kontrolldenken in der Kriminologie“, Anhang zur Neuausgabe meines Buches Verbrechermenschen, loc. cit., 229 ff. Zuerst erschienen im Kriminologischen Journal, 37/1 (2005), 39–52.

Gehirnstruktur bestimmt. Jedes Individuum ist ein gehirndeterminiertes Wesen, ich *bin* in gewissem Sinne mein Gehirn, wobei eingeräumt wird, dass die neuronale Vernetzung durch soziale Interaktionen in den ersten Kindheitsjahren bestimmend mitgeprägt wird. Doch wie es ein Forscher ausdrückte: die alte Debatte *„nature or nuture"* ist ausgestanden; *nature is nurture.*[3]

Wenn also der Mensch auch in seiner psychischen Verfassung, seinen Charakteranlagen und sozialen Neigungen, weitgehend durch seine biologische Tiefenausstattung festgelegt ist, dann erweist sich die humanistische Idee der Erziehung zur Autonomie als eine Illusion. Es besteht dann kein Grund, die Legitimität von Kontrollverfahren auf die illusionäre Annahme zu stützen, der Mensch könnte seine wahre Individualität nur ausbilden, indem er die Selbstbestimmbarkeit seines freien Willens nützt. In einem gewissen und recht fundamentalen Sinne steht der moderne Naturalismus quer zu der grundlegenden Rolle, welche der Gedanke der Autonomie in unseren westlichen Gesellschaften spielt. Und es ist noch nicht absehbar, wie diese Spannung in Zukunft modelliert werden wird; möglicherweise zuungunsten der Autonomie.

3. Die Erosion der klassischen Freiheitsidee

Moderne Demokratien westlicher Prägung sind fein ausbalancierte Gemeinschaften. Weil wir es gewohnt sind, in solchen Gemeinschaften zu leben, haben wir oft kein Gespür mehr für die Segnungen, die uns durch die historisch gewachsene Verzahnung von demokratischer Willensbildung, politischer Repräsentation, Rechtsstaatlichkeit, Grundrechten, freier Marktwirtschaft und Sozialstaatsorientierung zuteil werden. Die westlichen, zumal europäischen Demokratien seit 1945 haben es zuwege gebracht, Gesichtspunkte möglichst großer Freiheit, ökonomischen Wohlstands und sozialer Gerechtigkeit auf eine Weise simultan zu berücksichtigen, die in der Geschichte der Staaten einmalig ist.

Was wir definitiv nicht wissen, ist, ob unsere Epoche dauerhaft sein wird, ob sich der globalisierte Markt stabilisieren, die Freiheit des Einzelnen schützen, das sozialstaatliche System aufrechterhalten lässt. Was wir vermuten können – und leider müssen –, ist aber, dass das Gesamtsystem bloß unzureichend stabil gehalten werden kann, besonders wegen seiner Abhängigkeit von einer ökonomischen Basis, die sich der politischen Kontrolle entzieht, rasches Wachstum benötigt, steigende Arbeitslo-

3 Jan Volavka, „The Neurobiology of Violence. An Update", in: The Journal of Neuropsychiatry and Clinical Sciences, 11 (1999), 307–314 (313).

senraten produziert und dabei die sozialen Ungleichheiten permanent verstärkt. Mittlerweile gibt es nicht nur alarmierende Anzeichen dafür, dass die sozialstaatliche Komponente unserer Demokratien von Auszehrung bedroht ist. Es steht auch zu befürchten, dass die Praxis der Freiheit einem Wandel unterworfen ist, an dessen Ende die Idee der Freiheit selbst nicht mehr dem entsprechen wird, wofür sich die Menschen unseres Kulturkreises so lange, und zum Teil mit großen Opfern, eingesetzt haben.

Das klassische Freiheitsverständnis umfasst bekanntlich nicht nur die Grund- und Freiheitsrechte, die im Augenblick noch außer Diskussion stehen, vorbehaltlich einer gewissen Tendenz, der Furcht vor dem Terrorismus gefährliche Bauernopfer zu bringen. Denn der klassisch liberale Staat, dessen Menschenbild unverrückbar individualistisch ist – wobei sich die Freiheit des Einzelnen im Wechselspiel von rationalem Eigennutz und Gemeinwohlorientierung äußert –, versteht die Privatsphäre nicht einfach als eine Nichteingriffssphäre. Entscheidend ist vielmehr die Art des Nichteingreifens. Sie besteht, kurz gesagt, in einer *Selbstblendung des Staates.*

Das bedeutet, dass der Staat von sich aus, im Sinne einer Verpflichtung dem Bürger gegenüber, geeignete rechtliche und technische Vorkehrungen trifft, *um nicht wissen zu können,* was der Einzelne in seiner Privatsphäre tut. Dahinter steckt der Gedanke, dass die Privatsphäre sowohl vor unerwünschter Öffentlichkeit als auch vor Eingriffen staatlicher Organe schützen soll. Beispielsweise schließt mein Recht auf Freizügigkeit ein, dass ich mich – solange ich dadurch nicht andere oder die soziale Ordnung gefährde – effektiv jeder Art von Kontrolle *entziehen* darf, um unbehelligt nach meinen eigenen Vorstellungen leben und meiner eigenen Wege gehen zu können. Das schließt ein, dass die Behörden sich selbst der Möglichkeit berauben, durch das Anlegen von Datenpools oder die Verwendung von Datengenerierungs- und Datenzusammenführungstechnologien unter Umständen („wenn es die öffentliche Sicherheit erfordert“) doch Privatsphärenrekonstruktion zu betreiben.

Vergleicht man jedoch, wie dieses starke Recht auf Privatsphäre mittlerweile praktisch ausgeübt wird und welche Gedanken sich die Kontrollbehörden dazu machen, dann stößt man auf eine verwirrende Situation. Unabhängig davon, dass es in den europäischen Staaten aus guten Gründen eine allgemeine Meldepflicht des ständigen Wohnorts gibt, wird vieles, was wir tagaus, tagein tun, absichtlich oder unabsichtlich festgehalten und mehr oder minder dauerhaft gespeichert. Und in den meisten Fällen scheint uns das nicht sonderlich zu stören, es sei denn, wir sind gerade dabei, eine rechtsbrecherische Handlung zu setzen. Natürlich werden wir überwacht, wenn wir uns auf Bahnhöfen, öffentlichen Plätzen, in Banken und großen Kaufhäusern bewegen, seit einiger Zeit auch auf Autobahnen durch die Section Control, die man prak-

tisch zur Geschwindigkeitskontrolle verwenden will, aber darüber hinaus zur Komplettierung von Bewegungsprofilen einsetzen *könnte*. Immer mehr solcher Kontrollen, die eine Menge bisher ungenützter (und vom Recht vorläufig untersagter) Kontroll*möglichkeiten* einschließen, werden von Privaten etabliert, die damit ihr Eigentum oder die Sicherheit ihrer Kunden besser schützen wollen. Weshalb also sollte sich der Staat prinzipiell zurückhalten, wenn Sicherheitsargumente für die Installierung von Systemen der Bewegungs- und Aufenthaltskontrolle sprechen, die notfalls eine Identifizierung von Personen und die Erstellung von Mobilitätsprotokollen gestatten?

Ein Grund, warum der klassische Freiheitsbegriff heute obsolet zu werden beginnt, liegt in der Fülle von Datenspuren, die wir lang- oder kurzfristig an Speicherorten hinterlassen, welche primär gar nicht dem staatlichen Zugriff unterliegen und die wir oft selber nicht kennen. Gehe ich im Internet zum ersten Mal in eine elektronische Buchhandlung einkaufen, dann werde ich bei der Anmeldung über meinen Browser mit einem elektronischen Marker versehen, dessen eingebürgerter Name geeignet ist, Willkommensgefühle auszulösen, wie beim Empfang zu einer Nachmittagsjause: „Cookie". Dieser Marker erlaubt es, meine Kundenidentität festzuhalten. Was ich vielleicht nicht weiß: mein Surfverhalten während des Einkaufs kann registriert, mit meinem Namen verbunden und zu fremdnützigen Zwecken verwendet werden. Für Marketingfirmen, die auf vielen Websites Werbebanner haben, ist es unter gewissen Voraussetzungen möglich, Benutzer über einzelne Websites hinweg zu verfolgen. Obwohl Fachleute wissen, was derartige Praktiken vom Standpunkt des Datenschutzes aus *bedeuten*, besteht doch die Welt der Internetbenützer zu fast hundert Prozent aus Menschen, die *keine* Fachleute sind.

Elektronische Marker, so wird dem Konsumenten versichert, sind weitgehend harmlos, weil in ihnen keine Daten zur Privatsphäre der identifizierten Personen aufscheinen. Doch das hängt eben davon ab, wie empfindlich Online-Shopper darauf reagieren, dass unter Umständen ihr Surfprofil gespeichert und an andere weitergegeben wird. Man denke nur an Kunden, die im Netz nach pornografischen Novitäten oder Pharmazeutika Ausschau halten. Im Allgemeinen kann man sagen, dass die Menschen heute in einer Welt der Daten, Speicher und Kontrollen leben, die sie erst gar nicht mehr daran denken lässt, sich nach all den Spuren zu erkundigen (geschweige denn sich um sie zu kümmern), die sie irgendwann irgendwo hinterlassen, sobald sie sich in irgendeiner Form bemerkbar machen, sei es in einem Kommunikationssystem oder einfach in Räumen, in denen sie mit anderen interagieren.

Das hat Auswirkungen auf die herrschende Vorstellung von jener Art von Freiheit, die durch die Garantie der Privatsphäre gewährleistet werden soll. Der Einzelne ist

heute unfähig, der Archivierung seiner Daten, sei sie nun kurz- oder langfristig, erfolgreich entgegenzutreten. Denn erstens würde das bedeuten, sich sozial so gut wie *unsichtbar* zu machen, und zweitens ist für den Laien, also den durchschnittlichen Bürger, der Großteil des Archivierungsgeschehens und der daran anschließenden Möglichkeiten der Datenverknüpfung und Datenauswertung *undurchschaubar.*

Was sich daher ausbreitet, ist einerseits ein Gefühl, in nichttransparenter Weise immer mehr digitale „Abdrücke" des eigenen Lebens in immer mehr Speichern zu hinterlassen, wodurch im Gegenzug der Ruf nach einem effektiven Datenschutz zur Sicherung der Privatsphäre immer lauter wird. Andererseits jedoch scheint die Öffentlichkeit immer weniger abwehrend auf elektronische Überwachungsmethoden zu reagieren, soweit diese dazu dienen, die öffentliche Sicherheit zu gewährleisten. Denn die Sicherheit scheint in unseren hochkomplexen Gesellschaften permanent gefährdet, zurzeit namentlich durch Ausländerkriminalität und Terrorismus.

Deshalb ist man bereit, die Selbstblendungspflicht des Staates, wie sie der klassische Freiheitsbegriff fordert, zusehends gegen die Idee einer Überwachungsdemokratie einzutauschen. Von ihr wird angenommen, sie schütze die Freiheit und Integrität des gesetzestreuen Bürgers *dadurch*, dass der Staat alle notwendigen Technologien einsetzt, um die Sicherheit des Einzelnen zu gewährleisten, handle es sich nun um Telefon- oder Handyüberwachung, Nachforschungen in fremden Computern, das elektronisch unterstützte Erstellen von Bewegungs- und Persönlichkeitsprofilen, die Raster- oder Schleppnetzfahndung. Das bedeutet indessen der Tendenz nach, dass schließlich die Sicherheit gegenüber der Freiheit, ausgedrückt im Schutz der Privatsphäre, die Oberhand gewinnt. Dass jemand beim Internetsurfen auf heiklen Sexseiten oder bei einer Handyverabredung mit einer Frau, die nicht die eigene ist, im Zuge einer größeren Überwachungsoperation gegen das Kinderpornogeschäft oder einen Mädchenhändlerring gleich mitüberwacht wird, mag den sprichwörtlich anständigen Bürger kalt lassen. Zu Unrecht. Denn hier handelt es sich um ein Malheur, das jeder von uns schon deshalb auf sich beziehen sollte, weil die Grundrechte für alle gelten und ihre Verletzung im Einzelfall uns als Bürger eines freiheitlich-demokratischen Gemeinwesens kollektiv verletzt.

4. Die Notwendigkeit optionalen Räsonierens

Vor dem Hintergrund des bisher Gesagten sollte verständlich werden, warum die relative Unbedenklichkeit und unbestreitbare Sicherheitsleistung vieler biometrischer Methoden nur die eine Seite einer Medaille ist, deren andere solange nicht in den Blick gerät, als keine Kontexterweiterung hin zum Phänomen der Überwa-

chungsdemokratie stattfindet. Wichtige biometrische Methoden dienen ja generell wünschenswerten Effekten: Man kann persönliches Eigentum, einschließlich Informationen, besser schützen, indem man Computer oder Autos mit einem Fingerabdruckscanner ausrüstet. Man kann Zutrittssicherungen zu sensiblen Orten schaffen, indem man die Iris oder Handgefäßstruktur kontrolliert. Man kann die geforderte Identitätskontrolle einfacher und sicherer machen, indem man die Pässe mit biometrischen Daten ausrüstet. Kein Zweifel, das alles wirkt an der Oberfläche vertrauenserweckend, und die Politiker sehen es gerne, wenn man sie wissen lässt, dass durch die Biometrie neue Sicherheitsstandards definiert werden.

Betrachtet man allerdings die Biometrie als Teil eines in Zukunft immerhin möglichen Law-&-Order-Staates, der, statt durchgehend mit physischer Gewalt, vorwiegend mit den neuen elektronischen Technologien operiert, dann erscheint sie in einem weniger freundlichen Licht. Denn biometrische Daten generieren nicht nur Identifikationsspuren, die über das äußere Verhalten von Menschen in der Gesellschaft Auskunft geben. Sie liefern auch Informationen über Gesundheit und psychische Befindlichkeit, wobei heute noch gar nicht klar ist, welche Informationen in welcher Tiefe gewonnen werden können. Man denke beispielsweise an DNA-Screenings, wobei gerade der professionelle Datenschützer beim Ausmalen zukünftiger Szenarien nicht zu zimperlich sein sollte. Denn die Zukunft hat noch immer die kühnsten Erwartungen übertroffen.

In den Genen eines Menschen sind ja keineswegs bloß seine körperlichen Merkmale verankert, die schon an sich brisant genug sein mögen, wenn sie Rückschlüsse auf die Anfälligkeit für bestimmte Krankheiten zulassen. In den Genen eines Menschen ruht ein Großteil seines psychologischen Profils, und dessen Entschlüsselung ist, wie bereits erwähnt, ein alter Wunschtraum der Kontrollexperten. Dabei könnte die Verknüpfung genetischer Daten mit einem Gesundheits- und Risikoprofil, wie es sich aus elektronischen Krankenscheinen bei entsprechend langfristiger Datengenerierung auslesen ließe, neue Kontrollmaßstäbe setzen. Dem steht natürlich das Argument gegenüber, dass an einen solchen Eingriff in die Privatsphäre nie und nimmer zu denken sei. Doch zur politischen Klugheit gehört es, angesichts einer ungewissen Zukunft – und die Zukunft ist immer ungewiss – bei der Einführung und Handhabung neuer Technologien *optionale Szenarien* nicht aus den Augen zu verlieren.

Ich spreche jetzt als Bürger und Privatmensch, der in seiner Brieftasche eine E-Card mit sich führt. Dieser elektronische Krankenschein beinhaltet, soweit ich informiert bin, im Augenblick keine Daten, die es gestatten würden, mein Gesundheitsprofil auszulesen, Anhaltspunkte für meine chronischen Leiden, meine Süchte, meine

psychischen Pathologien zu finden oder die Anzahl meiner Krankenstände zu eruieren. Aber soweit ich ebenfalls informiert bin, *könnten* all diese Daten über meine E-Card verfügbar gemacht werden. Und in der Tat gehört einiges davon seit jeher zu den *„angedachten" Optionen*, die mit dem elektronischen Krankenschein verbunden sind, ohne dass derlei Eventualitäten vorerst an die große Glocke gehängt werden.

Könnte mein mich behandelnder Arzt aus meiner E-Card ersehen, welche Diagnosen mir bisher gestellt wurden, welche Medikamente ich bisher genommen und welchen Operationen ich mich mit welchem Erfolg bisher unterzogen habe, dann wäre es – so ein Argument, das von einschlägig befasster Seite zu hören ist – für ihn wesentlich leichter, mir eine adäquate Behandlung zuteil werden zu lassen. „Therapieoptimierung durch Datenvernetzung", lautet das Zauberwort. Dem hat man auch aus Unternehmerkreisen gleich freundlich zugestimmt. Denn auf diesem Wege könnte man Postenwerber dazu motivieren, ihre E-Card quasi als medizinisches Empfehlungsschreiben zur Einlesung vorzulegen, natürlich auf streng freiwilliger Basis…

Gewiss, das ist ein Szenario, welches im Moment so weit von der Realität entfernt ist, dass man es im Tone der Ironie zu schildern vermag. Doch wer weiß wie lange noch? In den USA hat man sich bereits daran gewöhnt, von einer „post-9/11 world" zu sprechen, also der Welt nach dem Terroranschlag auf das World Trade Center am 11. September 2001. Dies ist die Welt der *Domestic Surveillance*, wo es dem Staatsicherheitsdienst NSA (National Security Agency) erlaubt wurde, amerikanische Bürger ohne Gerichtsbeschluss abzuhören, falls der Verdacht besteht, sie seien auf irgendeine Weise mit irgendwelchen Leuten in Verbindung, die in irgendeiner Weise im Verdacht stehen, irgendwie in den internationalen Terrorismus verwickelt zu sein.

Erst jüngst wurde eine Klage in Portland, Oregon, auf der Basis konkreter Beweise eingereicht, weil die Anwälte einer islamischen Wohltätigkeitsorganisation abgehört wurden, womöglich bloß deshalb, weil sie Anwälte einer islamischen Wohltätigkeitsorganisation waren.[4] Aus den vielen Maßnahmen, die Präsident George W. Bush unter dem Titel der Domestic Surveillance zusammenfasste und noch zusammenfassen will, sticht jene besonders hervor, die das FBI, also eine Institution der inneren Sicherheit, ermächtigen soll, Informationen über US-Bürger zu beziehen,

---

4 Berichtsampler „The Debate over Domestic Surveillance" in der On-line-Ausgabe des National Public Radio (www.npr.org), 2. März 2006: „Oregon Lawsuit Challenges Domestic Spying": „A lawsuit filed in Portland, Ore., alleges that the federal government illegally wiretapped lawyers for an Islamist charity based in that state. As Colin Fogarty of Oregon Public Broadcasting reports, it isn't the first legal challenge to the warrantless surveillance program but it's the first to claim specific documented evidence."

die vom Pentagon, dem CIA und anderen geheimdienstlichen Organisationen gesammelt wurden.[5] Diese naheliegende, aber gegen den Privacy Act von 1974 verstoßende Initiative beruht ebenfalls auf dem einfachen Prinzip der Kontrolloptimierung durch die Zusammenlegung oder Vernetzung von Daten, die zunächst aus Gründen des Schutzes der Privatsphäre getrennt archiviert wurden.

Deshalb ist jene Kritiklinie nicht einfach abzuweisen, die auch mit Bezug auf das Archivieren biometrischer Daten darauf hinweist, dass bisher noch jedes Datenarchivierungsmonopol über kurz oder lang *korrumpierte*. Das hat verschiedene Gründe, von denen die explizit geäußerte politische Absicht immerhin die Schranke der Gesetzgebung überwinden muss. Aus der Vergangenheit weiß man jedoch, dass häufig Daten, die von einer berechtigten Stelle angeblich sicher verwahrt wurden, in nicht autorisierte Kanäle einflossen und schließlich im Internet verfügbar waren. Spätestens dann kann nicht mehr auf die gesicherte Datenebene zurückgekehrt werden. Es ist nicht einzusehen, dass für biometrische Informationen ausgeschlossen werden darf, was heute – um ein Beispiel aus einem ganz anderen Bereich zu zitieren – mit Kinofilmen passiert, die auf ein großes Publikumsinteresse stoßen. Von solchen Filmen gibt es im Internet häufig illegale elektronische Kopien, *bevor* noch eine Freigabe für die Kinoöffentlichkeit erfolgte.

Wie ist das möglich? Die Antwort lautet einfach: Daten ohne Zutritt sind wertlos, aber durch den menschlichen Faktor, der über Zutrittsberechtigungen ins Spiel kommt, wird auch dem Missbrauch das Tor geöffnet, von den unzähligen Möglichkeiten unberechtigter Zugriffe auf Daten ganz zu schweigen. Während es gegen die widerrechtliche Verwendung von Daten durch Zugriffsberechtigte kein technisches Wundermittel gibt, lässt der Versuch Zutrittsunberechtigter, an Daten zu gelangen, die Sicherungsspezialisten zur Höchstform auflaufen. Die Folge: es beginnt ein hochtechnischer Wettlauf zwischen den Möglichkeiten, auf geheime Daten Attacken zu starten, und der Entwicklung von Schutzmaßnahmen zur Attackenabwehr.

An der Technischen Universität Graz arbeitet eine Gruppe von Wissenschaftlern, die sich auf die Entschlüsselung jener Chip-Codes spezialisiert hat, durch die sich Produkte wie Bankomatkarten, Kreditkarten, Pässe oder E-Cards authentifizieren. Gelingt die Attacke, dann wird es möglich, auch andere Details elektronischer Karten auszuspionieren, einschließlich der Personal Identification Number (PIN), über

---

5 Bericht der Washington Post, 27. November 2005, Seite A06. Zitat: „The Pentagon has pushed legislation on Capitol Hill that would create an intelligence exception to the Privacy Act, allowing the FBI and others to share information gathered about U.S. citizens with the Pentagon, CIA and other intelligence agencies, as long as the data is deemed to be related to foreign intelligence."

welche sich die Zutrittsberechtigten definieren.[6] Freilich erforscht dieselbe Gruppe von Wissenschaftlern solche Möglichkeiten, um zusammen mit den Herstellern von Chipkarten attackensichere Zutrittssperren zu entwickeln. Das alles spielt sich in einem informationslogistisch heiklen Bereich ab, der zugleich öffentlich und privat finanziert wird, was bedeutet, dass keineswegs alle Ergebnisse publiziert werden. Doch selbst dem Laien, der weit von einem Verständnis der hier ablaufenden Dinge entfernt ist, muss einleuchten, dass Forschungen wie die eben erwähnten überall, wo man an der Entschlüsselung geheimer Daten interessiert ist, staatliche Sicherheitsdienste nicht ausgenommen, auf Interesse stoßen.

Allgemein lässt sich sagen, dass es Methoden gibt, die dem sanften Überwachungsstaat eher zuarbeiten als andere. Elektronische Pässe mit biometrischen Merkmalen sind bloß *ein* Beispiel neben E-Cards oder so genannten Bürgerkarten, mit denen man seine Amtsgeschäfte in Hinkunft elektronisch wird abwickeln können. Für jedes einzelne Produkt dieser neuen Dokumentengeneration sprechen gute Gründe. Im Fall elektronischer Pässe ist es ihre leichtere Handhabbarkeit an den Grenzen und auf Flughäfen (und damit eine raschere Abfertigung der Reisenden), ihre schwerere Fälschbarkeit und nicht zuletzt ihr überwachungstechnischer Vorteil. Doch man muss zugleich sehen, dass der herkömmliche Pass ebenfalls funktional war, während mit den neuen Pässen auch neue Probleme und Risiken auftreten. Davon bleiben selbst die Geheimdienste nicht unberührt, die in Zukunft, wegen der Fälschungsschwierigkeit elektronischer Pässe, ihre Agenten vielleicht mit den elektronischen Merkmalen real existierender Bürger auf Reisen schicken werden…

Unter einer folgenorientierten Betrachtung wären jedenfalls die Vor- und Nachteile elektronischer Dokumente – ebenso wie der Elektronisierung von Verwaltungsakten und der Archivierung personbezogener Informationen in elektronischen Datenbanken – auch und besonders hinsichtlich einer möglichen Verschärfung des politischen Klimas abzuwägen. Stichwort: Sicherheitsoptimierung durch Intensivierung der Ausforschungs- und Überwachungstechnologien. Die Tendenz zur Domestic Surveillance erscheint ja mittlerweile vielen Verantwortungsträgern keineswegs als eine Entartung des modernen Staates, sondern vielmehr als der legitime Ausdruck seines Sicherungsbedürfnisses angesichts der Globalisierung nicht nur der Märkte, sondern auch des Verbrechens und des Terrors.

---

6 Vgl. Stefan Mangard: (1) Calculation and Simulation of the Susceptibility of Cryptographic Devices to Power-Analysis Attacks, Master Thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, 2002; (2) Securing Implementations of Block Ciphers against Side-Channel Attacks, Ph.D. Thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, 2004.

5. Plädoyer für eine Moratoriumsmentalität

Einer der Verfasser des aktuellen Wikipedia-Artikels zum Stichwort „*Biometrie*“[7] sah sich veranlasst, uns folgende Frohbotschaft zu übermitteln: *„Auch österreichische Parlamentarier stehen neuen biometrischen Verfahren ohne Skepsis gegenüber. Das Parlament wurde mit einem Funknetz WLAN ausgestattet und die Abgeordneten bekamen Laptops mit einem Fingerabdruckscanner. An einem Seiteneingang wurde eine biometrische Gesichtserkennung installiert. Seit Januar 2005 wird der Zutritt zum Bundesministerium für auswärtige Angelegenheiten durch Venenerkennung kontrolliert.“* Als Österreicher muss ich gestehen, dass mich die hier – wohl ironisch akzentuierte – Skepsis-Resistenz unserer Parlamentarier gegenüber der Biometrie mit Sorge erfüllt. Oder hat diejenige Person, die diesen Absatz verfasste, eigenem Wunschdenken nachgegeben – bis hin zur Venenerkennung?

Man braucht gegenüber den Vorteilen der Implementierung biometrischer Verfahren in unseren sozialen Verkehr durchaus nicht blind zu sein; und den österreichischen Abgeordneten wäre auch die kindliche Freude zu gönnen, sollten sie stolze Besitzer von „Laptops“ mit einem Fingerabdruckscanner sein. Wesentlich scheint, dass sie sich in ihrer Rolle als Gesetzgeber des Umstandes bewusst bleiben, dass noch niemals in der Geschichte der Menschheit eine Technologie entwickelt worden ist, deren Möglichkeiten schließlich nicht in vollem Umfange ausgenützt wurden.

Heute trägt man Eulen nach Athen, wenn man sagt: Sobald die Atombombe technisch möglich war, musste allen Verantwortlichen klar sein, dass sie irgendwann zur Explosion gebracht wird. Und es gibt Zyniker – oder sind es nur Realisten? –, die sagen, dass die Großmächte dieser Welt von Zeit zu Zeit einen Krieg schon deshalb brauchen, um ihre neuen Waffensysteme zu testen. Ebenso darf man als sicher voraussetzen, dass, sobald das Klonen von Menschen technisch machbar ist, es auch gemacht werden wird, mögen noch so viele Humanisten und religiös Bewegte davor warnen.

Daraus lernen wir, falls wir überhaupt lernbereit sind, dass alles, was in der Biometrie drinnen steckt, auch irgendwann technisch umgesetzt und zumindest zeitweise von privaten Profiteuren und politischen Ideologen benützt werden wird. Zusammen mit all den anderen modernen Datengewinnungs- und Datenauswertungsmethoden ergibt sich daraus eine ernstzunehmende Gefahr für die Sicherung der Privatsphäre des Einzelnen und darüber hinaus – wie das Beispiel USA lehrt – allgemein

---

7 http://de.wikipedia.org/wiki/Biometrie (Stand: März 2006)

eine Gefahr für die Grund- und Freiheitsrechte, die zentral unser Verständnis von Demokratie betreffen.

Was wir also – neben reformfreudigen Politikern und einfallsfreudigen Sicherheitstechnikern, an denen wahrlich kein Mangel besteht – dringend brauchen, das sind kritische Politologen und Sozialwissenschaftler, die uns den Sinn der Demokratie als eines gemeinschaftlichen Orts der individuellen Freiheit immer wieder engagiert nahe bringen. Erst dann nämlich, unter der möglichen Perspektive eines Verlusts, werden wir das Universum der elektronischen Kontrollmethoden realistisch beurteilen. Diese Methoden, die sich rasch formieren, weisen weniger in Richtung einer Stärkung der liberalen Position, sondern in jene andere Richtung, die ich, mangels eines besseren Begriffs, als „Überwachungsdemokratie“ bezeichnete. Ich denke, dass wir erst lernen müssen, die Gefahren des sanften Überwachungsstaates richtig einzuschätzen. Und erst dann werden wir imstande sein, eine intuitive Vorsicht zu entwickeln – gleichsam eine unseren Bedrohungen angemessene Moratoriumsmentalität.

Peter Schaar

Meine sehr verehrten Damen und Herren, Sie haben die Möglichkeit sich jetzt zu äußern. Seien es eigene Beiträge oder Fragen an Herrn Prof. Strasser; wie gesagt, nachher haben Sie noch ausführlicher Gelegenheit, sich zu äußern und Fragen zu stellen.

Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit:

Herr Prof. Strasser, nur eine Verständnisfrage zu Ihrem hochinteressanten Vortrag: Habe ich Sie recht verstanden, dass in Österreich die Registrierung und Überwachung von menschlichen Bewegungen schon soweit fortgeschritten ist, dass dort eine Venenerkennung stattfindet ? Wenn ja, wie hat man sich das vorzustellen. Das kennt man in Deutschland nämlich noch nicht.

Peter Strasser:

Ja ich muss gestehen, bin auch etwas desperat. Ich hab das zitiert. Das ist aus diesem Wikipedia-Artikel zitiert. Ich weiß nicht, wer den geschrieben hat. Wir wissen ja auch, dass die Wikipedia nicht immer eine verlässliche Quelle ist. Es könnte auch ein durchaus irgendjemand gewesen sein, der unseren Parlamentariern bescheinigen wollte, sie seien in einer Weise unkritisch solchen Dingen gegenüber, dass sich eine Satire anbietet. Das alles habe ich natürlich nicht nachgeprüft. Natürlich weiß man: Es gibt Parlamentarier, die solchen Dinge gegenüber - weil sie sich schon aus Gründen der Modernität dazu verpflichtet fühlen - so aufgeschlossen gegenüberstehen, dass man sagen könnte, es wäre besser, wenn ein bisschen mehr kritisches Bewusstsein vorhanden wäre, auch wenn man möglicherweise stolz darauf ist, eine solche neue Technologie zu haben.

Peter Schaar:

Gibt es noch eine weitere Wortmeldung? Wenn das nicht der Fall ist, dann gehen wir über zu dem zweiten Vortrag des Tages. Vielleicht kann Herr Prof. Busch ja auch noch etwas zu der Frage sagen, weil er ja auch gerade im Bereich der Technologie ein ausgewiesener Experte ist. Nochmals vielen Dank Herr Prof. Strasser. Ich

denke es war eine gute Einführung hier mal über den normalen erwarteten Tellerrand der Biometriediskussion hinauszusehen. Denn wir haben es mit einer Technologie zu tun, die sich nicht in einem luftleeren Raum, sondern in einem sozialen und historischen Kontext entwickelt und leider greift die Diskussion sehr häufig zu kurz. Ich will mich da überhaupt nicht ausnehmen. Wir sehen einerseits die rechtlichen Anforderungen, andererseits die technologischen Aspekte und dann häufig die Anforderungen derjenigen, die als Bedarfsträger auftreten. Wir sehen aber letztlich nicht immer den sehr viel größeren Rahmen, der doch aus meiner Sicht letztlich entscheidend ist. Nämlich wie sich unsere Gesellschaft weiter entwickelt. Wichtig ist auch, dass wir die Technologie kennen. Darüber erwarte ich mir neue Erkenntnisse von Ihnen. Herr Prof. Busch, Sie haben das Wort.

Biometrische Verfahren – Chancen, Stolpersteine und Perspektiven

*Christoph Busch**

Einführung

Der Laptop, auf dem diese Zeilen in ein Word-Dokument getippt werden, ist - wie viele andere Laptops auch – (noch) nicht mit biometrischen Verfahren abgesichert. Biometrisch gesichert sind jedoch einige der physikalischen Zugangskontrollen, die ich regelmäßig nutze – beispielsweise Zugangstüren zum Mitarbeiterbereich im Fraunhofer-Institut für Graphische Datenverarbeitung IGD. Die in diesem Artikel beschriebenen Perspektiven sind daher nicht nur theoretischer Natur sondern auch durch einige Jahre an praktischer Erfahrung geprägt.

Warum beschäftigten wir uns überhaupt mit biometrischen Verfahren? Aus einer Technikperspektive betrachtet liegt der Grund darin, dass die klassischen Authentisierungsmechanismen, wie beispielsweise die Wissensauthentisierung (Passwort), die Authentisierung über Token (Schlüssel) oder dergleichen mit eindeutigen Nachteilen versehen sind. Passwort und Token kann man – meist unter Missachtung einer Sicherheitsrichtlinie – weitergeben, man kann sie vergessen oder verlieren. Um bei der ansteigenden Zahl der logischen und physikalischen Zugangskontrollen dem Verlust vorzubeugen, werden oft ungeeignete Speicherorte oder identische Passworte verwendet [NTA2002]. In einer ersten Betrachtung der biometrischen Verfahren stellen wir fest, biometrische Charakteristika können wir hingegen nicht vergessen, wir können sie auch nicht delegieren. Biometrische Verfahren ermöglichen die Feststellung der Identität (Authentisierung) einer Person in der logischen und physikalischen Zugangskontrolle und die Biometrie kann Probleme anderer Authentisierungsverfahren lösen.

* Christoph Busch ist Professor im Fachbereich Media an der Hochschule Darmstadt. Am Fraunhofer-Institut für Graphische Datenverarbeitung IGD ist er tätig in der biometrischen Forschung und Standardisierung unter anderem als Obmann im DIN-NI37 und in der ISO/IEC JTC1 SC37 (Biometrics).

Schließlich ist die Biometrie auch im Zusammenhang mit der gewünschten Steigerung der Inneren Sicherheit in Deutschland und Europa von Bedeutung: In der Diskussion um *Machine Readable Travel Documents* (MRTD) spielen einerseits die neuen Rahmenbedingungen für elektronische EU-Pässe (ePass), wie sie durch die Festlegungen der International Civil Aviation Organization (ICAO) [ICAObd] erfolgten, eine wichtige Rolle. In der Umsetzung einer entsprechenden EU-Verordnung [EU2004] wird in den bundesdeutschen Reise-Pässen seit November 2005 zunächst das Passbild elektronisch gespeichert. Ab 2007 sollen dann auch Fingerbilder im ePass gespeichert werden. Andererseits werden auch ID-Karten in naher Zukunft mit Biometrie erweitert werden. So wurde vorbereitend bereits im Rahmen der Europäischen Standardisierung im CEN Technical Committee 224 eine European Citizen Card genormt [CEN2005], die einen biometrischen Vergleich in der Karte selbst ermöglichen wird. Die genaue Ausprägung des neuen Bundesdeutschen Personalausweises, der in 2007 eingeführt werden soll, wird allerdings derzeit noch diskutiert.

Was ist Biometrie?

In der Internationalen Standardisierung wurde der Begriff biometrics wie folgt definiert: "*automated* recognition *of individuals based on their behavioural and biological characteristics*" [ISO2006a]. Biometrische Verfahren analysieren also das Verhalten des Menschen und/oder die Eigenschaft der biologischen Charakteristika. Die biologischen Charakteristika gliedern sich einerseits in anatomische Charakteristika – die geprägt werden durch Strukturen des Körpers (nicht nur der menschlichen Oberfläche!) und andererseits in physiologische Charakteristika – die geprägt werden durch Funktionen des Körpers (zum Beispiel die Erkennung einer Person durch Analyse ihrer Stimme).

Der Vorgang der biometrischen Authentisierung liefert eine eindeutige Verknüpfung einer Person mit ihrer Identität unabhängig davon, wo diese Identität gespeichert ist - auf einem vorgelegten nachweisbar authentischen Dokument oder in einer gegebenenfalls zentralen Datenbank. Der Vorgang der biometrischen *Wieder*erkennung lässt sich in die folgenden Schritte untergliedern:

- Erfassung der biologischen Charakteristika mit geeigneten Sensoren (Kamera, Mikrofon etc.) und Speicherung als digitale Repräsentation.
- Vorverarbeitung zur Datenverbesserung oder –bereinigung.
- Merkmalsextraktion zur signifikanten Beschreibung der Muster.
- Vergleich der Merkmale mit dem Referenzmuster.

Der Vorgang bedingt, dass grundsätzlich alle Teilnehmer vorab eingelernt wurden (Enrolment) um die notwendigen Referenzdaten zu bilden. Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen Dokument (zum Beispiel dem ePass) kombiniert werden, kann das Referenzbild beispielsweise auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1 Vergleich). Bei einem Identifikationssystem hingegen wird das erfasste Bild mit vielen eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster (der *Best Match*) ermittelt (1:n Vergleich). Die Ähnlichkeit zwischen präsentiertem Bild und dem Best Match muss jedoch ein definiertes Mindestmass erreichen, damit eine zuverlässige Zuordnung der mit dem Referenzbild verbundenen Identität vorgenommen werden kann.

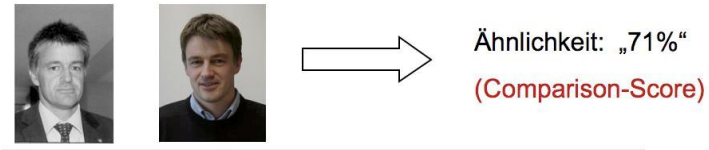


Abbildung 1: Biometrische Verifikation

In Abbildung 1 wird bereits eine der Herausforderungen an ein biometrisches Verifikationssystem deutlich, die vielleicht auch als Stolperstein bezeichnet werden kann: Als Ergebnis des Vergleiches eines präsentierten (aktuellen) Bildes mit einem Referenzbild erhalten wir einen Ähnlichkeitswert (Comparison Score). Es wird die Übereinstimmung beider Bilder festgestellt, wenn der Ähnlichkeitswert einen definierten Schwellenwert überschreitet. Hat die Person seit der Aufzeichnung des Referenzbildes durch natürliche Alterung Ihr Aussehen verändert, so steigt die Wahrscheinlichkeit, dass der Schwellenwert nicht mehr erreicht werden kann. Das in Abbildung 1 gezeigte Referenzbild hat ein Alter von nur fünf Jahren. Nach den geltenden Regelungen sind Pässe allerdings zehn Jahre gültig. Die Frage, ob alte Referenzen noch zu ähnlich guten Comparison Scores führen, wie sie bei neuen Referenzen erzielt werden können, ist heute schwer zu beantworten, da bisher keine Testdaten in ausreichender Qualität über einen entsprechend langen Zeitraum erfasst wurden.

Chancen

Die Diskussion zur Biometrie berührt verschiedene Szenarien. Ein bereits angesprochenes Szenario ist der neue ePass. In der Diskussion um die technologische Ausprägung haben uns viele Themen zu den Datenformaten der Referenzdaten, der Speicherform auf dem Token und den Kommunikationsprotokollen beschäftigt.

Welche Chancen in der Biometrie liegen erkennen wir, wenn wir die Malheure – wie Herr Strasser es so schön formuliert hat – im täglichen Leben betrachten und analysieren, ob die Biometrie eine Lösung für das Problem bietet. Ein Problem - sagen wir eine Herausforderung - die auf uns zukommt, ist die Frage der Beschleunigung der Grenzkontrollen. Diese Thematik wird in Anbetracht des unglaublich wachsenden Verkehrs an den Flughäfen immer wichtiger und zudem noch verstärkt durch die neuen Flugzeugmodelle, die in Kürze auch operativ im Einsatz sein werden. Die australische Regierung hat sich schon vor mehr als vier Jahren mit dem Thema befasst, da die Problematik insbesondere in Sydney sehr massiv ist. Durch die geographische Lage des australischen Kontinents kommen alle internationalen Flüge in einem sehr kurzen Zeitfenster am frühen Morgen an. Es gibt weder einen örtlichen noch einen zeitlichen Spielraum, die bisherigen Grenzkontroll-Prozesse zu erweitern. Man hat sich daher in Sydney überlegt, ob es möglich ist, mit einer biometrisch gestützten Grenzkontrolle die Transaktionsprozesse an den Grenzen schneller zu gestalten. Aus dieser Überlegung heraus entstand das SmartGate Projekt, welches das Ziel verfolgt die Prozesse einfacher/schneller und sicherer zu gestalten [SmG2004]. Die Analyse der Untersuchungs-Daten aus dem ersten Betriebsabschnitt des SmartGate-Systems im Jahre 2004 hat unter anderem die Transaktionszeiten der Biometrie-gestützten Grenzkontrolle im Vergleich mit den Transaktionszeiten von Reisenden in den manuellen Abfertigungen ermittelt. Das Ergebnis zeigt eine Verbesserung von 48 Sekunden auf 17 Sekunden für eine biometrische Grenzkontrolle, die zwar als Verifikation ausgeprägt ist – jedoch noch Datenbank gestützt realisiert wurde. Ende Mai 2006 wurde ein internationales ePass Interoperability Test Event in Berlin durchgeführt [DIN2006]. Dort wurden allerdings lediglich Nettozeiten mit ca. 6 Sekunden für das reine Auslesen aus einem mit Basic Acces Control abgesicherten Reisepass bestimmt. Für eine verlässlichere Bewertung sind weitere Vergleichsmessungen von Bruttozeiten (Auslesen der biometrischen Referenzdaten und biometrischer Vergleich) erforderlich. Ob es letztlich zu einer Prozessbeschleunigung kommen kann wird aber auch von der Ausgestaltung des Workflows an der Grenze abhängen, d.h. ob die biometrische Passkontrolle ersetzend oder zusätzlich zur manuellen Passkontrolle eingesetzt wird, oder ob es wie

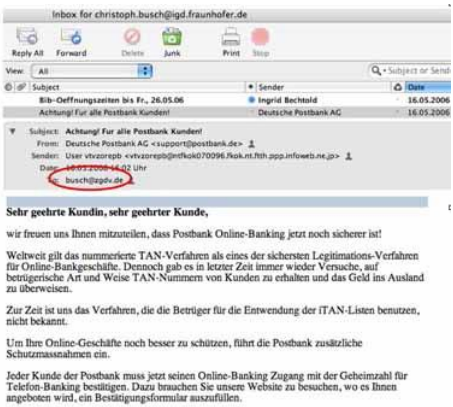
beim SmartGate-System teilautomatisierte Kontrollspuren geben wird (siehe Abbildung 2)

Abbildung 2: Teilautomatisierte biometrische Grenzkontrolle SmartGate, Sydney

Es sei angemerkt, dass für die erste Option die technischen Voraussetzungen derzeit nicht gegeben sind. Dennoch hat das Szenario das Potential einer Prozessoptimierung, wenn die Kinderkrankheiten der ersten Installationen einmal überwunden sind.

Das zweite Szenario, das ich hier betrachte, ist die elektronische Signatur, die nach der Signaturverordnung dann aktiviert werden kann, wenn der Signaturschlüssel durch eine sichere Authentisierung frei geschaltet wird: Authentisierung durch i) Besitz und Wissen oder durch ii) Besitz und ein oder mehrere biometrische Merkmale (SigV §15 Abs.1) [SigV2001]. Zu diesem Szenario möchte ich folgende Begebenheit berichten: Vor einigen Jahren beteiligte sich ein mittelständiges Unternehmen an einem Projektantrag für die EU-Kommission. Damals hatte die EU-Kommission zur Förderung der elektronischen Signaturen dazu aufgefordert, die Anträge elektronisch zu unterschreiben. Projektanträge werden in der Regel am letzten Tage vor der Abgabefrist fertig (wie übrigens genauso auch Folien zu Vorträgen und Beitragseinreichungen zu Konferenzen). In dem besagten Konsortium war einer der Partner am Abgabetag auf Dienstreise und beruhigte aber seine Partner im Konsortium etwa mit den Worten: "*Das ist kein Problem - die elektronische Signatur kann meine Sekretärin leisten. Sie hat die Karte und sie hat das Passwort*". Auf diesem Weg wurde das Verfahren auch abgewickelt. Meine damalige Vermutung, dass es sich um einen Einzelfall handele, musste ich mittlerweile korrigieren, nachdem ich Berichte von Mitarbeitern aus großen Unternehmen gehört habe, die das Verfahren als gelebte Praxis berichten. Manch einer mag die geschilderte Bege-

benheit so bewerten: "dies ist kein Thema für die Biometrie. Das kann man durch Awareness-Maßnahmen, also durch Aufklärung erledigen *("Die Leute müssen wissen, dass es so nicht geht").* Mir stellt sich dabei jedoch die Frage: Wenn es nach Signaturverordnung für die Kombination zwischen Besitz und Biometrie sichergestellt sein muss, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist, warum ist es dann für die andere Kombination aus Besitz und Wissen nicht verpflichtend, dass dieser Missbrauch ausgeschlossen wird?


Inbox for christoph.busch@igd.fraunhofer.de

Reply All Forward Delete Junk Print Stop

View: All

Subject | Sender | Date

Bib-Oeffnungszeiten bis Fr., 26.05.06 — Ingrid Bachtold — 16.05.2006

Achtung! Fur alle Postbank Kunden! — Deutsche Postbank AG — 16.05.2006

Subject: Achtung! Fur alle Postbank Kunden!

From: Deutsche Postbank AG <support@postbank.de>

busch@egdv.de

Sehr geehrte Kundin, sehr geehrter Kunde,

wir freuen uns Ihnen mitzuteilen, dass Postbank Online-Banking jetzt noch sicherer ist!

Weltweit gilt das nummerierte TAN-Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschäfte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrügerische Art und Weise TAN-Nummern von Kunden zu erhalten und das Geld ins Ausland zu überweisen.

Zur Zeit ist uns das Verfahren, die die Betrüger für die Entwendung der iTAN-Listen benutzen, nicht bekannt.

Um Ihre Online-Geschäfte noch besser zu schützen, führt die Postbank zusätzliche Schutzmassnahmen ein.

Jeder Kunde der Postbank muss jetzt seinen Online-Banking Zugang mit der Geheimzahl für Telefon-Banking bestätigen. Dazu brauchen Sie unsere Website zu besuchen, wo es Ihnen angeboten wird, ein Bestätigungsformular auszufüllen.

Abbildung 3: Beispiel einer Phishing-Mail

Ein anderes Beispiels-Szenario: Am 16. Mai 2006 bekam ich die in Abbildung 3 dargestellte E-Mail - vermeintlich von der Postbank. Der dargestellte Text lässt vermuten, das diese E-Mail mit hoher Wahrscheinlichkeit nicht von der Postbank versandt wurde. Da ich zudem auch kein Konto bei der Postbank habe, sah ich mich auch nicht veranlasst, den Server zu besuchen und dort Informationen zu hinterlassen. Zwei Dinge beunruhigen mich: Zum einen wird hier eine E-Mail-Adresse verwendet, die ich seit dem 1. Oktober 1997 nicht mehr verwende und die auch nicht mehr im Internet verfügbar und greifbar ist. Dies zeigt die Nachhaltigkeit der Adressensammlungen. Zum anderen nimmt nicht nur die Anzahl dieser Phishing-Mails dramatisch zu, sondern auch die daraus abgeleiteten Betrugsdelikte. Am gleichen Tage, dem 16. Mai, wurde die neue Kriminalstatistik für das Jahr 2005 vorgestellt [BKA2006]. Während die Kriminalitätsrate in Deutschland insgesamt gesunken ist, nahm der Computerbetrug nach § 263a um 11,9 Prozent auf 15.875 Fälle zu und der Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten stieg um 21,3

Prozent auf 5.788 Fälle[1]. Auch hier stellt sich die Frage, wie das Problem gelöst werden kann. Der Weg zurück zur "Filiale an der Ecke", in der man die Banktransaktionen in Auftrag gibt, ist schon aus ökonomischen Gründen nicht realisierbar. Es wird beim Internetbanking bleiben – dieses muss aber sicher ausgestaltet werden. Optimistisch betrachtet ist die Spezifikation des neuen digitalen Personalausweises (DPA) ja noch nicht abgeschlossen. Vielleicht lässt sich die Herausforderung langfristig damit lösen, dass man einen digitalen Personalausweis mit biometrischer Authentisierung für das Internetbanking einsetzt.

Standards und Tests

Oft wird berichtet, biometrische Systeme seien noch nicht gut genug für den praktischen Einsatz. Die Frage nach den Fehlerraten aktueller Systeme lässt sich durch Tests der Erkennungsleistung (Biometric Performance) beantworten. Weiter wird berichtet, "Standards existieren noch nicht!". Nachdem erst im Jahr 2002 das internationale Standardisierungcommittee SC37 gegründet wurde[2], welches die Biometriestandardisierung betreibt, konnten schon im Sommer 2005 nach einer sehr kurzen Bearbeitungszeit die ersten Standards publiziert werden [ISO2005a], [ISO2005b], [ISO2005c], [ISO2005d]. Sie sind nun verfügbar und können in Anwendungen integriert werden.

Die Standardisierung im Bereich der Informationstechnologie wird erarbeitet von einem Joint Technical Committee (JTC) zwischen der International Organization for Standardizaton (ISO) und der International Electrotechnical Commission (IEC). Ein wichtiger Teil der Arbeit des JTC1 Subcommittees SC37 ist es, Datenaustauschformate zu formulieren, nach denen die Repräsentation einer biometrischen Charakteristik, zum Beispiel ein Gesichtsbild, das Bild eines Fingerabdrucks oder eines Irismusters, in einem spezifizierten Datensatz kodiert werden kann. Dieser Datensatz kann dann als Referenz in einer SmartCard oder in einer Datenbank abgelegt werden. Wenn es sich um ein offenes System handelt, muss diese Referenz interoperabel sein, d.h. ein anderer Hersteller muss das Format des Datensatzes lesen und verstehen können und zudem auf derartigen Daten eine gute Erkennungsleistung herstellen können.

---

1 Dazu schreibt die Arbeitsgruppe Identitätsschutz im Internet unter https://www.a-i3.org/content/view/706/28/ "Nach Angaben des BKA ist insbesondere das Phishing durch die ständige Zunahme des Online-Banking zu einem 'gefährlichen Kriminalitätsphänomen' geworden"

2 ISO/IEC JTC 1 on Information Technology Subcommittee 37 on Biometrics (http://www.jtc1.org)

Bei der Spezifikation des ePasses war die Interoperabilität ein sehr hohes Ziel, so dass zwei bildbasierte Standards eingeflossen sind: Das ist einerseits der Standard ISO/IEC IS 19794-5 zur Speicherung von Gesichtsbildern, der derzeit schon umgesetzt wird und andererseits der Standard ISO/IEC IS 19794-4 zur Speicherung von Fingerbildern, die dann ab 2007 in den Pässen ergänzt werden.

Das Standardisierungsgremium hat sich weiterhin damit beschäftigt, wie die Repräsentation einer biometrischen Charakteristik durch die Berechnung eines Merkmalvektors als kompakter Datensatz (*Template*) kodiert werden kann, wobei die Interoperabilität nicht eingeschränkt werden soll.

Die Abbildung 4 zeigt links ein Fingerbild wie es entsprechend 19794-4 gespeichert werden kann. Mit verschiedenen Bildverarbeitungsoperationen kann aus diesem Fingerbild das Skelett der Papillarlinien (Ridge) abgeleitet werden. An den Verzweigungs- und Endpunkten der Linien werden als signifikante Merkmale sog. Minutien platziert.

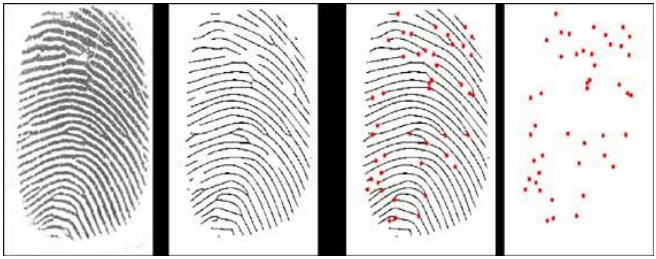


Abbildung 4: Extraktion von Minutien aus einem Fingerbild

Die Punktwolke aller Minutien (Abb.4 rechts) repräsentiert den ursprünglichen Fingerabdruck in einer sehr kompakten Form, wobei für jede einzelne Minutie die Koordinate, der Richtungswinkel der Papillarlinie und einige Zusatzinformationen wie beispielsweise der Typ der Minutie (Endpunkt oder Verzweigungspunkt) im Template gespeichert werden. Der entsprechende "Minutien-Standard" wird als ISO/IEC IS 19794-4 geführt.

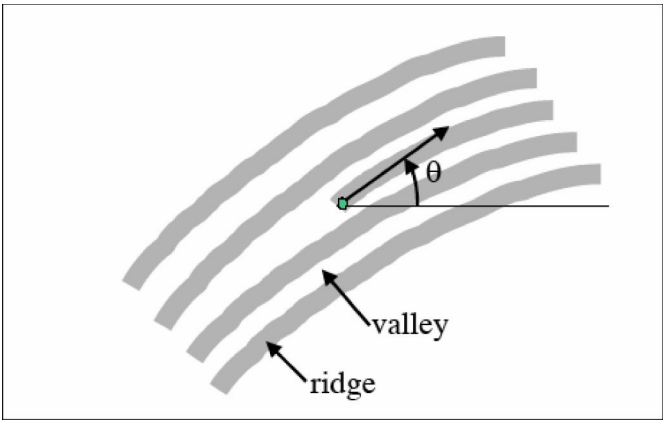


Abbildung 5: Minutie am Endpunkt einer Papillarlinie

Es liegt in der Natur der Sache, dass zur Speicherung der Datensätze nach 19794-4 kleinere Datenspeicher verwendet werden können bzw. bei einer festen Größe des Datenspeichers mehrere Referenzen abgelegt werden können. Die Verwendung mehrerer Referenzen zu einer Person (z.B. drei Aufnahmen des Gesichtes aus mehreren Posen oder Minutien von allen zehn Fingern) kann dann zur Steigerung der Erkennungsleistung genutzt werden. Eine der ersten Anwendungen dieses Datenformates war die Identifikationskarte für Seefahrer, die von der International Labour Organization (ILO) mit einer Vorversion des Minutien-Standards schon im Herbst 2004 getestet wurde. Bei diesen Tests zeigten sich zunächst Probleme, da die Datensätze, die nach diesem Standard gespeichert wurden, nur eingeschränkt interoperabel waren [ILO2004]. Die einzelnen Datenfelder waren zwar auslesbar und die Implementierung augenscheinlich richtig, jedoch war die Erkennungsleistung auf Datensätzen von Fremdherstellern in der Regel sehr gering. Die Gründe für diese anfänglichen Probleme lagen im Wesentlichen in einer unterschiedlichen Auslegung des Standardtextes bei der Spezifikation einzelner Datenfelder, was mittlerweile in Zusammenarbeit mit den Herstellern behoben werden konnte, wie die neueren ILO-Tests zeigen [ILO2005], [ILO2006]. Ein ganz ähnlicher Ansatz wurde vom National Institute of Standards and Technology (NIST) im *Minutiae Interoperability Exchange Test* (MINEX) verfolgt [NIST2006]. Dieser Test ist eindrucksvoll, denn

a) die Ergebnisse sind sehr positiv und zeigen, dass Interoperabilität sowohl mit bildbasierten als auch mit templatebasierten Referenzen erreichbar ist
b) die Ergebnisse basieren auf der größten Zahl von Datensätzen, die bisher bei einem Test verwendet werden konnten.

Die Daten zum MINEX-Test wurden als Lifescans von 250.000 Personen im Rahmen des US-Visit-Programms erhoben.

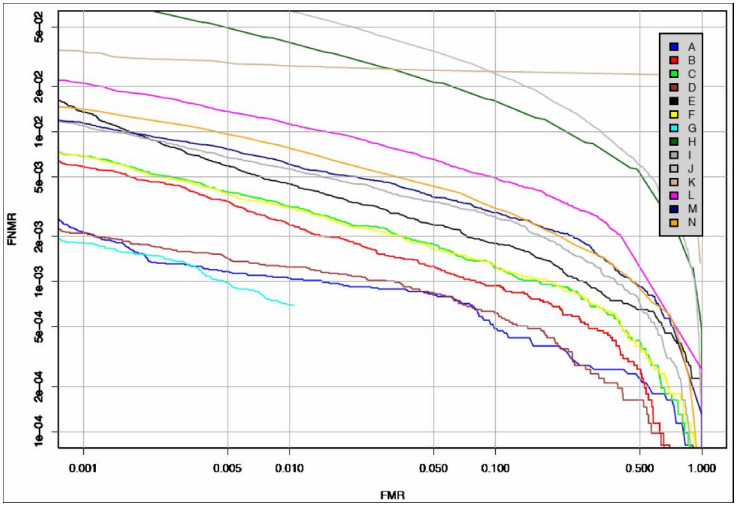


Abbildung 6: DET-Kurven der 14 beteiligten Hersteller im MINEX-Test

Die Abbildung 6 zeigt die Detection-Error-Tradeoff-Characteristic (DET), wobei die False-Non-Match-Rate (FNMR)[3] in der vertikalen Achse bei einer ausgewählten False-Match-Rate (FMR)[4] abgelesen werden kann. Die Kurven beschreiben die Eigenschaften eines Systems bei verschiedenen Konfigurationen (Schwellwerten). Je näher eine DET-Kurve links unten am Ursprung des Koordinatensystem liegt, desto positiver ist die Erkennungsleistung des durch die Kurve beschriebenen Systems. Die hellblaue Kurve zeigt das beste System, das im MINEX-Test zum Einsatz

3 Die False-Non-Match-Rate (FNMR) gibt die Anzahl der Fälle an, in denen das biometrische System fälschlicherweise keine Übereinstimmung von Vergleichsdaten und der biometrischen Referenz festgestellt hat. Nach ISO/IEC IS 19795-1 ergibt sich die False-Reject-Rate (FRR) unter Berücksichtigung der FNMR und der Failure-to-Acuire-Rate (FTA), d.h. derjenigen Fälle, in denen das biometrische System die biometrische Charakteristik einer Person in ausreichender Qualität gar nicht erfassen konnte.

4 Die False-Match-Rate (FMR) gibt die Anzahl der Fälle an, in denen das biometrische System fälschlicherweise eine Übereinstimmung von Vergleichsdaten und der biometrischen Referenz festgestellt hat. Nach ISO/IEC IS 19795-1 ergibt sich die False-Accept-Rate (FAR) unter Berücksichtigung der FMR und der Failure-to-Acuire-Rate (FTA).

kam. Für dieses System kann bei einer FMR von 0,01 ein üblicher[5] Arbeitspunkt auf der DET-Kurve betrachtet werden. Für diesen Arbeitspunkt ergibt sich aus dem Test für die bildbasierten Datensätze eine FNMR von 0,0047, während die templatebasierten Datensätze mit einer FNMR von 0,0129 leicht schlechter abschneiden. Werden jedoch statt einer Referenz zwei Referenzen einer Person verwendet, d.h. es wurde sowohl der Abdruck des rechten und des linken Zeigefingers aufgenommen, so kann die Erkennungsleistung bei gleicher FMR sogar auf eine FNMR von 0,0002 (bildbasierte Datensätze) bzw. auf eine FNMR von 0,0007 (templatebasierte Datensätze) verbessert werden. Durch die Verwendung einer zweiten Fingerinstanz (Multi-Instance: Zweifinger-Minutien-System) wird der Merkmalsraum also derart vergrößert, dass der Verlust an Erkennungsleistung beim Übergang von Bildern zu Templates (Mintuien-Information) mehr als kompensiert werden kann. Im gleichen Zuge lassen sich durch ein Zweifinger-Minutien-System die Anforderungen an die Kapazität des Datenträgers stark reduzieren.

Wie oben schon geschildert, ist es zur Erreichung der vollen Interoperabilität biometrischer Systeme nicht nur erforderlich, dass die von Fremdherstellern geschriebenen Datensätze gelesen und verstanden werden können, sondern ferner, dass sich auf diesen Daten auch ein gute Erkennungsleistung erzielen lässt. Diese Leistung soll nicht signifikant schlechter sein, als die Erkennungsleistung auf Datensätzen, die mit eigenen Implementierungen (für die Bildverarbeitung, Skelettierung und Minutienextraktion) generiert wurden.

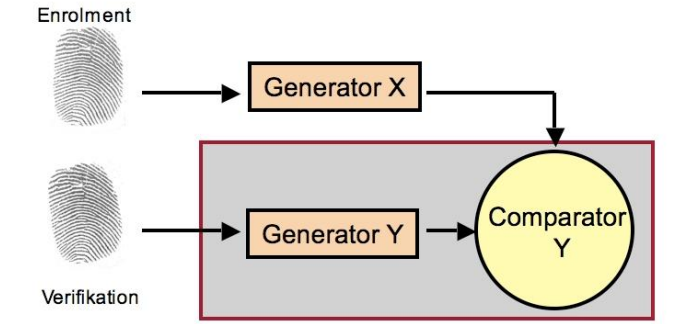


Abbildung 7: Vergleich der Templates von unterschiedlichen Herstellern

[5] Eine FMR von 0,01 wird oft betrachtet, da dieser Werte in der Praxis von Systemen erreicht werden kann und das damit assoziierte Sicherheitsniveau in vielen Fällen akzeptiert wird.

Das in Abbildung 7 gezeigte Szenario entspricht der realen Welt der Seefahrerkarte und könnte auch dem Prozess bei der Nutzung einer *European Citizen Card* (ECC) entsprechen, wenn diese nach dem jetzt vorliegenden Standard implementiert wird. Beim Enrolment wird an der Meldestelle ein Fingerbild aufgenommen. Aus diesem Bild wird mit der Software eines Herstellers X die Minutien-Information extrahiert und das Template als Referenz in die Ausweiskarte gespeichert. Bei einer späteren Nutzung der Karte wird bei einem physikalischen oder logischen Zugangskontrolldienst die biometrische Charakteristik der Person erneut erfasst. Es wird wiederum ein Template generiert – in diesem Fall jedoch mit einem Template-Generator des Herstellers Y – und dann ein Vergleich zwischen beiden Templates auf Ähnlichkeit durchgeführt. In Abbildung 7 wird der Vergleich mit einer Software des Herstellers Y durchgeführt. Es könnte jedoch auch die Software eines dritten Herstellers Z zum Einsatz kommen.

NF = 2	A	B	C	D	E	F	G	H	I	J	K	L	M	
A	0.0011	0.0092	0.0080	0.0021	0.0130	0.007	0.0049	0.0248	0.0049	0.0755	0.0292	0.0161	0.0213	0.0
B	0.0027	0.0024	0.0072	0.0018	0.0073	0.007	0.0017	0.0456	0.0049	0.0589	0.0588	0.0105	0.0083	0.0
C	0.0052	0.0057	0.0032	0.0025	0.0104	0.003	0.0039	0.0851	0.0081	0.1571	0.1048	0.0177	0.0099	0.0
D	0.0021	0.0046	0.0045	0.0013	0.0097	0.004	0.0035	0.0325	0.0062	0.0877	0.0442	0.0154	0.0126	0.0
E	0.0025	0.0061	0.0056	0.0028	0.0045	0.005	0.0035	0.0280	0.0102	0.0900	0.0362	0.0163	0.0147	0.0
F	0.0054	0.0060	0.0032	0.0025	0.0103	0.003	0.0038	0.0855	0.0081	0.1597	0.1058	0.0177	0.0097	0.0
G	0.0040	0.0032	0.0085	0.0022	0.0061	0.008	0.0007	0.0308	0.0068	0.0715	0.0693	0.0116	0.0074	0.0
H	0.0084	0.0421	0.0393	0.0143	0.0767	0.039	0.0384	0.0422	0.0210	0.9999	0.0724	0.0413	0.0753	0.0
I	0.0073	0.0184	0.0252	0.0100	0.0333	0.024	0.0083	0.1137	0.0056	0.1206	0.1170	0.0207	0.0313	0.0
J	0.0077	0.0119	0.0259	0.0082	0.0276	0.025	0.0070	0.1572	0.0103	0.0640	0.5736	0.0198	0.0296	0.0
K	0.0018	0.0130	0.0108	0.0051	0.0134	0.010	0.0049	0.0280	0.0068	0.0929	0.0275	0.0270	0.0313	0.0
L	0.0115	0.0109	0.0218	0.0097	0.0258	0.021	0.0066	0.0795	0.0105	0.0861	0.1123	0.0113	0.0267	0.0
M	0.0099	0.0096	0.0106	0.0049	0.0116	0.010	0.0039	0.1007	0.0134	0.1573	0.1929	0.0247	0.0061	0.0
N	0.0063	0.0077	0.0086	0.0042	0.0094	0.008	0.0056	0.0368	0.0104	0.0862	0.0353	0.0169	0.0157	0.0
Mean	0.0054	0.0108	0.0130	0.0051	0.0185	0.012	0.0069	0.0636	0.0091	0.1648	0.1128	0.0191	0.0214	0.0
Rank	2	5	7	1	8	6	3	12	4	14	13	9	10	
Med.	0.0053	0.0084	0.0086	0.0035	0.0110	0.008	0.0044	0.0439	0.0081	0.0889	0.0709	0.0173	0.0152	0.0
Rank	3	5	6	1	8	7	2	12	4	14	13	11	9	

Abbildung 8: Interoperabilität und Erkennungsleistung

Es liegt in der Natur der Implementierungskenntnisse, dass in der Regel der Vergleich auf eigenen Templates etwas besser liegt als auf anderen. Betrachtet man den Gewinner des ersten Tests (aus Abbildung 6) nun hinsichtlich seiner Erkennungsleistung bei Interoperabilität, so kann man in der rot umrandeten Spalte in Abbildung 8 die FNMR auf Templates von Fremdherstellern ablesen. Für das Zweifinger-Minutien-System ergibt sich als Mittelwert eine FNMR von 0,0069 und ein Medianwert von 0,0044. Ein sehr brauchbares Ergebnis.

Die Stolpersteine

Erkennungsleistungen, wie sie vom MINEX-Test berichtet werden, können nur dann erzielt werden, wenn die Qualität der aufgezeichneten Bilder entsprechend gut ist. Für die Qualität der Fingerbilder sind in erster Linie die Qualität des Sensors und etwaige dermatologische Probleme der Person entscheidend. Umwelteinflüsse wie beispielsweise schwankende Luftfeuchtigkeit können mit geringem Aufwand beim Prozessaufbau kontrolliert werden.

Bei der zweidimensionalen Gesichtserkennung ist es unerlässlich, dass das Bildmaterial in sehr guter Bildqualität vorliegt. Während die Qualität des Sensors in diesem Fall mit geringem Aufwand sichergestellt werden kann, spielen ein Vielzahl von möglicherweise stark beeinträchtigenden Umwelteinflüssen und vor allem die Aufnahmesituation eine große Rolle. Wichtige Kriterien für ein gutes Gesichtsbild sind eine ausreichende Ausfüllung des Gesichtes im 2D-Bild (ca. 70%), eine Frontalaufnahme, ein guter Kontrast, Bildschärfe, Ausleuchtung, ein neutraler Gesichtsausdruck und keine Verdeckung des Gesichtes bzw. der Landmarken durch Haare, Brillen oder Kopfbedeckungen. Werden diese Bildqualitätskriterien nicht erfüllt, muss mit einer sehr schwachen Erkennungsleistung des biometrischen Systems gerechnet werden. Die Einhaltung all dieser Kriterien sowohl bei der Aufnahme des Referenzbildes (z.B. ePass-Ausstellung) als auch beim späteren Vergleich (bei der Grenz-Kontrolle) ist schwer herzustellen: Nur selten werden die Gesichtsausrichtung (Pose) der Gesichtsausdruck (Mimik) und die Beleuchtungssituation identisch sein. Dies könnte zu einem Stolperstein werden, der die Nutzung der biometrischen Information in den ersten ausgegebenen ePass-Exemplaren verhindert.

Die Anforderungen in den biometrischen Anwendungs-Szenarien enthalten nicht selten auch Kriterien an die Sicherheit eines Systems. Eine Untersuchung der einzelnen Komponenten wird dann erforderlich. Oft werden in der Diskussion eines Szenarios/Systems die Eigenschaften des Sensors problematisiert, die eigentlich nicht überraschen sollten: Ein biometrisches System verarbeitet biometrische Samples. Unter einem biometrischen Sample versteht man nach der Definition[6] eine analoge oder digitale Repräsentation einer biometrischen Charakteristik [ISO2006a]. Beispiele für eine Repräsentation einer biometrischen Charakteristik sind Fotos eines Gesichtes, der Iris, des Fingerbildes und vieles Andere mehr. Diese Repräsentation wird aufgezeichnet durch einen Sensor (*biometric device*). Die Aufzeichnung

[6] Biometric sample: analog or digital representation of biometric characteristics prior to feature extraction process and obtained from a biometric device.

kann ggf. viele Zwischenschritte enthalten. Denken wir an den Fingerabdruck, der in der Kriminalistik seit über 100 Jahren verwendet wird. Von Beginn an wurde als Träger ein Papierbogen verwendet, auf dem der Finger abgerollt wurde. Erst viel später wurde im Verarbeitungsprozess dieser Papierbogen in einen Scanner eingelegt und digitalisiert. Der Bogen und auch der an einem Tatort hinterlassene Fingerabdruck sind jedoch bereits analoge Repräsentationen der biometrischen Charakteristik. Auch bei anderen biometrischen Systemen wie beispielsweise der Stimmerkennung, kann es durchaus so sein, dass bei der Verarbeitung analoge Datenträger zwischengeschaltet werden. Der Vergleichsalgorithmus in einem Gesichtserkennungssystem, der letztlich die Authentisierungsprobe mit dem Referenzbild vergleicht, hat keine Kenntnis darüber wie das Authentisierungsbild (biometric sample) entstanden ist. Woher soll der Algorithmus wissen, ob eine lebende Person vor der Kamera steht, ein gedrucktes Foto vor die Kamera gehalten wird oder gar ein Mobiltelefon, auf dessen Display das Bild einer Person dargestellt wird? Es ist keine große Überraschung, wenn ich den Algorithmus in einem Zugangskontrollsystem mit einem Foto von meinem Gesicht davon überzeugen kann, dass dieses Foto und die in der Datenbank hinterlegte biometrische Referenz von ein und derselben Person stammen. Das ist die Aufgabe des Algorithmus. Viele Systeme können keine Lebenderkennung durchführen oder beschränken sich auf die Auswertung einer Bildfolge[7].

Ähnliches gilt für die Fingerbilderkennung, wobei in diesem Fall erschwerend hinzukommt, dass die biometrische Charakteristik selbst flüchtig ist. Fingerabdrücke in guter Qualität können auf glatten Oberflächen wie Gläsern oder CD-Hüllen detektiert und ohne großen Aufwand aufgezeichnet werden. Der Fingerabdruck auf dem Glas ist bereits eine analoge Repräsentation der biometrischen Charakteristik. Nach der Aufzeichnung ist es nur noch ein kleiner Schritt, einen Silikonfinger zu erstellen und damit die meisten Livescanner zu täuschen.
Für den neuen ePass ist nach heutigem Stand der Technik anzunehmen, dass unter Verwendung der beiden biometrischen Charakteristiken 2D-Gesichtsbild und Fingerbild keine Systeme ausgeliefert werden können, die wirklich überwindungssicher sind d.h. deren Sensoren nicht von einem Replikat der biometrischen Charakteristik wie einem Silikonfinger getäuscht werden können.

Die Entwicklung von überwindungssicheren Sensoren ist jedoch notwendig, wenn wir heutige Prozesse optimieren wollen oder müssen. Es bleibt wünschenswert, dass

7 Damit lässt sich das gedruckte Einzelbild detektieren, nicht aber ein abgespielter Videofilm.

die Sensoren eines biometrischen Systems überwindungssicher werden und dann auch eine unüberwachte physikalische Zugangskontrolle erlauben.
Die Prozesse an der Grenze werden zunächst noch anders gestaltet sein. Ein Grenzbeamter wird fünf bis zehn Kontrollspuren im Auge behalten. Wie heute schon im SmartGate-Projekt wird er versuchen zu verhindern, dass Replikate präsentiert werden. Aber natürlich wäre es auch für dieses Szenario sinnvoll, überwindungssichere Systeme einzusetzen. Die *International Civil Aviation Organization* (ICAO), die Passstandards kontinuierlich weiter entwickelt [ICAO2006], denkt bereits in diese Richtung. Sie hat im Oktober 2004 in ihrem *request for* information die Hersteller aufgefordert, die Technologieentwicklungen mitzuteilen, die zukünftig eine nicht überwachte Grenzkontrolle ermöglichen: "*... new technologies is now sought ...technologies and processes that are suitable for automated self-identification at international borders that will enable unattended border crossing*" [ICAO2004].

Kleine Schritte in diese Richtung sind auch heute schon möglich, wenn verschiedene Informationskanäle verknüpft werden. Beispielsweise gibt es bereits heute Hersteller, deren Systeme Fingervenen analysieren[8]. Warum also nicht die Information aus dem Fingerbild, das die Papillarleisten der Fingerkuppe abbildet, mit den Informationen aus dem Bild der Fingervenen verknüpfen und somit Fingererkennung bei guter Erkennungsleistung überwindungssicher gestalten? Ein Angriffsversuch mit einem Silikonfinger könnte dann leicht erkannt werden, da die Merkmale aus dem Venenbild nicht vorhanden sind (bei einem Silikon-Voll-Finger) bzw. nicht mit den Fingervenen-Merkmalen in der Referenz übereinstimmen (bei einem über die Fingerkuppe gestreiften dünnen Silikon-Film)
Auch bei der Gesichtserkennung ist die Multi-Channel-Analyse mit mehreren Sensoren ein Erfolgsversprechender Ansatz, der gegenwärtig in den akademischen und industriellen Forschungslabors verfolgt wird. Der Ansatz fußt auf einer zusätzlichen dreidimensionalen Vermessung des Gesichtes. Beispielsweise durch ein aktives Messverfahren mittels Projektion farbiger Streifen oder Muster auf das Gesicht kann die Tiefeninformation als dritte Dimension erfasst werden (siehe Abbildung 9).

[8] Die Unternehmen Sony und Hitachi bieten Venenbilderkennungssysteme bereits an.

Abbildung 9: Aufnahmesituation mit 3D-Gesichtsscanner

Diese Information kann über die ganze Gesichtsfläche ermittelt werden und liefert eine vollständiges Profil (Gesichts-Geometrie) der Person. Zusätzlich wird an jedem Oberflächenpunkt eine Farbinformation bestimmt.

Abbildung 10: 3D-Gesichtsmodell

Das resultierende dreidimensionale Modell erlaubt eine gegenüber der einfachen zweidimensionalen Frontalaufnahme bessere Erkennung bei Kopfrotationen oder ungünstigen Kamerawinkeln. Bevor ein Authentisierungsmodell mit einem Referenzmodell verglichen werden kann, müssen jedoch auch in diesem Fall Landmarken des Gesichtes bestimmt werden. Darunter versteht man die charakteristischen Punkte des Gesichtes, wie "Eckpunkte der Augen", "Augenmitte", "Mundwinkel", "Nasenansatz" usw.. Die Gesichtserkennungsverfahren nutzen diese Landmarken zur groben Orientierung des Modells, so dass die Ausrichtung der Modelle identisch hergestellt werden kann. Erst dann können Ähnlichkeitsmaße bestimmt werden, die nun auf Geometrieinformationen wie lokalen Krümmungsmaßen oder Abstandsmaßen zwischen den geometrischen Oberflächen beruhen. Die Farbinformationen und Texturmerkmale an den Landmarken können natürlich weiter als Merkmalsinformation genutzt werden.

Ein wichtiger Vorteil der dreidimensionalen Erfassung ist die Invarianz gegenüber Skalierungen. Während bei der zweidimensionalen Aufnahme der unbekannte Abstand der Person zur Kamera zu unterschiedlich großen Bildern führt, sind die dreidimensional erfassten Modelle immer metrisch korrekt. Es wird deutlich, dass bestehende Grundmaße des Kopfes - wie zum Beispiel der Augenabstand - erhalten bleiben und nicht durch Umrechnung auf eine einheitliche Bildformatgröße (und einheitlichen Augenabstand) verloren gehen. Diese Grundmaße lassen sich im Sinne von Bertillon[9] zur Vorklassifikation bei einem Identifikationszenario nutzen: Auch wenn die Grundmaße selbst nicht ausreichende Trennschärfe liefern, so lässt sich bei einer 1:n Suche in einer großen Datenbank der Suchraum deutlich verkleinern, da nur noch innerhalb eines bestimmten Abschnittes der Datenbank gesucht werden muss (*Binning-Ansatz*). Ein einzelner Abschnitt (engl. *bin*) enthält dabei genau diejenigen Referenzen, die identische bzw. sehr ähnliche Grundmaße haben.

Bei der 3D-Gesichterkennung liegt gegenüber dem herkömmlichen zweidimensionalen Verfahren deutlich mehr an Information vor, was eine höhere Trennschärfe für das Klassifikationsverfahren und somit auch bessere Erkennungsergebnisse bedeuten sollte. Die Erkennungsverfahren sind jedoch derzeit noch Gegenstand der Forschung [3DFace]. Unabhängig vom Entwicklungsstand der Verfahren, kann man der 3D-Gesichtserkennung eine verbesserte Robustheit hinsichtlich der Überwindungsangriffe attestieren, da ein Replikat deutlich schwieriger zu erstellen ist. Schon die Beschaffung der 3D-Geometrie ist ohne Kooperation der zu replizierenden "Zielperson" mit erheblichem Aufwand verbunden. Die Produktion eines 3D-PrintOuts ist

9 Alfons Bertillon (1853-1914) – Mitbegründer der Anthropometrie.

zwar technisch beispielsweise mit einem Stereo-Lithographieverfahren möglich - ein derart hergestellter künstlicher Kopf könnte jedoch mit einfachen Lebenderkennungs-Mechanismen auch automatisch detektiert werden, was die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert.

Werfen wir zum Abschluss des Themas Überwindungssicherheit noch einen Blick in die fernere Zukunft: Ist mit der 3D-Gesichtserkennung das Problem der Überwindungssicherheit gelöst, können Angriffe auf biometrische Systeme ausgeschlossen werden? Hat die Eingangsthese damit wieder bestand, in der formuliert wurde: "*Wissen oder Besitz kann man leicht weitergeben, eine biometrische Charakteristik jedoch aber nicht*"? Gilt die These noch, wenn sich die Medizin so weiter entwickelt? Im Herbst 2005 wurde in Frankreich erstmals erfolgreich die Transplantation eines Gesichtes durchgeführt. Nur ein erster Schritt auf einem Gebiet, das noch lange nicht abschließend erforscht ist. Unterstellt man der Medizin auf diesem Gebiet das gleiche Fortschrittspotential, wie es auf dem Gebiet der Herztransplantationen und Schönheitsoperationen in den letzten Jahren gezeigt wurde, entsteht mit etwas Phantasie ein Szenario, in dem die heute verwendeten biometrischen Charakteristiken nicht mehr untrennbar mit einer Person ("Identität?") verbunden sind. Eine Mehrdeutigkeit entsteht dabei auch im Falle einer DNA-basierten Identifikation. Eine Person mit einem transplantierten Gesicht trägt zwei DNA-Muster, wie übrigens auch viele operierten Personen heute schon - beispielsweise Personen die als Leukämiepatienten Stammzellen empfangen haben.

Die in den beiden Beispielen oben angesprochene multimodale Analyse einer Person ist nicht wirklich ein neuer Trend in der Biometrie. Schon im Lehrbuch von R. Heindl wurde 1927 vorgeschlagen, besonders kritische Fälle wie die Identifikation von Zwillingen durch einen multimodalen Ansatz zu lösen, in dem das Gesichtsbild und zwei Fingerbilder ausgewertet werden [HEI1927].

Der Begriff der multimodalen Analyse wird in verschiedenen Formen benutzt. Genauer betrachtet ist der Begriff Multi-Biometrics ein sinnvoller Oberbegriff und Multi-Modal nur eine Ausprägungsform. Der Technische Report der ISO zu Multi-Biometrics [ISO2006b] stellt die Ausprägungsformen gegenüber und erläutert diese:

- Multi-Presentation: Es werden mehrere Aufnahmen einer Person gemacht (beispielsweise um verschiedene Posen abzudecken)
- Multi-Instance: Aufnahmen von zwei Exemplaren der selben biometrischen Charakteristik (Finger links, Finger rechts, Iris links, Iris rechts.
- Multi-Modal (Multi-Channel): Aufnahme eines Körperteil oder verschiedener Körperteile, wobei unterschiedliche biometrische Charakteristiken erfasst werden (Gesichtsbild und Gesichtsgeometrie).

- Multi-Sensorial: Aufnahme einer biometrischen Charakteristik mit unterschiedlichen Sensoren (optischer und kapazitiver Fingerbildscanner)
- Mutli-Algorithmic: Ein biometrisches Sample wird von verschieden Verfahren analysiert.

Je nach Szenario und vor allem je nachdem, welche obere Grenze für die Transaktionszeit gesetzt wird, lassen sich auch mehrere der genannten Ansätze zusammenschalten (z.B. mehrere Präsentationen **und** mehrere Sensoren). Je nach Szenario werden durch Multi-Biometrics verschiedene Ziele gleichzeitig verfolgt bzw. auch erreicht:
- Performanzsteigerung (wie im MINEX-Test für Multi-Finger gezeigt),
- Überwindungssicherheit (Pappilarlinien und Fingervenen - wie oben diskutiert),
- Kompensation des Posenproblems (Um eine schlechte Erkennungsleistung durch mögliche Rotationen des Kopfes zu verhindern, werden mehrere Aufnahmen mit unterschiedlichen Posen als Referenzen gespeichert)
- Diskriminierungsarmut (Personen, deren Fingerbild – temporär – nicht auswertbar ist, können über Gesichtsbild-Vergleich authentisiert werden)

Immer schnellere und effizientere Hard- und Software wird bei gleichen Transaktionszeiten in Zukunft verstärkt die Umsetzung der Multi-Biometrics Ansätze in der Praxis ermöglichen.

Technischer Datenschutz und Zusatzinformation

Dieser Beitrag schließt mit einer Betrachtung der heutigen Möglichkeiten zum technischen Datenschutz und den Zusatzinformationen, die in biometrischen Referenzen möglicherweise verborgen sind.

Zum ersten Punkt ist eine Bewertung zu korrigieren, die in der Diskussion der letzten Jahre vielfach geäußert wurde: "*Biometrische Verfahren sind schlecht für den Nutzer, weil die Referenzdaten im Zweifelsfalls nicht zurückgerufen werden können. Der Mensch hat nun mal nur ein Gesicht, er hat nur zehn Finger, er hat zwei Iriden*". Der zweite Teil der Aussage ist unstrittig richtig, wir haben für die aufgezählten biometrischen Charakteristika die genannte Anzahl der Instanzen. Der erste Teil der Aussage zur Datensicherheit der Referenzdaten in einem Token oder in einem Datenbank-Record ist jedoch unter Berücksichtigung der aktuellen Forschungsarbeiten auf diesem Gebiet zu überprüfen.

Unverändert richtig ist die Annahme, dass biometrische Samples im Sinne unseres Datenschutzverständnisses personenbezogene Daten sind, die einem besonderen Schutz zu unterwerfen sind. Bei der Analyse der Datensicherheit sind zwei Konzepte zur Speicherung der Referenzdaten zu betrachten: Im ersten Konzept wird die biometrische Authentisierung mit einem Token verknüpft, so dass die biometrische Referenz beispielsweise auf einer SmartCard gespeichert werden kann. In diesem Fall verbleiben die sensitiven Referenzdaten im Besitz der Person und somit unter seiner Kontrolle. Sofern die SmartCard die entsprechende Kapazität hat, kann darüber hinaus auch bei der Authentisierung der Vergleich in dieser Karte durchgeführt werden. Bei diesem sogenannten *Comparison on Card*[10] liefert die Karte ein positives oder negatives Ergebnis an die Anwendung zurück, ohne dass die Anwendung Zugriff auf die Referenzdaten erhält. Dies ist vor allem dann ein guter Schutz für die sensitiven biometrischen Samples, wenn die Karte über eine direkte Schnittstelle zum bildgebenden Sensor verfügt (z.B. kapazitiver Fingerbild-Sensor) und auch auf die Authentisierungsdaten kein Zugriff der Anwendung erfolgen kann. Die Karte bleibt für die nutzende Person ein vertrauenswürdiger Token. Kartenbasierte biometrische Systeme, wie die *European Citizen Card* oder der digitale Personalausweis sollten dies umsetzen. Sie sollten dieses Konzept realisieren, damit das Referenzmuster die Karte nicht mehr verlässt. Der oben genannte Minutien-Standard ist eine Möglichkeit, bei guter Erkennungsleistung die Datensätze kompakt zu kodieren. Die Abbildung 11 zeigt zum Minutien-Standard noch einmal eine Alternative.

10 In der Internationalen Standardisierung wurde der Begriff Comparison bewusst ersetzend für den seither genutzten Begriff Matching geprägt, da Comparison das Ergebnis des Vergleichs offen lässt – hingegen Matching suggeriert, dass der Vergleich auf der Karte tatsächlich positiv ausfallen wird.

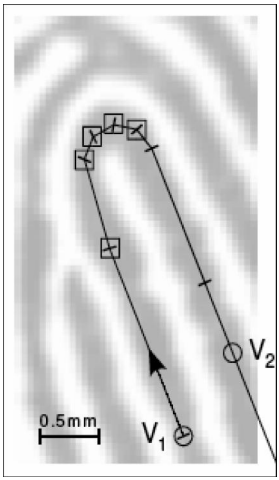


Abbildung 11: Polygone zur Kodierung von Papillarlinien

Sollte es für einen Vergleichsalgorithmus erforderlich sein, dass das komplette Fingerbild ausgewertet werden kann, so steht mit dem neuen Standard ISO/IEC IS 19794-8 ein Standard zur Verfügung, der zusätzlich zu den Finger-Minutien auch das ganze Skelett der Papillarlinien als Polygonzüge abspeichert [ISO2006c]. Wie in Abbildung 11 dargestellt, passen sich die Längen der einzelnen Polygonkanten der Krümmung der Papillarlinien an. Dies bedeutet hinsichtlich des Speicherplatzes nur einen geringen Mehrbedarf gegenüber ISO/IEC IS 19794-2, der noch deutlich unter dem Speicherbedarf für ein Fingerbild liegt (ISO/IEC IS 19794-4).

Im zweiten Konzept werden die Referenzdaten in einer zentralen oder dezentralen Datenbank abgespeichert, wie es im Beispiel der Zugangskontrolle zum österreichischen Parlament der Fall ist. Mit der Speicherung von Samples in einer Datenbank werden einige potentielle Probleme assoziiert: Diese reichen vom Identitätsdiebstahl (beim Zugriff auf Bilddaten) und der damit einhergehende Wunsch, gespeicherte Referenzdaten "zurückrufen" zu können, über die Gefahr des Cross-Matching (auch bei der informationsreduzierenden Verwendung von Templates als Referenzdaten könnten Datenbank-Administratoren durch Abgleich der Datensätze Querbezüge herstellen) bis hin zur Thematik der Zusatzinformation (die potentiell als medizinische Überschussinformation aus den Bilddaten auslesbar ist). Zur Lösung dieser Probleme gibt es einen sehr viel versprechenden Forschungstrend, der als *Template Protection* bezeichnet wird [VEEN2006] und der das Speichern von Bild- oder Templatedaten in einer Datenbank entbehrlich macht. Die Vorgehensweise ist ange-

lehnt an die Absicherung von Passwortdaten in einem Unix-System. Bei der Unix-Authentisierung ist es nicht so, dass das von einem Nutzer verwendete Passwort im Klartext im System (oder in einer Datenbank) gespeichert werden. Vielmehr wird bei der Einrichtung eines Nutzeraccounts (*Enrolment*) unter Verwendung einer Einwegfunktion (*Hashfunktion*) ein Hashwert berechnet. Die Funktion hat die Eigenschaft, dass Sie nicht invertierbar ist, d.h. aus dem Hashwert lässt sich das Passwort nicht zurückrechnen. Zudem werden nur solche Einwegfunktionen eingesetzt, die kollisionsfrei sind, d.h. es gibt nicht zwei Eingabestrings (Passworte) für die sich derselbe Hashwert berechnet. Die Hashwerte für alle Nutzer werden in einer öffentlich zugänglichen Datei (/etc/paswd) gespeichert. Wenn der Nutzer sich erneut authentisieren möchte, wird wiederum von dem Input ein Hashwert gebildet, welcher dann mit dem in der Tabelle hinterlegten Hashwert verglichen wird.

Analog kann das Verfahren zum Schutz von Templates ablaufen. Biometrische Samples und damit auch Merkmalvektoren sind allerdings - im Unterschied zu den Passwort-Datensätzen - mit einem Rauschen belegt. Dies ist durch die Variation der Umwelteinflüsse (z.b. Lichtverhältnisse) aber auch durch die Variation der biometrischen Charakteristik selbst (z.B. Alterung) bedingt. Aus diesem Grunde müssen die im Template gespeicherten Merkmale noch einmal gefiltert werden, um eindeutige Datensätze reproduzieren zu können. Anschaulich kann man diese Filterung als *Quantisierung* des Merkmalvektors verstehen, bei dem für ein bestimmtes Merkmal verschiedene Wertebereiche jeweils auf einen Mittelwert abgebildet werden. Für die berechneten quantisierten Merkmale wird eine Qualitätsprüfung vorgenommen, um die Robustheit des Verfahrens sicherzustellen. Das bedeutet, dass nur diejenigen stabilen Merkmale weiterverarbeitet werden, die auch wiederholt mit dem gleichen Mittelwert berechnet wurden. Um die Erneuerbarkeit des Vektors herzustellen, werden anschließend aus dem Merkmalvektor einzelne Komponenten selektiert, wobei die Selektionsfunktion durch ein Geheimnis gesteuert wird. Über den verbleibenden reduzierten Vektor wird der Hashwert berechnet und in der Datenbank abgelegt.

Bei einer biometrischen Verifikation wird das präsentierte Sample nur in einem gewissen Maße ähnlich sein zu dem Sample, das beim Enrolment verwendet wurde. Durch den geschilderten Ansatz lassen sich jedoch die gleichen stabilen Komponenten im Merkmalvektor berechnen und mit dem gleichen Geheimnis kann ermittelt werden, welche Komponenten für die Hashberechnung erforderlich sind. Der sich durch diesen Ansatz ergebende Gewinn für die Datensicherheit der personenbezogenen Daten ist enorm.

Die Thematik der Zusatzinformation wurde schon vor mehr als vier Jahren von den Datenschutzexperten auf der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung formuliert: "*Die gespeicherten und verarbeiteten Daten dürfen keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben*" [KD2002]. Oft wird in diesem Kontext auf die Informationen im Irismuster verwiesen. Die Schulmedizin verwirft den Ansatz der Iridologie und ist der Ansicht, dass das Irismuster zur Diagnose nicht zu verwenden ist [ERN2000]. Allerdings ist ein Zusammenhang von klassifizierbaren Informationen (z.B. Größe der Pupille, Pupillenreflex, Farbe der Sklera etc.) mit einer Gruppe von Ursachen (neurologische Störungen, Ermüdung, Alkohol etc.) anzunehmen. Bestimmte auffällige Muster, wie beispielsweise eine verkleinert Pupille (*Miosis*) können darauf schließen lassen, dass Medikamente eingenommen wurden oder starker Alkoholkonsum bzw. Ermüdung vorliegen. Ein vor etwa vier Jahren am Fraunhofer IGD gestarteter Versuch mit einer Gruppe von Testpersonen, die testweise zum intensiven Alkoholkonsum bereit waren, zeigte jedoch gegenüber dem nüchternen Zustand eine derart geringe augenscheinliche Veränderung, dass eine rechnergestützte Auswertung in der Praxis als nicht aussichtsreich erscheint.

Seltener wird über den Fingerabdruck diskutiert. Dabei sind nach Auskunft von Experten bis zu 11% der Bundesbürger von dermatologischen Problemen an den Fingerkuppen betroffen, die eine Erfassung und Auswertung des Fingerbildes erschweren [HER2004]. Allerdings kann man das Fingerbild nach Ausprägung in der Schwangerschaft als statisch betrachten, wenn man von verletzungsbedingten temporären Veränderungen absieht. Das ausgeprägte Grundmuster selbst kann jedoch, wie eine Untersuchung von Schuster ergeben hat, als Indikator für eine Krankheit betrachtet werden [SCHU1996]. Nach seinen Untersuchungen zeigte sich bei einer siebenjährigen Analyse von Patienten, die an der Chronic Intestinal Pseudoobstruction (CIP)[11] leiden, dass diese Patienten mit einer Wahrscheinlichkeit von 54% ein ungewöhnliches Fingerbild[12] aufweisen, das in der Normalpopulation nur mit 7% existiert. Das Fingerbild war also in gewisser Weise ein Indikator für diese Krankheit. Dennoch ergibt sich im Gegensatz zur Iris eine andere Bewertung: Das Grundmuster im Fingerbild ist ein Leben lang stabil und wird sich nicht zeitweise anpassen. Bei allen analytischen Anstrengungen kann ein Fingerbild nicht preisgeben, ob eine Person, Bier, Wein oder sonstige Alkoholika zu sich genommen hat.

---

11 Bei CIP handelt es sich um eine Erkrankung des Magen-Darm-Traktes, bei der die Patienten unter Schmerzen, Erbrechen, Übelkeit, Durchfall oder Verstopfung leiden, so dass oftmals von einem Geschwür o.ä. ausgegangen wird; bei einer Operation wird dann jedoch nichts gefunden (daher die Bezeichnung pseudoobstruction). Die Ursache sind meist degenerierte Muskeln oder Nerven im Magen-Darm-Trakt.

12 Die Publikation spricht von "digital arch" – vermutlich ist das Bogen-Grundmuster damit gemeint.

Am wenigsten wird eigentlich die Analyse der Zusatzinformation in Gesichtsbildern diskutiert, obwohl bekanntermaßen Alkohol, Ermüdung und selbst Gemütszustände das Gesicht verändern. Unterschiedliche Ausdrucksformen des Gesichtes (*Expressions*) beeinflussen die Erkennungsleistung. Zu den Kriterien beim Enrolment zählt daher auch, dass die Personen möglichst mit einem neutralen Gesichtsausdruck zu photographieren sind. Wird die Biometrie hier jedoch mehr verraten, als die konventionelle Zugangskontrolle mit manueller Inspektion? Personen mit besonderen Auffälligkeiten wie "Schweiß auf der Stirn" oder ein "rotes Gesicht" wurden schon bisher einer besonderen Prüfung unterzogen.

Insgesamt ist zu sagen, dass die Problematik der Überschussinformation vielleicht weniger dringend ist, als der diskriminierungsfreie Umgang mit den Nicht-Nutzern, d.h. denjenigen Nutzern, die eine biometrische Charakteristik, wie beispielsweise den Fingerabdruck nicht in ausreichender Qualität präsentieren können. Eine Benachteiligung dieser Personen in einer zukünftigen Biometrie-gestützten Grenzkontrolle sollte ausgeschlossen werden.

Ausblick

Dieser Artikel hat einige Entwicklungen aufgezeigt, die Verbesserungen von technischem Datenschutz und biometrischer Erkennungsleistung bringen werden. Eine gute Erkennungsleistung ist dabei jedoch auch immer von der Qualität der Eingangsbilder abhängig. Dies sicherzustellen liegt in der Verantwortung der Systembetreiber.

Darüber hinaus ist es erforderlich, dass Technolgie-Entwickler, Systembetreiber, Datenschützer und Verbrauchervertreter im Dialog bleiben und sicherstellen, dass zukünftige Technologie datenschutzkonform ausgestaltet wird.

Referenzen

[3DFace]	EU Integrated Project: "3D Face", 2006 http://www.3dface.org
[BKA2006]	Polizeiliche Kriminalstatistik 2005, http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2006/Polizeiliche__Kriminalstatistik__20054__de,templateId=raw,property=publicationFile.pdf/Polizeiliche_Kriminalstatistik_20054_de.pdf
[CEN2005]	CEN/TC 224: "Identification card systems – European Citizen Card – Part2 Logical data structures and card services", TC 224 WI 188:2005
[DIN2006]	ePassport Interoperability Test Event, 29 May - 1 June 2006, Berlin/Germany, http://www.interoptest-berlin.de/
[EU2004]	EU-Council Regulation No 2252/2004 - of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States
[ERN2000]	E. Ernst: „Iridology: not useful and potentially harmful“, Arch Ophthalmol., 118:120-121, 2000
[HEI1927]	R. Heindl: "Daktyloskopie", Verlag Walter de Gruyter, 1927
[HER2004]	M. Herbst: "Unveränderliche biometrische Kennzeichen", Vortrag auf dem CAST-Workshop am 15.07.2004
[ICAObd]	ICAO TAG 14 MRTD/NTWG. "Biometrics Deployment of Machine Readable Travel Documents", Version 2.0, Mai 2004
[ICAO2004]	ICAO TAG 14 MRTD/NTWG. "Request for Information", Oktober 2004
[ICAO2006]	International Civil Aviation Organization: "Supplement to Doc9303-part 1sixth edition", 2006
[ILO2004]	International Labour Organization: "ILO Searfarers' Identity Documents Biometric Testing Campaign Report – Part 1," 2004
[ILO2005]	International Labour Organization: "ILO Searfarers' Identity Documents Biometric Testing Campaign Report – Part 2", 2005
[ILO2006]	International Labour Organization: "ILO Searfarers' Identity Documents Biometric Interoperability Test Report – ISBIT- 3", to be published in 2006
[ISO2005a]	International Standards ISO/IEC IS 19794-2: "Information technology – Biometric data interchange formats – Part 2: Finger minutiae data", 2005

[ISO2005b] International Standards ISO/IEC IS 19794-4: "Information technology – Biometric data interchange formats – Part 4: Finger image data", 2005

[ISO2005c] International Standards ISO/IEC IS 19794-5: "Information technology – Biometric data interchange formats – Part 5: Face image data", 2005

[ISO2005d] International Standards ISO/IEC IS 19794-6: "Information technology – Biometric data interchange formats – Part 6: Iris image data", 2005

[ISO2006a] International Standards ISO/IEC JTC1 SC37 Standing Document 2:" Harmonized Biometric Vocabulary", 2006

[ISO2006b] International Standards ISO/IEC PDTR 24722: " Mutlimodal and Other Multibiometric Fusion", 2006

[ISO2006c] International Standards ISO/IEC IS 19794-8: "Information technology – Biometric data interchange formats – Part 8: Finger pattern skeletal data", 2006

[NIST2006] National Institute of Standards and Technology: "MINEX - Performance and Interoperability of the INCITS 378 Fingerprint Template", http://fingerprint.nist.gov/minex04/minex_report.pdf

[NTA2002] NTA Monitor Password Survey, 2002

[SigV2004] Verordnung zur elektronischen Signatur, 2001, http://www.gesetze-im-internet.de/sigv_2001/

[SmG2004] J. Wayman: "Face Recognition at Sydney Airport", report on Second BSI-Symposium on biometrics 2004, 2004

[VEEN2006] M. Van der Veen et al: "Face Biometrics with Renewable Templates", SPIE Conference, 2006

Peter Schaar

Sehr geehrter Herr Prof. Busch,

ich denke, dass wir alle dazu gelernt haben. Für mich kann ich das jedenfalls sagen. Außerdem hat der Vortrag viele Ansatzpunkte für die Diskussion nachher gebracht. Vielen Dank auch dafür, Herr Prof. Busch. Jetzt haben Sie erstmal das Wort meine Damen und Herren.

Constanze Kurz, Humboldt- Universität zu Berlin

Meine Frage richtet sich auf den Hinweis, dass die Biometrie zur Beschleunigung beitragen würde, und Sie brachten als Beispiel dafür den biometrischen Ausweis, der jüngst eingeführt wurde, den ePass. Nun weist aber insbesondere die Gewerkschaft der Polizei immer darauf hin, dass diese Biometrie selbstverständlich nur zusätzlich eingeführt wird, also weiterhin nach den Schengenstandards kontrolliert werden wird. Von einer Beschleunigung kann also an der Grenze keine Rede sein. Und wenn man dazu nimmt, dass die Ergebnisse der Studien des Bundesinnenministeriums ja abweichend von der MINEX-Studie für die deutschen Hersteller wesentlich schlechtere Erkennungsleistungen ausgeben, dann ist natürlich von einer deutlichen Entschleunigung zu reden, also wir werden mit längeren Wartezeiten zu rechnen haben.

Christoph Busch

Also es ist zunächst richtig, dass die Grenzkontrolle in absehbarer Zeit überwacht durchgeführt wird. Die Aussage der Gewerkschaft der Polizei finde ich richtig, notwendig und auch gar nicht anders durchführbar. Solange die Sensoren nicht überwindungssicher sind, können wir uns das nicht leisten, sicherheitstechnisch nicht leisten eine unüberwachte Kontrolle zu haben. Die Situation der Zunahme des Luftverkehrs des Verkehrs insgesamt steht aber außer Frage und bei den Australiern wird dieses Problem eben ganz besonders dramatisch, weil sie sich von den Räumlichkeiten und vom Zeitfenster gar nicht anders ausbreiten können. Es gibt keine Alternative, als alle Passagiere in diesem schmalen Zeitfenster zwischen 6:00 und 09:00 Uhr morgens abzufertigen. Deswegen war da das starke Interesse die Transaktionsdauer zu quantifizieren. Das hat man getan und man sollte sicherlich auch noch an anderen Stellen quantifizieren, wie lange denn derzeit die manuelle Abfertigung

dauert. Aber darüber lässt sich trefflich streiten. Das sind die Daten die ich habe, wenn wir andere Daten daneben legen können, kann man das mal analysieren. Aber ich glaube, dass man einen Zeitgewinn bekommen kann. Wie lange der einzelne Vergleich mit welchem Hersteller auch immer dauert, ob das jetzt ein japanischer Hersteller oder ein US-amerikanischer oder ein deutscher Hersteller ist, das sind meines Erachtens nur graduelle Unterschiede auf die Gesamtbruttozeit der Transaktion.

Biometrie – Schutz und Gefährdung von Grundrechten

*Alexander Roßnagel**

Meine sehr verehrten Damen und Herren,

ich will versuchen, die Informationen, die Ihnen die beiden vorangegangenen Vorträge präsentiert haben, aus rechtswissenschaftlicher Sicht zusammen zu führen und rechtlich zu bewerten. Daraus will ich dann Schlussfolgerungen für die Verwendung und die Gestaltung von Biometriesystemen ziehen. Diese Themen will ich Ihnen in folgender Art und Weise präsentieren: Zuerst will ich ganz kurz noch einmal andeuten, wie breit die künftigen Einsatzbereiche für Biometrie sind. Dann will ich zeigen, dass und wo Biometrie helfen kann, Grundrechte zu schützen. Der Schwerpunkt meines Vortrags wird aber auf der Frage liegen, ob und wie Biometrie Grundrechte gefährden kann. Ich will danach untersuchen, unter welchen Voraussetzungen Biometrie rechtlich zulässig ist, will auf die Frage der Auswahl unterschiedlicher Biometrieverfahren eingehen, vor allen Dingen aber einen Schwerpunkt auf die Ausgestaltung von Biometrieverfahren legen. Schließlich beabsichtige ich, zwei wichtige Anwendungen beispielhaft anzusprechen, nämlich die Benutzung von Biometrie in Ausweisen und die Verwendung von Biometrie in Arbeitsverhältnissen. Zum Schluss will ich versuchen, an den Vortrag von Herrn Strasser anzuschließen und einen Ausblick auf die künftige Entwicklung wagen, um dann – es folgt ja danach eine Diskussion mit Bundestagsabgeordneten – die Frage zu verfolgen: Gibt es aus rechtswissenschaftlicher Sicht einen Bedarf an gesetzlichen Regelungen zur Biometrie ?

* Alexander Roßnagel ist Professor Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes am Fachbereich Wirtschaftswissenschaften der Universität Kassel und wissenschaftlicher Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel.

1. Einsatzbereiche der Biometrie

Biometrie steht direkt an der Schwelle ihres gesellschaftsweiten Einsatzes. Wir werden in den nächsten Jahren erleben, dass Biometrie im privaten Bereich breit eingesetzt werden wird[1].

- Biometrie wird genutzt werden, um Geld abzuheben oder auch am Online-Banking teilzunehmen.
- In Restaurants werden wir mit unserem Fingerabdruck bezahlen.
- Zugangskontrollen z.B. zur Wohnung, zum Kraftfahrzeug, zum PC, zur Signaturkarte oder zu ähnlichen Dingen werden mit Biometrie realisiert.
- Auch wird es viele Geräte geben, die sich an den Nutzer anpassen und über den Fingerabdruck oder andere Biometrieverfahren erfahren, mit welchem Nutzer sie es jeweils zu tun haben[2].

Im Betrieb wird Biometrie bereits heute in Hochsicherheitsbereichen eingesetzt. Biometrieverfahren werden immer weiter um sich greifen und auch für Single-Sing-On, den Schutz von Geheimnissen, zur Gewährleistung von Rechtssicherheit (bei elektronische Signaturen) sowie zur innerbetrieblichen Leistungsabrechnung etwa in der Kantine oder der betrieblichen Tankstelle genutzt werden[3].

Und auch im staatlichen Bereich – es wurden ja schon Beispiele wie Pässe[4], Personalausweise[5], Ausländerpapiere und Führerscheine angesprochen – wird Biometrie vor allem zur Authentifizierung in immer mehr Anwendungen eingesetzt werden[6].

---

1 Siehe z.B. Gundermann/Probst, Biometrie, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, 1977; Hornung, Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft, Kritische Justiz 2004, S. 350.

2 Schwenke, Individualisierung und Datenschutz – Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung, Wiesbaden 2006, S. 49 ff..

3 Siehe hierzu z.B. Hornung/Steidle, Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausufemdes Kontrollpotential, Arbeit und Recht 2005, S. 201 ff.; Steidle, Multimedia-Assistenten im Betrieb – Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, Wiesbaden 2005, S. 232 ff..

4 Siehe z.B. Roßnagel/Hornung, Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck – Die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaat en ausgestellten Pässen und Reisedokumenten –, Die Öffentliche Verwaltung 2005, S. 983 ff.; Hornung, Biometric Passports and Identity Cards: Technical, Legal, and Policy Issues, European Public Law 2005, S. 501 ff..

5 Reichl/Roßnagel/Müller, Digitaler Personalausweis. Eine Machbarkeitsstudie, Wiesbaden 2005; Roßnagel/Hornung, Biometrische Daten in Ausweisen, Datenschutz und Datensicherheit 2005, S. 69 ff..

6 Siehe Hornung (Fn. 1), Kritische Justiz 2004, S. 349.

In Großbritannien, Kanada und USA werden biometrische Verfahren etwa auch eingesetzt, um die Doppelzahlung von Sozialleistungen zu verhindern[7].

2. Schutz von Grundrechten

Biometrie kann helfen eine Reihe von Grundrechten in ihrer Wahrnehmung zu unterstützen. Beispielhaft seien die durch Art. 2 Abs. 1 GG geschützte Entfaltung der Persönlichkeit und die durch Art. 12 Abs. 1 GG geschützte Berufsfreiheit genannt. Man könnten auch noch weitere und andere Grundrechte nennen. Es hilft der Entfaltung der Persönlichkeit, wenn jeder in der Lage ist, in kritischen Momenten seine Identität verlässlich nachzuweisen. Biometrie kann sehr große Komfortgewinne bieten, wenn man nicht mehr mit mehreren Karten hantieren muss, wenn man sich nicht mehr viele PINs und TANs und ähnliche schwer zu merkende Geheimnisse merken muss, wenn man sich das gesamte von Karten- und Nummern-Management ersparen und die Authentifizierung allein mit seiner Iris oder seinem Fingerabdruck realisieren kann[8]. Jeder kann mit Biometrie seine eigenen Ressourcen wie PC, Kraftfahrzeug und ähnliche Dinge gegen Missbrauch besser schützen, wenn er sich als berechtigter Nutzer ausweisen kann und andere, die dies ebenfalls tun wollen, es sehr schwer haben. Ist jemand Gewerbetreibender, kann er Biometrie beispielsweise einsetzen, um den Zugang zu seinen Betriebs- und Geschäftsgeheimnissen zu schützen. Er kann seine Kunden und seine Mitarbeiter besser authentifizieren, als dies bisher der Fall ist. Herr *Busch* hat drauf hingewiesen, dass man Biometrie als Zugriffsschutz bei Signaturen einsetzen kann. Wenn nur der Signaturschlüssel-Inhaber durch ein allein ihm verfügbares biometrisches Merkmal gegenüber der Signaturkarte nachweisen kann, dass er der berechtigte Nutzer ist, steigert dies die Rechtssicherheit spürbar[9]. Herr *Busch* hat auch bereits auf eine Reihe von Rationalisierungsmöglichkeiten hingewiesen. Diese werden natürlich von den Unternehmen künftig alle genutzt werden. Das hilft der Verwirklichung ihrer Berufsfreiheit.

Alle diese positiven Aspekte für Grundrechte setzen aber voraus, dass Biometrie freiwillig genutzt wird. Ich sehe aus grundrechtlicher Sicht kein großes Problem, wenn Biometrie freiwillig genutzt werden kann und die Freiwilligkeit gesichert ist. Diese kann allerdings in manchen Konstellationen in Frage stehen. Dann muss man

---

7 Gundermann/Probst (Fn. 1), S. 1979.

8 Siehe Hornung (Fn. 1), Kritische Justiz 2004, S. 344.

9 Siehe z.B. Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Baden-Baden 2003, S. 64 ff..

über die tatsächliche Freiwilligkeit der Nutzung diskutieren. Aber unterstellt Biometrie wird freiwillig genutzt, gibt es für die Zulässigkeit von Biometrie kein grundsätzliches Problem. Allerdings bleibt dann immer noch die konkrete Ausgestaltung des Biometrieverfahrens zu bedenken.

3. Gefährdung von Grundrechten

Interessant wird die Frage aus rechtlicher Sicht, wenn Biometrie nicht freiwillig, sondern unfreiwillig benutzt wird, wenn also jemand durch den Staat oder von anderen gezwungen wird, seine biometrischen Merkmale abzugeben und überprüfen zu lassen. In diesem Fall spielen vor allem drei Grundrechte eine Rolle:

- Die in Art. 1 GG geschützte Menschwürde verhindert normativ, dass der Betroffene katalogisiert oder auf biometrische Daten reduziert wird[10]. Das Grundrecht soll verhindern, dass alle Lebensäußerungen einer Person mit technischen Mitteln überwacht werden. Die Menschenwürde ist allerdings erst dann verletzt, wenn Kontrolltechnik sehr umfangreich und sehr intensiv für solche Zwecke genutzt würde. Bei all den Biometrieanwendungen, über die wir heute reden, ist die Grenze zu einem Verstoß gegen die Menschwürde noch relativ weit weg[11]. Man sollte die Menschenwürde in solch einer Diskussion nicht zur kleinen Münze schlagen und bei jeder passenden (oder unpassenden) Gelegenheit als Argumentationshilfe nutzen. Die Menschenwürde ist als Schutzschild gegen ganz große Bedrohungen des Menschseins gedacht.

- Interessanter für die derzeitigen Anwendungen ist die Vereinbarkeit eines Biometrieverfahrens mit der informationellen Selbstbestimmung[12]. Sie ist ein Grundrecht, das das Bundesverfassungsgericht angesichts der Risken der automatischen Datenverarbeitung aus einer Zusammenschau von freier Entfaltung der Persönlichkeit und Menschwürde heraus entwickelt hat[13]. Sie soll vom Grundsatz her dem Einzelnen ermöglichen, selbst über die Verwendung seiner

---

10 Siehe hierzu z.B. BVerfGE 27, 1 (6); 30, 1 (25f.); 45, 187 (228), 65, 1 (52).

11 Siehe hierzu auch Gundermann/Probst (Fn. 1), S. 1986 ff.; Hornung (Fn. 1), Kritische Justiz 2004, S. 351.

12 S. hierzu z.B. Gundermann/Probst (Fn. 1), S. 1982; Albrecht (Fn. 8), S. 152 ff.; Reichl/Roßnagel/Müller (Fn. 5), S. 110 ff.; Hornung, Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005, S. 178 ff..

13 Siehe auf europäischer Ebene mit weitgehend gleichem Schutzgehalt Art. 8 Abs. 2 EMRK und Art. 8 Grundrechte-Charta.

personenbezogenen Daten zu bestimmen[14]. In dieses Grundrecht darf eine staatliche Anordnung nur eingreifen, wenn sie in Form eines Gesetzes ergeht. Bereits der Wesentlichkeitsgrundsatz fordert, dass ein Eingriff nur in dieser Form zulässig ist. Er wurde durch das Volkszählungsurteil des Bundesverfassungsgerichts dahingehend konkretisiert, dass jeder Eingriff in das Grundrecht auf informationelle Selbstbestimmung einer klaren und bereichsspezifischen gesetzlichen Grundlage bedarf[15]. Dieser Eingriff muss außerdem dem Verhältnismäßigkeitsgrundsatz entsprechen[16]. Er muss also erstens geeignet sein. Ungeeignet wären Biometrieverfahren, bei denen die Missbrauchsmöglichkeiten zu hoch sind. Er muss zweitens erforderlich sein, es darf somit kein weniger eingreifendes Alternativverfahren geben. Demnach muss man das jeweils ausgewählte Verfahren immer an den möglichen, gleich geeigneten Alternativen messen. Eingesetzt werden darf nur das Verfahren, das am wenigsten intensiv in Grundrechte eingreift. Und der letzte Prüfstein der Verhältnismäßigkeit ist die Zumutbarkeit. Zu fragen ist, ob der Eingriff dem Betroffenen angesichts des Ziels, das man mit ihm verfolgt, objektiv zumutbar ist. Ein solches Ziel könnte beispielsweise die öffentliche Sicherheit sein und dann wäre das Biometrieverfahren, das hierfür eingesetzt wird, daran zu überprüfen, ob es bezogen auf das angestrebte Ziel diese drei Kriterien der Verhältnismäßigkeit erfüllt.

- Das dritte Grundrecht, das wir hier beachten müssen, ist das Gleichbehandlungsgebot des Art. 3 GG: Es darf allein aufgrund körperlicher Merkmale keine Benachteiligung geben. D.h. wir müssten eigentlich nach Biometrieverfahren suchen, die gleichmäßig auf die Bevölkerung insgesamt oder den Teil von ihr, der Adressat ist, anwendbar sind. Sofern hier ein Verfahren ausgewählt wird oder ausgewählt werden muss, das nicht gleichmäßig auf alle anwendbar ist, muss es zumindest nachteilsfreie Ersatzverfahren geben. Es darf auf jeden Fall kein spürbarer Nachteil deswegen geben, weil bei jemand zum Beispiel die Fingerkuppe nicht so ausgeprägt ist, dass sie entsprechend gut lesbar ist[17].

---

14 Zum Personenbezug biometrischer Daten siehe einerseits Saeltzer, Sind diese Daten personenbezogen oder nicht?, Datenschutz und Datensicherheit 2004, S. 218 ff. und andererseits Hornung, Der Personenbezug biometrischer Daten, Datenschutz und Datensicherheit 2004, S. 429 ff.; Albrecht (Fn. 9), S. 154 ff.; Gundermann/Probst (Fn. 1), S. 1983 ff..

15 Siehe BVerfGE 65, S. 1 (43 ff.).

16 Siehe im Zusammenhang mit Biometrieverfahren Roßnagel/Hornung (Fn. 5), Datenschutz und Datensicherheit 2005, S. 70 f..

17 Siehe hierzu z.B. Albrecht (Fn. 9), S. 164 ff.; Hornung (Fn. 12), S. 199 ff.; Reichl/Roßnagel/Müller (Fn. 5), S. 110.

Zusammenfassend kann man an dieser Stelle bereits festhalten: Biometrie ist nicht grundsätzlich verfassungswidrig, sondern in vielen Fällen eine Verbesserung der Verwirklichungsbedingungen von Grundrechten. Sie ist sogar selbst in dem Fall, in dem sie zwangsweise zur Anwendung kommt, rechtfertigungsfähig, wenn bestimmte Voraussetzungen erfüllt sind. Die wichtigste Voraussetzung ist, dass die Anwendung verhältnismäßig ist, also angesichts des verfolgten Ziels geeignet, erforderlich und zumutbar. Und die Verhältnismäßigkeit ist – das ist entscheidend – herstellbar. Es kommt also im Detail darauf an, wie die Biometrie in der jeweiligen Nutzung konkret ausgestaltet ist.

4. Zulässigkeit von Biometrieverfahren

Im Folgenden will ich einzelne Rechtfragen von Biometrieverfahren ansprechen und für diese zeigen, zu welchen Ergebnissen die dargestellten Grundsatzentscheidungen des Verfassungsrechts oder – soweit es vorhanden ist – des einfachen Rechts führen. Hierbei ist vorab festzustellen, dass man in Bezug auf das Verfassungsrecht hinsichtlich genereller Aussagen mit dem Verhältnismäßigkeitsgrundsatz ein kleines Problem hat: Seine Ergebnisse sind nämlich – wie der Name es sagt – von den Verhältnissen abhängig. Es kann Verhältnisse geben, unter denen eine bestimmte Maßnahme zulässig ist. Unter anderen Verhältnissen ist die gleiche Maßnahme unzulässig. Ich werde versuchen, Ihnen im Folgenden die jeweiligen Grundsätze vorzustellen, aber bei bestimmten Gestaltungen der Verfahren und bei einer bestimmten Dringlichkeit des jeweiligen Anliegens ist es nicht ausgeschlossen, dass der Verhältnismäßigkeitsgrundsatz dann vielleicht doch zu anderen Ergebnissen führt.

4.1 Auswahl von Biometrieverfahren

Steht man vor der Entscheidung, Biometrieverfahren einzusetzen, hat man die Wahl unter mehreren möglichen Verfahren. Für die folgenden Überlegungen will ich die derzeit drei gebräuchlichsten Verfahren berücksichtigen, nämlich Gesichtserkennung, Fingerabdruck und Iris-Scan[18]. Für die Auswahl zwischen diesen müssen aus dem Blickwinkel des Grundrechts- und des Datenschutzes mindestens fünf Kriterien berücksichtigt werden.

---

18 Siehe zu diesen z.B. Reichl/Roßnagel/Müller (Fn. 5), S. 75 ff.; zu weiteren s. z.B. Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Biometrische Identifikationssysteme, BT-Drs. 14/10005 (2002); Albrecht (Fn. 9), 39 ff.; Steidle (Fn. 3), S. 237 ff.; Hornung (Fn. 12), S. 74 ff..

Das erste Kriterium ist die Ausprägung des Merkmals. Es betrifft die Aspekte, die ich gerade im Zusammenhang mit dem Gleichbehandlungsgebot des Art. 3 GG dargestellt habe. Das Kriterium ist dann bestmöglich erfüllt, wenn das Biometrieverfahren niemand diskriminiert[19].

Zweitens – das ist eine Anforderung aus dem Schutz der informationellen Selbstbestimmung – muss die biometrische Kontrolle transparent sein. D.h. für den Betroffenen muss jederzeit feststellbar sein, dass er kontrolliert wird. Die Erfüllung dieses Kriteriums ist am besten dann gewährleistet, wenn das Verfahren nur dann funktioniert, wenn er mitwirkt. Verfahren bei denen es möglich ist, biometrische Daten zu erheben, ohne dass der Betroffene mitwirkungsbereit sein muss, sind in dieser Hinsicht riskant[20].

Drittens sind in dieser Hinsicht Verfahren dann weniger geeignet, wenn für sie die Kontrolldaten auch in anderer Weise gefunden oder beschafft werden können. Herr *Busc*h hat auf das Beispiel hingewiesen, dass, wenn er eine Flasche angreift, sein Fingerabdruck zurück bleibt und für Identifizierungszwecke ohne seine Mitwirkung genutzt werden kann. Das dritte zu beachtende Kriterium ist somit die Flüchtigkeit der biometrischen Spuren. Danach sind Biometrieverfahren, die nur der Identitätskontrolle dienen[21], für den Grundrechtsschutz umso riskanter, je flüchtiger die Merkmale sind, also getrennt von dem jeweiligen originalen biometrischen Merkmal auftreten können[22].

Herr *Busch* hat auch darauf hingewiesen, dass es bei der Kontrolle biometrischer Merkmale möglicherweise Zusatzinformationen gibt, die je nach Verfahren unterschiedlich aussagekräftig und umfangreich sein können. Diese Zusatzinformationen sind für den Kontrollzweck, zu dem das Biometrieverfahren eingesetzt wird, überflüssig. Je mehr überflüssige Informationen ein Biometrieverfahren liefert, umso riskanter ist es aus der Sicht des Grundrechtsschutzes[23].

---

19 Siehe hierzu z.B. Albrecht (Fn. 9), S. 164 ff.; Hornung (Fn. 12), S. 199 ff.; Reichl/Roßnagel/Müller (Fn. 5), S. 124f..

20 Siehe hierzu z.B. Gundermann/Probst (Fn. 1), S. 2005; Hornung (Fn. 12), S. 184 f. und S. 197; Reichl/Roßnagel/Müller (Fn. 5), S. 124.

21 Nur einer 1:1-Kontrolle und keiner n:1-Feststellung.

22 Siehe hierzu z.B. Hornung (Fn. 12), S. 185; ders., (Fn. 1), Kritische Justiz 2004, S. 352; Reichl/Roßnagel/Müller (Fn. 5), S. 124.

23 Siehe z.B. Golembiewski/Probst, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren, 2003, http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, S. 64f.; Gundermann/Probst (Fn. 1), S. 1976; Albrecht (Fn. 9), S. 172; Hornung (Fn. 12), 185; Reichl/Roßnagel/Müller (Fn. 5) S. 123.

Schließlich bleibt als das letzte Kriterium die Leistungsfähigkeit des Biometrieverfahrens. Die Leistungsfähigkeit ist bezogen auf die jeweilige Anwendung und den mit ihr verfolgten Zweck zu bestimmen. Hierbei kann es einen großen Unterschied machen, ob mit dem Biometrieverfahren Grenzkontrollen durchgeführt werden sollen oder ein Single-Sign-On-Verfahren realisiert werden soll. Für beide können die Anforderungen sehr unterschiedlich sein. Grundsätzlich ist für die Leistungsfähigkeit zum einen die Falsch-Akzeptanz-Rate zu betrachten. Dies ist ein Unterkriterium, das sich auf die Eignung des Verfahrens niederschlägt[24]. Beispielsweise wäre bei einem biometrischen Grenzkontrollverfahren, das genau so viele Personen mit falscher Identitätsangabe durchlässt, wie dies bisher bei geübten Grenzkontrolleuren bei Verwendung des bisherigen Personalausweises der Fall ist, der zusätzliche Grundrechtseingriff, der in der Kontrolle biometrischer Daten liegt, nicht gerechtfertigt, weil dieses Verfahren im Vergleich zu dem jetzigen Verfahren kein Gewinn bringt und deswegen bezogen auf das Ziel, eine höhere Sicherheit zu erreichen, ungeeignet wäre. Die Falsch-Rückweisungs-Rate als zweites Unterkriterium betrifft sowohl die Eignung als auch die Erforderlichkeit des Grundrechtseingriffs[25]. Im Verhältnis mehrerer Biometrieverfahren zueinander, ist das Verfahren zu wählen, das bei gleicher Eignung weniger Personen zu unrecht zurückweist und ihnen eine Sonderkontrolle, weitere zusätzliche Maßnahmen und Zeitverzögerungen abfordert. Schließlich bezieht sich die Ausgestaltung des Ersatzkontrollverfahrens als drittes Unterkriterium auf die Zumutbarkeit des Eingriffs. Wenn die Rate der Ersatzverfahren zu hoch ist[26] oder sehr umständlich und zeitraubend ist, kann der damit verbundene Grundrechtseingriff für die Betroffenen objektiv nicht zumutbar sein[27].

Das schwierige Problem bei der Auswahl von Biometrieverfahren ist, dass die einzelnen Verfahren bezogen auf die Kriterien nicht eindeutig positiv oder negativ sind, sondern die Kriterien von ihnen sehr unterschiedlich erfüllt werden. Daher fällt es schwer, eines der Verfahren als besonders grundrechtsschonend herauszugreifen. Vielmehr ist für das jeweilige Anwendungsfeld genau zu prüfen, welches der Verfahren hinsichtlich der – je nach den Verhältnissen unterschiedlich zu gewichtenden – Kriterien mehr oder weniger Vorteile bietet. In der folgenden Tabelle erfolgt eine – tendenzmäßige – Zuordnung von Kriterium und Verfahren.

---

24 Siehe hierzu Reichl/Roßnagel/Müller (Fn. 5), S. 121 ff.

25 Siehe näher Reichl/Roßnagel/Müller (Fn. 5), S. 121 ff.; Hornung (Fn. 12), S. 179 ff..

26 Diese Rate hängt vor allem mit der Merkmalsausprägung zusammen.

27 Siehe Hornung (Fn. 12), S. 199 ff..

Verfahren Kriterien	Gesicht	Finger	Iris
Merkmalsausprägung	+	–	+
Mitwirkung	–	+	+ +
Flüchtigkeit	+ +	–	+ +
Zusatzinformation	–	–	– –
Leistungsfähigkeit	– –	-	+

4.2 Gestaltung von Biometrieverfahren

Es wurde bereits darauf hingewiesen, dass die Verhältnismäßigkeit des Grundrechtseingriffs beeinflusst, die Beeinträchtigung reduziert oder die Zumutbarkeit gesteigert werden kann, je nachdem wie das Biometrieverfahren gestaltet wird. Um dies zu erläutern, werden im Folgenden beispielhaft typische Phasen von Biometrieverfahren angesprochen, deren Gestaltung Einfluss auf die Rechtmäßigkeit des gesamten Verfahrens haben kann.

4.2.1 Speicherung biometrischer Daten

Betrachten wir die Speicherung der Vergleichsdaten. Im Enrollment-Prozess werden biometrische Daten erhoben, um später zum Vergleich mit den jeweils aktuellen Kontrolldaten zu dienen. Hier stellt sich zuerst die Frage, welche Daten gespeichert werden sollen. Hinsichtlich der Anforderungen der Datensparsamkeit und Erforderlichkeit, ist es datenschutzrechtlich erheblich günstiger, wenn keine Volldaten gespeichert werden, sondern Templates, weil sie weniger personenbezogene Merkmale

zum Ausdruck bringen[28]. Kann man in der Anwendung templatefreie Verfahren verwenden, hätte man ein Verfahren, bei dem noch weniger personenbezogene Daten zum Einsatz kommen. In diesen Verfahren werden die Templates nur dazu benutzt, um in kryptographischen Verfahren eingesetzt zu werden. Mit diesen wird irgendein beliebiger Satz verschlüsselt und das Kryptogramm als Kontrolldatum genommen. Bei der Kontrolle wird aus den aktuellen biometrischen Kontrolldaten auf die gleiche Weise ein Kryptogramm erzeugt und mit dem Vergleichskryptogramm verglichen[29]. Ähnlich verhält es sich mit den Hashwerten, die bei Template-Protection-Verfahren zum Einsatz kommen, über die Herr *Busch* in seinem Vortrag berichtet hat. Auch wenn keine anonymen technischen Verfahren verwendet werden, reicht es in vielen Fällen für die Kontrollzwecke aus, Berechtigungen zu vergleichen. In diesen kommt es nicht auf die Identifizierung des Einzelnen an, sondern entscheidend ist nur, dass er berechtigt ist, zum Beispiel ein bestimmtes Betriebsgelände zu betreten. Dann wäre es nicht notwendig, die Vergleichsdaten personenbezogen zu speichern. Vielmehr würde es ausreichen, eine anonymisierte Liste von Vergleichsdaten zu haben und mit deren Hilfe zu prüfen, ob derjenige, der Eintritt begehrt, in dieser Liste aufgeführt ist. Zusammenfassend ist festzustellen, dass es vielfältige Gestaltungsformen gibt, die datensparsamer sind, als die personenbezogene Speicherung von Volldaten. Sind diese für die Anwendung ebenso gut geeignet, ist die Speicherung von Volldaten im Regelfall unzulässig.

Das Bundesdatenschutzgesetz kennt besonders schützenswerte Daten, die in § 3 Abs. 9 definiert sind[30]. Diese dürfen nach § 28 Abs. 6 – 9 BDSG im Regelfall[31] nur erhoben, gespeichert und genutzt werden, wenn die ausdrückliche Zustimmung des Betroffenen vorliegt. Zu diesen Daten gehören Daten über die rassische und ethnische Herkunft. Diese Kategorien von Daten sind in diese Regelung des Bundesdatenschutzgesetzes deswegen aufgenommen worden, um rassistische Diskriminierungen zu vermeiden[32]. Beim Gesichtsbild ist es nicht zu vermeiden, dass solche Daten erhoben und verarbeitet werden, die Rückschlüsse auf die rassische und ethnische Herkunft ermöglichen. Dies führt zu der Schlussfolgerung, dass die im privaten Bereich – in dem dann der § 28 Abs. 6 – 9 BDSG zur Anwendung kommt – die Kon-

---

28 Siehe z.B. Gundermann/Probst (Fn. 1), S. 1975, 1984, 1997.

29 Siehe z.B. Gundermann/Probst (Fn. 1), S. 1976, 1985, 1997; Albrecht (Fn. 12), S. 56.

30 Siehe zu diesen Tinnefeld, Geschützte Daten, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, S. 496 ff..

31 Zu den hier in der Regel nicht einschlägigen Ausnahmen des § 28 Abs. 6 BDSG s. Simitis, in: ders. (Hrsg.), BDSG-Kommentar, 6. Aufl. 2006, § 28 Rn. 320 ff..

32 Siehe Simitis (Fn. 31), § 3 Rn. 256.

trolle des Gesichtsbildes nur mit ausdrücklicher Zustimmung des Betroffenen vorgesehen werden kann[33]. Das Gleiche gilt für Iris-Scan, wenn bei ihm zugleich auch Daten über die Gesundheit anfallen.

Weiterhin ist für die rechtliche Bewertung einer Biometrie-Anwendung entscheidend, an welchem Ort die Daten gespeichert werden. Wir haben in den vorgehenden Vorträgen gehört, dass eine zentrale Speicherung mit erheblich größeren Risiken verbunden ist als eine dezentrale Speicherung beim Betroffenen. Die dezentrale Speicherung beim Betroffenen hat auch noch den Vorteil, dass die Kontrollzwecke, wenn die biometrischen Daten in einer Chipkarte, in einem RFID oder in einem anderen schützbaren Datenträger aufbewahrt werden, durch zwei Sicherungsfunktionen erfüllt werden, nämlich durch die Sicherungsfunktionen des „Seins“ (die Biometrie) und des „Habens“ (die Sachherrschaft über das Token).

Schließlich ist noch wichtig, zu welchem Zweck die Daten gespeichert werden. Im Regelfall wird es nur zulässig sein, sie für Authentisierungszwecke – also für die Verifikation des Merkmalträgers – zu verwenden. Dies muss dann auch technisch– am besten durch die Wahl des Orts der Speicherung – entsprechend sichergestellt sein und ein Missbrauch ausgeschlossen werden.

4.2.2 Verarbeitung biometrischer Daten

Betrachten wir die zweite Phase, in der biometrische Daten verarbeitet werden. Das ist die Kontrolle des Merkmalsträgers. Für diese werden Kontrolldaten erhoben und mit den bereits früher erhobenen Vergleichsdaten verglichen. Auch hier muss durch Organisation und Technik der Kontrolle sicher gestellt sein, dass nur eine Verifikation im 1:1-Vergleich möglich ist und keine Identifikation einer Person innerhalb einer großen Menge unbekannter Menschen (n:1).

Eine weitere Frage, die sich stellt, ist, wo die Erhebung der Kontrolldaten und ihr Vergleich mit den Vergleichsdaten stattfinden. Auf den ersten Blick erscheint es sicherer, wenn die Daten beispielsweise auf der Chipkarte verglichen werden. Dies scheint besser geeignet zu sein, die Zweckbindung der Verifikation sicher zu stellen. Aber es besteht bei einem Matching-on-Card ein gewisses Fälschungsrisiko. Die Karte könnte ja so manipuliert sein, dass sie, egal was sie prüft, immer das Ergebnis „OK“ liefert. Der Kontrolleur müsste diesem Ergebnis der Karte, die unter der Herrschaft des zu Kontrollierenden steht, blind vertrauen. Wollte man diesen Weg gehen,

[33] Siehe z.B. Steidle (Fn. 3), S. 245f.; siehe auch Gundermann/Probst (Fn. 1), S. 1993 f., S. 2006.

wären technische Lösungen gefragt, die sicherstellen, dass bei der Vergleichsprüfung durch die Karte keine Manipulationen stattfinden. Auch ist der datenschutzrechtliche Mehrwert dann fraglich, wenn die Kontrolldaten – wie im Regelfall – außerhalb der Karte erhoben werden (müssen), so dass ohnehin biometrische Daten außerhalb der Karte genutzt werden. Anders wäre es nur dann, wenn beispielsweise ein Fingerabdrucksensor auf der Karte implementiert wäre. Dies ist bei der Erhebung von Fingerabdrucksdaten möglich, bei anderen biometrischen Verfahren aber derzeit ausgeschlossen[34].

Wenn die Kontrolle nicht in der Karte stattfindet, sondern außerhalb in einer Kontrolleinheit, muss nach § 9 BDSG sichergestellt sein[35], dass die so erhobenen Daten nicht für andere Zwecke verwendet werden[36]. In diesem Fall hat der Kontrolleur eine höhere Sicherheit, weil die Kontrolleinheit unter seiner Herrschaft steht. Hier besteht dann ein Missbrauchsrisiko in anderer Hinsicht, nämlich dass die aktuell erhobenen biometrischen Kontrolldaten für andere Zwecke entfremdet werden. Die Karte muss in der Kontrollsituation die Vergleichsdaten liefern, die dann ebenfalls für andere Zwecke verwendet werden könnten. Die Lösung wird darin bestehen müssen, dass die Zweckbindung der Verifikation technisch realisiert wird – etwa dadurch, dass nach der Kontrolle die nicht mehr benötigten Daten immer sofort gelöscht werden. Die Kontrolleinheit müsste auch für die kontrollierende Instanz eine „Blackbox" sein, aus der die erhobenen Daten nicht ausgelesen werden können.

Es wurde bereits darauf hingewiesen, dass das Datenschutzrecht für den Betroffenen eine ausreichende Transparenz fordert. Die Daten müssen nach dem Grundsatz des § 4 BDSG beim Betroffenen unter seiner Mitwirkung erhoben werden[37]. In dieser Hinsicht besteht ein gewisses Risiko bei der Gesichtsbildkontrolle, weil hier ein Erheben der biometrischen Daten auch ohne Mitwirkung des Betroffenen möglich sein könnte. Erfolgt dabei zugleich eine Beobachtung öffentlich zugänglicher Räume, sind der Umstand der Beobachtung und die verantwortliche Stelle außerdem nach § 6b BDSG erkennbar zu machen. Wenn die Kontrolle auf der Karte stattfindet oder auf ihr ein Fingerabdrucksensor installiert ist, dann unterfällt die Karte auch noch den Unterrichtungs- und Transparenzpflichten, die § 6c BDSG vorsieht[38].

---

34 Siehe auch Roßnagel/Hornung (Fn. 5), Datenschutz und Datensicherheit 2005, S. 73.

35 Siehe Heibey, Datensicherung, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, S. 576 ff..

36 Siehe zur Zweckbindung Albrecht (Fn. 12), S. 166 ff..

37 Siehe für biometrische Verfahren Gundermann/Probst (Fn. 1), S. 2005.

38 Siehe hierzu z.B. Hornung, Datenschutz für Chipkarten, Datenschutz und Datensicherheit 2004, S. 15 ff..

4.2.3 Sicherung von Biometrieverfahren

Der letzte hier zu erörternde Gegenstand der rechtsgemäßen Technikgestaltung ist die Sicherung der Biometrieanwendungen[39]. Zum einen müssen die biometrischen Vergleichsdaten fälschungssicher erhoben werden. Dies ist vor allem eine organisatorische Aufgabe des Enrollment-Prozesses. Zum anderen müssen die biometrischen Vergleichsdaten fälschungssicher gespeichert sein. Dieses Ziel kann durch elektronische Signaturen erreicht werden. Drittens müssen die Daten ausspähungssicher sein. Dies kann durch ihre Verschlüsselung erreicht werden. Viertens muss der Kontrollprozess so erfolgen, dass keine Manipulationen (z.B. Silikonfinger, Tonträger, Bild) stattfinden können. Dies schließt rein automatische Kontrollen vielfach aus und fordert eine Beobachtung der biometrischen Kontrollen. Alternativ könnte eine sichere Lebenderkennung eingesetzt werden. Fünftens muss die Zweckbindung sowohl der Vergleichsdaten als auch der Kontrolldaten gewährleistet werden. Für beide muss technisch sichergestellt sein, dass nur während eines berechtigten Kontrollvorgangs und nicht außerhalb eines solchen auf diese Daten zugegriffen werden kann. Dies kann zum einen dadurch erreicht werden, dass der zugriffsgeschützte Träger der Vergleichdaten und das Kontrollgerät sich gegenseitig authentifizieren, und dadurch gewährleistet werden, dass ein Ausschleusen der Kontroll- oder der empfangenen Vergleichsdaten aus der Kontrolleinheit technisch nicht möglich ist. Schließlich sind die Daten sofort nach der Kontrolle automatisch zu löschen. Werden diese Anforderungen erfüllt, kann die Verarbeitung personenbezogener Daten in Biometrieverfahren, die zulässigerweise stattfindet, aus Sicht der Sicherheit akzeptiert werden. Wenn diese Anforderungen nicht erfüllt werden können, besteht eine sehr große Vermutung, dass die Nutzung der Biometrie Probleme hat, das Verhältnismäßigkeitsprinzip zu erfüllen.

4.3 Anwendungsbeispiele

Hinsichtlich der Zulässigkeit von Biometrieanwendungen und ihrer Gestaltung will ich abschließend kurz auf zwei wichtige Anwendungsfelder eingehen – auf Biometrie in staatlichen Ausweisen und in betrieblichen Anwendungen.

---

39 Siehe hierzu Roßnagel/Hornung (Fn. 5), Datenschutz und Datensicherheit 2005, S. 71.

4.3.1 Biometrie in Ausweisen

Der Einsatz von Biometrieverfahren in staatlichen Ausweisen ist nur auf gesetzlicher Grundlage möglich. Dies ergibt sich bereits aus dem Wesentlichkeitsgrundsatz und seiner Ausprägung im Volkszählungsurteil. Eine solche Grundlage haben wir für den Pass durch die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten[40], die im Januar 2005 in Kraft getreten ist[41]. Für den Personalausweis haben wir im gültigen Personalausweisgesetz keine solche ausreichende Rechtsgrundlage. Es gibt eine Ankündigungsregelung in § 1 Abs. 4 PersAuswG. Aber der Gesetzgeber hat in § 1 Abs. 5 PersAuswG ausdrücklich festgehalten, dass er über eine Reihe von Fragen wie die Auswahl der Biometrieverfahren noch mal eigens in einem Gesetz entscheiden will[42]. Für staatliche Ausweise gelten alle die Gestaltungsanforderungen, die bereits dargestellt worden sind[43]. Die wichtigsten sind sogar im Personalausweisgesetz eigens für Personalausweise geregelt: Nach § 1 Abs. 5 Satz 2 PersAuswG darf keine zentrale Speicherung der Vergleichsdaten stattfinden. Vielmehr müssen diese im Ausweis gespeichert sein. Die Daten dürfen nach § 3 Abs. 5 PersAuswG nur für die Verifikation des Ausweisträgers und die Überprüfung der Echtheit des Ausweises verwendet werden. Sie dürfen nicht in anderen Dateien gespeichert werden, um mit diesen Datensammlungen in einer größeren Menschenmenge bestimmte Personen zu suchen oder einzelne Personen zu identifizieren[44]. Schließlich muss es effektive diskriminierungsfreie Ersatzverfahren geben, wenn diese Ausweise zur Kontrolle benutzt werden und die überprüften Merkmale in der Kontrolle bei bestimmten Personen nicht greifen[45].

Ich möchte noch auf einen Punkt hinweisen, der mir bisher etwas unterbelichtet erscheint. Das Bundesverfassungsgericht hat für Risiken für Grundrechte, die durch technische Systeme verursacht werden, mehrfach geurteilt, dass der Staat sich schützend und fördernd vor die Grundrechte stellen muss[46]. Er hat hier eine Sorgepflicht dafür, dass die Voraussetzungen zur Ausübung der Grundrechte auch im Verhältnis

---

40 Amtsblatt der Europäischen Union Nr. L 385 vom 29. Dezember 2004, S. 1.

41 Siehe Roßnagel/Hornung (Fn. 4), Die öffentliche Verwaltung 2005, S. 984 ff..

42 Siehe z.B. Hornung (Fn.12), S. 173 ff..

43 Siehe näher Reichl/Roßnagel/Müller (Fn. 5), S. 120 ff. und S. 226 ff..

44 Siehe z.B. Roßnagel/Hornung (Fn. 5), Datenschutz und Datensicherheit 2005, S. 69.

45 Siehe z.B. Reichl/Roßnagel/Müller (Fn. 5), 228; Hornung (Fn. 12), S. 199 ff..

46 Siehe z.B. BVerfGE 39, S. 1 (42); 46, S. 160; 49, S. 89, (140 ff.); 53, S. 30 (57); 79, S. 174 (201f.).

zu technischen Systemen gewährleistet sind. Mit Blick auf biometrische Verfahren in Ausweisen bedeutet dies, dass die Bundesrepublik Deutschland eine Sorgepflicht hat, dass die Grundrechte von deutschen Bürgern im Ausland auch wahrgenommen werden können. Aus ihrer verfassungsrechtlichen Pflicht heraus muss sie Einfluss darauf nehmen, dass biometrische Verfahren in internationalen Vereinbarungen und in der internationalen Standardisierung so gestaltet werden, dass sie mit den Voraussetzungen und Anforderungen der Grundrechte vereinbar sind. Werden beispielsweise bei der International Civil Aviation Organization (ICAO)[47] Standards für Fragen entwickelt, welche Biometrieverfahren für Pässe verwendet werden, ob die biometrischen Daten verschlüsselt oder unverschlüsselt gespeichert werden, ob sie signiert oder nicht signiert werden, dann ist der Vertreter der Bundesrepublik in den jeweiligen Gremien in seiner Entscheidung nicht ganz frei, sondern ist als Staatsvertreter an diese Sorgepflicht gebunden und muss seinen Einfluss geltend machen, dass dort Lösungen gewählt werden, die unserem Grundrechtsverständnis entsprechen.

4.3.2 Biometrie im Arbeitsverhältnis

Auf den Einsatz von Biometrieverfahren im Arbeitsverhältnis kann hier nur sehr kurz eingegangen werden. Im Gegensatz zu Biometrieverfahren in staatlichen Anwendungen gelten im Arbeitsverhältnis einige Besonderheiten[48]. Rechtsgrundlage für ihren Einsatz ist der Arbeitsvertrag[49] und das daraus abzuleitende Direktionsrecht des Arbeitgebers. Dieses ist aber begrenzt durch das Mitbestimmungsrecht der Personalvertretung[50]. Das Bundesarbeitsgericht hat 2004 eindeutig entschieden, dass dem Betriebsrat hinsichtlich der Einführung von Biometrieverfahren ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 und 6 BetrVG zusteht[51]. Das Gleiche muss nach den vergleichbaren Bestimmungen auch für den Personalrat gelten. Bei der inhaltlichen Ausgestaltung dieses Mitbestimmungsrechts ist zu beachten, dass das Betriebsverfassungsgesetz in § 75 Abs. 1 beiden Parteien aufgibt, alle Arbeitnehmer ohne Diskriminierung gleichermaßen nach Recht und Billigkeit zu behandeln[52], und

---

47 Siehe zur ICAO näher http://www.luftrecht-online.de/einzelheiten/verwaltung/icao.htm und http://www.icao.int/icao/en/atb/fal/mrtd/guide.htm

48 Zur Biometrie im Arbeitsverhältnis s. z.B. Albrecht (Fn. 12), S. 195 ff.; Hornung (Fn. 1), Kritische Justiz 2004, S. 354; Steidle (Fn. 3), S. 232 ff.; Hornung/Steidle (Fn. 3), Arbeit und Recht 2005, S. 201 ff..

49 Siehe z.B. Gundermann/Probst (Fn. 1), S. 2004.

50 Siehe näher Albrecht (Fn. 9), S. 203 ff.; Hornung/Steidle (Fn. 3), Arbeit und Recht 2005,S. 201 ff..

51 Siehe BAG, Datenschutz und Datensicherheit 2004, S. 433 ff.

52 Siehe z.B. Steidle (Fn.3), S. 246 f..

ihnen in § 75 Abs. 2 zur Pflicht macht, die Persönlichkeitsrechte der Arbeitnehmer zu schützen[53]. Über diesen Verweis sind alle bisherigen Ausführungen zur rechtsgemäßen Gestaltung von Biometrieverfahren auch im Arbeitsverhältnis zu beachten. Besondere Relevanz im Arbeitsverhältnis haben die Anforderungen, dass die Verfahren, die angewendet werden, diskriminierungsfrei sind, dass – wo immer möglich – pseudonyme und anonyme Daten eingesetzt werden und dass – wo dies der Zweck der Biometrieanwendung ermöglicht – die biometrischen Vergleichsdaten im Betriebsausweis oder in ähnlichen Trägern gespeichert werden, die sich im Gewahrsam des Arbeitnehmers befinden.

5. Zukunftsperspektiven

Wenn über biometrische Verfahren, ihre Vorteile und ihre Risiken nachgedacht wird, dürfen wir uns nicht auf die Betrachtung beschränken, wie sich die Biometrie und ihre Anwendungen in den nächsten zwei, drei Jahre weiterentwickeln. Vielmehr müssen wir uns auch die Frage stellen, was sein würde, wenn Biometrie – über die Anwendungen, die eingangs aufgezählt wurden hinaus – immer weiter entwickelt und immer breiter genutzt wird. Erlauben sie mir zu diesen Zukunftsperspektiven vier kurze Bemerkungen.

Zum einen müssen wir uns bei allen Diskussionen über künftige Perspektiven klar machen, dass bei biometrischen Verfahren mit nicht veränderlichen körperlichen Merkmalen gearbeitet wird, die – wenn es funktioniert – eine eindeutige Identifizierung ermöglichen und die möglicherweise – was heut noch nicht so ganz sicher ist – zusätzliche Informationen bieten. Dies bedeutet, dass jede unfreiwillige Nutzung von Biometrieverfahren ein gravierender Grundrechtseingriff ist.

Daher könnte zweitens, wenn Biometrie in dieser Weise in großem Umfang genutzt wird, der Punkt erreicht werden, an dem Quantität in Qualität umschlägt und wir nicht mehr in einer Gesellschaft leben, die das Bundesverfassungsgericht vor Augen hatte, als es sein Volkszählungsurteil formuliert und die informationelle Selbstbestimmung als objektiven Maßstab für eine freie und demokratische Gesellschaft entwickelt hat. Ich würde mich freuen, wenn zu der Frage, wie eine solche Entwicklung verhindert werden kann, in der folgenden Podiumsdiskussion die eine oder andere Überlegung angestellt würde.

---

53 Siehe z.B. Albrecht (Fn. 9), S. 197 ff.; Hornung/Steidle (Fn. 3), Arbeit und Recht 2005,S. 201 ff..

Drittens könnte zu einer solchen Entwicklung beitragen, dass eine breite Verwendung von Biometrie gesellschaftliche Strukturen verändern kann. Überall in der Gesellschaft werden derzeit Identitätsinfrastrukturen aufgebaut[54]. Neben den vorhandenen staatlichen Identitätsinfrastrukturen mit staatlichen Ausweisen als Identitätsrepräsentanten, werden im Kontext unterschiedlicher E-Commerce- und E-Goverment-Anwendungen viele weitere Identitätsinfrastrukturen etabliert. Für alle diese verschiedenen Identitätsinfrastrukturen werden jeweils eigene Identitätsrepräsentanten wie Zertifikate, Namen zum Einloggen, Betriebs- oder Kundenausweise vergeben. Mit deren Hilfe versuchen die Betreiber dieser Infrastrukturen, mehr über ihre Klienten, Kunden und Partner zu erfahren und diese an sich zu binden. Diese vielen Identitätsinfrastrukturen, die immer mehr Menschen bei immer mehr Handlungen identifizieren und dies protokollieren, sind derzeit nur deshalb noch akzeptabel, weil sie die Daten getrennt voneinander sammeln und halten. Umgekehrt sind sie umso problematischer, je mehr diese Daten zusammengeführt werden. Mit Hilfe von Biometrie könnten diese Identitätsinfrastrukturen nicht nur effektiver arbeiten, sondern auch leichter die bisherige, Grundrechte und Freiheit schützende informationelle Gewaltenteilung aufheben.

Viertens ist für die nachfolgende Diskussion wichtig, dass der Gesetzgeber solche möglichen oder gar absehbaren Entwicklungen nicht unberücksichtigt lassen darf. Ihn trifft eine Schutzpflicht für die ihm anvertrauten Grundrechte und für die demokratische Struktur unserer Gesellschaft[55]. Selbst wenn er diese zu einem bestimmten Zeitpunkt durch gesetzliche Vorkehrungen erfüllt, trifft ihn bei einer Veränderung der Umstände und – mit ihnen – der Risiken eine Nachbesserungspflicht[56]. Um dieser rechtzeitig nachkommen zu können, ist er verpflichtet, die Entwicklung ständig zu beobachten[57]: Wo entstehen kritische Entwicklungen, denen rechtzeitig durch eine Nachbesserung der Rechtsordnung zu begegnen ist. In der nachfolgenden Podiumsdiskussion der Bundestagsabgeordneten würde ich daher gern die folgende Frage diskutiert sehen: Haben wir in der Bundesrepublik Deutschland Strukturen, Institutionen und Verfahren, die ausreichend fähig sind, die Entwicklung zu beobachten und zu prognostizieren, aus den Erkenntnissen zu lernen und Instrumente einzusetzen, um wirksam Einfluss nehmen zu können?

---

54 Siehe hierzu näher Roßnagel (Hrsg.), Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung, Baden-Baden 2006.

55 Siehe Fn. 46.

56 Siehe z.B. BVerfGE 49, S. 89 (130f.); 65, S. 1 (56); BVerfG, Neue Juristische Wochenschrift 2005, S. 1340.

57 Siehe näher Roßnagel, Die parlamentarische Verantwortung für den technischen Fortschritt, Zeitschrift für Rechtspolitik 1992, S. 55 ff..

6. Gesetzgebungsbedarf?

Abschließend soll die Frage nicht unbeantwortet bleiben, ob wir aktuell Regelungen zur Biometrie benötigen. Wenn man nicht die eben erörterte Langzeitperspektive im Blick hat, sondern die nächsten zwei, drei Jahre – also die jetzige Legislaturperiode, dann möchte ich folgende Antwort geben. Im hoheitlichen Bereich ist ohnehin für jeden Einsatz von Biometrie eine entsprechende gesetzliche Grundlage erforderlich. In dieser gesetzlichen Regelung sollten zur Klarstellung die verfassungsrechtlich geforderten und hier erläuterten Gestaltungsanforderungen für die jeweilige Biometrieanwendung geregelt werden. Für den Einsatz von Biometrie in Arbeitsverhältnissen gibt es durch die betriebliche Mitbestimmung und die Ausgestaltung von Betriebsvereinbarungen ein taugliches Instrument, das ermöglicht, die Probleme unter Beachtung der beteiligten Interessen in Selbstregulierung zu regeln. Im Bereich des allgemeinen Privatrechtsverkehrs kann man mit der gebotenen Auslegung vorhandener Regelungen zu einem derzeit vertretbaren Ergebnis gelangen. Die allgemeinen datenschutzrechtlichen Erlaubnisregeln, insbesondere die allgemeine Interessenabwägung des § 28 Abs. 1 Satz 2 Nr. 2 BDSG, reichen nicht aus, um einen besonders intensiven Grundrechtseingriff wie den unfreiwilligen Einsatz von Biometrie zu rechtfertigen. Das Bundesverfassungsgericht fordert für Eingriffe in die informationelle Selbstbestimmung präzise und bereichsspezifische Regelungen. An dieser Forderung gemessen ist die allgemeine Interessenabwägung bereits für die üblichen Interessenkonflikte bedenklich. Keinesfalls aber kann diese inhaltsleere Regelung einen Eingriff in die informationelle Selbstbestimmung rechtfertigen, der sich in seiner Intensität von dem üblichen Interessenkonflikt zwischen Datenverarbeiter und Betroffenen deutlich abhebt[58]. Hätte der Gesetzgeber die Erhebung biometrischer Daten auch gegen den Willen des Betroffenen allein auf der Grundlage einer Interessenabwägung durch den Datenverarbeiter zulassen wollen, hätte er dies ausdrücklich regeln müssen. Da er dies nicht getan hat, ist eine Nutzung von Biometrieverfahren gegen den Willen des Betroffenen unzulässig. Die mit seinem Einverständnis erfolgende Nutzung hat die bereits genannten Anforderungen rechtsgemäßer Technikgestaltung zu beachten.

---

58 Zumindest aber muss regelmäßig ein Überwiegen der Interessen des Betroffenen angenommen werden – so z.B. Gundermann/Probst (Fn. 1), S. 2005.

Die Koalition hat sich vorgenommen, die Modernisierung des Datenschutzrechts weiter voranzutreiben[59]. Für dieses Reformvorhaben hätte ich hinsichtlich der Biometrie zwei Vorschläge:

Erstens wäre es sinnvoll, die Transparenzanforderungen für Biometrieverfahren einheitlich zu regeln. Derzeit fallen nämlich einzelne Biometrieanwendungen unter die Transparenzanforderungen von §§ 6b und 6c BDSG, andere aber nicht. Das ist unbefriedigend. Es wäre im Hinblick auf eine Gleichbehandlung und einen lückenlosen Grundrechtsschutz hilfreich, eine Regelung zu schaffen, die für alle Biometrieanwendungen sicherstellt, dass sie nur unter Mitwirkung des Betroffenen stattfinden dürfen und ihm gegenüber die Erhebung von Daten transparent signalisieren müssen.

Mein zweiter Vorschlag ist, die Zweckbindung von Daten aus Biometrieverfahren strafrechtlich abzustützen. Eine rein technische Sicherung der Zweckbindung wird vermutlich nicht vollständig und ausnahmslos möglich sein. Daher sollte ergänzend – ähnlich wie die Weitergabe von Patientendaten unter Strafe steht – eine unbefugte Weitergabe von Daten aus Biometrieverfahren ebenfalls unter Strafandrohung gestellt werden.

Meine sehr verehrten Damen und Herren, ich bin am Ende meiner Ausführungen zur verfassungs- und datenschutzrechtlichen Bewertung von Biometrieverfahren angelangt und bedanke mich sehr für Ihre Aufmerksamkeit.

59 Koalitionsvertrag vom 11. November 2005, S. 109.

Peter Schaar:

Vielen Dank, lieber Herr Prof. Roßnagel.

Es war eine gute Idee, die Reihenfolge so zu wählen. Die Wissenschaftler haben die verschiedenen Aspekte zusammengeführt, die gesellschaftspolitischen, die technologischen und die rechtlichen. Eben diese Gestaltungsmaxime wird sicher in der Diskussioneine Rolle spielen werden. Wie auch bei den beiden anderen Vorträgen möchte ich Ihnen jetzt noch die Gelegenheit zu einer Kurzintervention oder einer Frage geben.

Dr. Christoph Bruch, Humanistischen Union:

Meine Name ist Christoph Bruch von der Humanistischen Union. Ich habe eine Frage, die sich auf den Komplex bezieht, wie es sich auswirkt, wenn man mit einem Ausweis mit biometrischen Daten reist. Die Bundesregierung schickt ihre Staatsbürger mit den biometrischen Daten auf Reisen. Sie haben ja ausführlich dargelegt, welche für Anforderungen erfüllt sein müssen, um eine fassungskonforme Nutzung dieser neuen Technik zu ermöglichen. Aber als Sie, Herr Prof. Roßnagel, über die Erfüllung dieser Anforderungen bei den internationalen Vereinbarungen sprachen, denen die Bundesregierung in diesem Kontext beigetreten ist, sind Sie in den Konjunktiv gefallen und was Sie nicht kommentiert haben, was ist denn, wenn die internationalen Vertragspartner nicht vertrauenswürdig sind.

Alexander Roßnagel:

Die Grundrechte gelten nur gegenüber der Bundesrepublik Deutschland. Man kann sich in einem anderen Staat nicht auf die deutschen Grundrechte berufen, sondern dort nur auf die Grundrechte, die dort gelten. Wir wissen ja alle, dass das weltweit etwas verschieden ist. Auf was ich hingewiesen habe, ist der Umstand, dass die Verpflichtung der Bundesrepublik Deutschland, für die Grundrechte ihrer Bürger zu sorgen, nicht an der Grenze aufhören kann. Und in den Konjunktiv bin ich deswegen gefallen, weil ich die Anstrengungen der Vertreter der Bundesregierung in den entsprechenden Gremien als Außenstehender, als interessierter Außenstehender, noch nicht als so heftig wahrgenommen habe, wie ich mir das wünschen würde. Man könnte in diesen Gremien vielleicht noch etwas entschiedener für die Grundrechte, die in der Bundesrepublik Deutschland gelten, eintreten. Ich weiß, dass dies

ein schwieriges Terrain ist. Hier geht es um Diplomatie. Deswegen kann man in diesem Zusammenhang auch nicht so knallhart argumentieren, dass ein bestimmtes Verhalten eindeutig ein Rechtsverstoß sei. Es besteht nur eine Sorgepflicht: Man muss sich Sorgen machen, man muss sich darum kümmern. Also, in diesem Fall ist der Maßstab – auch verfassungsrechtlich – ganz klar viel, viel weicher, als wenn sich der Sachverhalt in der Bundesrepublik abspielt.

Peter Schaar

Gibt es weitere Fragen oder Anmerkungen. Ja, Sie haben das Wort.

Constanze Kurz, Humboldt-Universität zu Berlin:

Sie haben mehrfach darauf hingewiesen, dass eine zentrale Speicherung der biometrischen Daten nicht mit den Gesetzen vereinbar ist, vereinbar wäre. Nun befindet sich ja die Verwaltung in einem großen Umbruch und die dezentrale Speicherung wird zunehmend vernetzt. Wäre aus juristischer Sicht eine indizierte Suche über dezentrale Dateien mit einer zentralen Speicherung gleichzustellen?

Alexander Roßnagel

Ja, eindeutig. Es geht um den Effekt, den das für Grundrechte hat und nicht um die technische Ausgestaltung. Wenn der Effekt vernetzter dezentraler Datenbanken für die informationelle Selbstbestimmung der gleiche ist, wie der einer einzigen Datenbank, dann sind beide auch in rechtlicher Hinsicht gleichzusetzen.

Peter Schaar

Gibt es noch eine weitere Frage. Wenn das nicht der Fall ist, danke ich Ihnen. Ich danke Ihnen, Herr Prof. Roßnagel, auch für Ihre Antworten und noch mal für Ihren Vortrag. Wir gehen jetzt ohne weitere Pausen und Unterbrechungen über zu der politischen Debatte.

Podiumsdiskussion

Peter Schaar:

Nach der sehr interessanten wissenschaftlichen Runde, in der Professoren aus unterschiedlichen Fachbereichen das Thema beleuchtet haben, denke ich, dass wir nun eine ebenfalls sehr interessante Diskussion folgen wird. Ich möchte die hier anwesenden Vertreter der Fraktionen des Deutschen Bundestages kurz vorstellen:

Zu meiner Rechten sitzt Herr Dr. Hans Peter Uhl. Er ist Rechtsanwalt und war 20 Jahre in der Kommunalpolitik in München tätig. Das ist ein reicher Schatz an Erfahrungen mit praktischen Verwaltungsproblemen, die sicherlich auch eine Rolle spielen können bei der Diskussion über die Anwendung biometrischer Verfahren in der Verwaltungspraxis. Er ist – wie im übrigen auch die Damen zu meiner Linken - Mitglied im Innenausschuss des Deutschen Bundestags. Er vertritt dort die CDU/CSU-Fraktion. Links neben mir sitzt Frau Gisela Piltz. Sie ist ebenfalls Rechtsanwältin, Innenausschussmitglied und datenschutzpolitische Sprecherin der FDP-Fraktion. Links von ihr sitzt Frau Petra Pau. Sie ist - wie im übrigen ich auch - nicht Juristin. Aber Sie ist Lehrerin und hat seit kurzer Zeit auch ein zusätzliches wichtiges Amt im Bundestag inne. Sie ist nämlich Stellvertretende Präsidentin des Deutschen Bundestages. Sie ist Abgeordnete der Fraktion DIE LINKE. Ebenfalls herzlich Willkommen, Frau Pau. Ganz links außen ist die Vertreterin von BÜNDNIS 90/DIE GRÜNEN, Frau Silke Stokar von Neuforn. Auch Sie ist Innenpolitikerin und von Beruf Groß- und Außenhandelskauffrau. Sie ist im Innenausschuss Obfrau Ihrer Partei.

Meine Damen und Herren, ich denke, dass die in den Vorträgen angesprochenen Fragen auch Sie beschäftigen. Im Zusammenhang mit Ihrer Tätigkeit im Innenausschuss sie zu entsprechenden Fragestellungen sachkundig. Ich möchte mit einer grundsätzlichen Frage anfangen: Sehen Sie eigentlich bei der Einführung biometrischer Merkmale in die ePässe hinsichtlich des Verfahrens der Beschlussfassung die demokratische Legitimation als gegeben an ? Der Prozess wurde auf internationaler Ebene angestoßen. So hat die ICAO, die Internationale Luftfahrtorganisation, eine UN-Behörde, bestimmte Vorgaben gemacht, die zwar rechtlich nicht verbindlich sind, aber einen de-facto-Standard bilden. Die Europäische Union hat am 13. Dezember 2004 durch den Rat die „Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ verabschiedet, die jetzt - auch in

Deutschland – umzusetzen ist. Ist das eigentlich eine ausreichende demokratische Legitimation, die die Einführung biometrischer Daten in Ausweisdokumente erfahren hat ?

Ich würde gerne mit Ihnen, Herr Dr. Uhl, beginnen.

Dr. Hans-Peter Uhl:

Sie haben nach der demokratischen Legitimation des Verfahrens gefragt. Meine Antwort ist: Es gibt viele Formen der demokratischen Legitimation, unterschiedlichste Arten und Ausprägungen. Die intensivste Form der demokratischen Legitimation pflegt die Schweiz. Da wird eine Bürgerbefragung gemacht. Natürlich kann man es so auch machen. Danach gibt es noch 20 weitere Varianten des Themas „demokratische Legitimation". Wenn die demokratisch gewählte Bundesregierung in einem Gremium, das auch demokratischen Ursprungs ist, wie die EU-Kommission oder sonstige Gremien in Brüssel, zu irgend einem Verfahren die Zustimmung gibt, dann ist das Verfahren demokratisch legitimiert. Ob das noch mal mit einem Parlamentsvorbehalt versehen wird, und wie dann dieser Parlamentsvorbehalt abgearbeitet wird - z.B. vor allem dann, wenn das Parlament mehrheitlich nein sagt, die Bundesregierung aber in Brüssel ja gesagt hat -, ist wiederum eine interessante juristische staatsbürgerliche oder sonstige Rechtsfrage. Aber das Verfahren ist demokratisch legitimiert. Sie können dann nicht sagen, dass sei undemokratisch.

Peter Schaar:

Vielen Dank Herr Dr. Uhl. Frau Piltz, wie sehen Sie dies ?

Gisela Piltz:

Herr Schaar, Sie haben gefragt, ob aus meiner Sicht das Verfahren der Einführung biometrischer Merkmale in den Pass ausreichend demokratisch legitimiert ist. Also ich glaube, dass es rechtlich nicht zu beanstanden ist. Aber ich halte es als Parlamentarierin für nicht ausreichend legitimiert. Es hat auf internationaler Ebene eine Vereinbarung gegeben und wurde so im Ministerrat beschlossen. Der damalige Bundes-

innenminister Otto Schily hat das Verfahren in Brüssel durchgesetzt. Er hat darüber hinaus - nicht nur wie auf internationaler Ebene gefordert - ein biometrisches Merkmal, sondern – sag ich mal ganz böse – dort, weil es ihm „Spaß“ gemacht hat, zwei biometrische Merkmale in den Pass hinein verhandelt, ohne dass dies im Europäischen Parlament überhaupt behandelt wurde. Auch das deutsche Parlament ist überhaupt nicht mit dieser wichtigen Frage befasst worden. Und auch wenn ich damals schon in der Opposition gewesen wäre und wahrscheinlich auch wieder verloren hätte, mit dem was ich gewollt hätte, hätte ich doch wenigstens gerne mal über die Angelegenheit diskutiert. Man hätte die Fragen stellen müssen: Ist das sinnvoll ? Machen wir das richtig ? Ist die Aufnahme der Fingerabdruck und die Gesichtserkennung das Richtige oder gibt es noch etwas besseres ? Oder, wer wird mit der technischen Durchführung beauftragt ? Machen wir das mit der Bundesdruckerei oder nicht ? Ja, auch die Frage, ob die Bundesdruckerei den Auftrag bekommt und die Bundesdruckerei alles macht, ohne dass das jemand beeinflussen kann, sowie, dass die Geräte der Bundesdruckerei jetzt überall in Einwohnermeldeämtern stehen, ist am Parlament vorbei entschieden worden. Und ich finde bei einer wichtigen Frage der nationalen Sicherheit gehört so etwas ins Parlament und in den Innenausschuss und nicht nur in von der Bundesregierung beschickte Gremien.

Peter Schaar:

Ich gebe die selbe Frage an Frau Pau.

Petra Pau:

Ja, ich schließe mich da gleich an. Ich denke eher, dass der Bundesinnenminister an dieser Stelle mit Absicht auch das Deutsche Parlament ausgespart hat. Vielleicht hat er dies auch aus einer anderen für ihn und nicht nur für ihn, sondern in dem Fall auch für Josef Fischer schlechten Erfahrung heraus so gemacht. Wir haben im Moment gerade das EUGH-Urteil zur Übermittlung der Fluggastdaten an die USA auf den Tisch bekommen, in dem die rechtliche Grundlage für das Zustandekommen dieses Abkommens beanstandet wurde. Ich erinnere mich noch gut, dass der Deutsche Bundestag quer über die Fraktion die Ablehnung der Übermittlung dieser Fluggastdaten beschlossen hat und damit eigentlich auch unseren Regierungsvertretern einen entsprechenden Verhandlungsauftrag erteilt hat. Dann hat aber Josef Fischer im Ministerrat die Hand dafür gehoben, gegen den eindeutigen Beschluss des Bundestages. Ich denke, eine solche, wenigstens moralische Fessel wollten sie sich nicht anlegen. Und insofern muss ich dem Kollegen Uhl widersprechen: So ganz demo-

kratisch ist es hier nicht zugegangen. Die anderen Dinge hat Frau Piltz schon beschrieben.

Peter Schaar:

Danke schön. Frau Stokar.

Silke Stokar von Neuforn:

Das damals gut gemeinte Verfahren, im Passgesetz einen Gesetzesvorbehalt, d.h. die Beteiligung des Bundestages in wesentlichen Fragen der Biometrieeinführung, zu verankern, ist - ich habe das ja direkt mitbekommen - total daneben gegangen. Das war ein gut gemeinter Versuch der Grünen-Fraktion zu sagen, wir wollen an dem Verfahren „Einführung biometrischer Merkmale“ sowohl innerhalb der Koalition als auch als Abgeordnete im Parlament in irgend einer Weise beteiligt sein. Die Punkte, die damals in das Passgesetz und das Personalausweisgesetz aufgenommen worden sind, sind Punkte gewesen, die hier ebenfalls in der Debatte genannt worden, also: eine enge Zweckbindung, kein Ausbau einer Zentraldatei und natürlich auch Einfluss auf die Auswahl der biometrischen Merkmale. Was ist passiert? Das ist hier ja ganz gut geschrieben worden. Und natürlich ist es rechtlich nicht zu beanstanden. Ich halte das allerdings schon fast für eine bewusste Ausgrenzung des Parlamentes in einem geheim gehaltenen Verfahren. Wir haben ja noch nicht mal die Protokolle der Verhandlung bekommen. Hat etwa die Bundesregierung auf EU-Ebene den Druck massiv erhöht, um sehr schnell auf der Grundlage einer EU-Verordnung nationales Recht zu umgehen ? Weder der Deutsche Bundestag, noch das Europäische Parlament wurden beteiligt. Es gab niemals eine parlamentarische Abstimmung zur Einführung biometrischer Merkmale in den Pass. Und sogar die Angleichung des nationalen Rechtes, die meiner Meinung nach rechtswidrig war, wurde auf Grund einer Verordnung vorgenommen. Bis heute hat man das nationale Recht noch nicht angeglichen. Ein Machtmittel, das wir haben wollten, war der Parlamentsvorbehalt. Aber wir haben kein Parlamentsbeteiligungsgesetz. Auch das ist den Neuwahlen zum Opfer gefallen. Uns fehlt natürlich in diesem ganzen Bereich die europäische Verfassung und damit auch die stärkeren Möglichkeiten der Einbindung des europäischen Parlamentes. Insgesamt wurde das Ganze aus machtpolitischen Gründen vom Innenminister durchgezogen, verordnet und ist leider auch ohne großen Protest der Bevölkerung Realität im Bereich des Reisepasses geworden. Für mich war das ein Lehrstück in „wie schalte ich auch in einer Demokratie Abgeordnete und Parlament von der politischen Gestaltung aus“.

Peter Schaar:

Vielen Dank.

Ein besonders wichtiger Aspekt ist die Frage des zweiten biometrischen Merkmals im Pass, den Fingerabdruck. Wir haben in der Vorgabe der ICAO keine entsprechende Verpflichtung für die Staaten. In der EU ist es über die bereits genannte Verordnung eine Verpflichtung geworden. Die Einführung war für alle Beobachter und Beteiligte völlig überraschend - jedenfalls als verpflichtendes Merkmal. Es ist im Entwurf der entsprechenden Verordnung nicht so vorgesehen gewesen, sondern dort hieß es, man könne - sozusagen optional - auch ein zweites Merkmal verwenden. Und als dann der Beschluss bekannt gegeben wurde, wurde gesagt, naja, also wir haben uns doch so entschieden, dass es rein muss. Das ist eine politische Entscheidung der beteiligten Minister gewesen. Der damalige Innenminister hat das auch wohl ganz persönlich zu seiner Sache gemacht und dort durchgeboxt, im wahrsten Sinne des Wortes. Er ist aber auch nicht auf großen Widerstand gestoßen. Jetzt stellt sich ja heraus, dass außerhalb Europas niemand, soweit ich weiß, jedenfalls kein relevanter Staat oder eine Staatengemeinschaft dieser Linie folgt. Die Pässe sind an den Außengrenzen zu kontrollieren und man kann auch mit Personalausweisen als EU-Bürger in die Europäische Union einreisen. Man muss den Pass nicht immer an der Grenze vorzeigen. Und jetzt stellt sich mir natürlich die Frage, sollte nicht darauf hingewirkt werden, diese Entscheidung noch einmal kritisch zu überprüfen, zumal ja bisher noch nicht damit begonnen wurde, dieses zweite Merkmal in den Pass einzuführen. Wir haben aus den Vorträgen auch gelernt, insbesondere aus dem was Herr Prof. Busch gesagt hat, dass z.B. die Frage, wie das Datum dort gespeichert werden soll, d.h. ob es als Vollbild oder das Template gespeichert werden soll, durchaus in der wissenschaftlichen Diskussion heute anders beurteilt wird als es die Innenminister damals beurteilen konnten, weil sie seinerzeit diese Informationen gar nicht hatten. Die Frage ist, sollte auf die Einführung verzichtet oder sollte der Fingerabdruck als zweites biometrische Merkmal gleichwohl eingeführt werden und/oder wäre es auch denkbar, dass man sich hier auch auf europäischer Ebene für ein Moratorium einsetzt ? Die Bundesregierung könnte das ja durchaus machen und auf die neueren Erkenntnisse verweisen. Möchte dazu jemand etwas sagen

Herr Dr. Uhl.

Dr. Hans-Peter Uhl:

Als ehemaliger Münchner Kreisverwaltungsreferent komme ich von der Sicherheits- und nicht von der Datenschutzseite her und bin als sicherheits- und jetzt innenpolitischer Sprecher der CDU/CSU Fraktion zunächst Sicherheitspolitiker. Als solcher hat man ein Interesse an möglichst vielen Daten und an möglichst viel Datenabgleich, weil damit kann man Sicherheit produzieren. Das man dabei aber Grenzen einhalten muss, insbesondere die des Grundgesetzes ist mir eine Selbstverständlichkeit. Von der Datenschutzseite her, wäre ich durchaus gerne in Richtung Grenzziehung sensibilisiert worden. Ich bin offen für ein Gespräch und will mich mit den ganzen Bedenken auch auseinandersetzen. Aber ich halte es für einen ganz natürlichen politischen Prozess, dass man bei den verschiedenen biometrischen Daten versucht die zu nehmen, die am tauglichsten sind, für das was wir vorhaben, z.B. Grenzkontrolle, Ein- und Ausreise oder sonstige Kontrollen. Wenn die Gesichtsfelderkennung das eine biometrische Datum ist, die Fingerabdrücke das andere, die Iriserkennung in der Anwendbarkeit Probleme macht, dann muss man sich halt irgendwann für das eine oder das andere biometrische Datum entscheiden. Da wir die Gesichtsfelderkennung jetzt schon in Form des Passphotos verwenden, ist dies gar nichts neues. Das Passphoto wird jetzt nur digital erfasst. Also zunächst mal sehe ich hier keinerlei Grundrechtseingriff. Wenn ich ein Passphoto, dass ich jetzt schon im Pass habe, digital erfasse, dann ist es halt digital erfasst, was soll´s.

Wenn man sich auf EU-Ebene auf diese zwei biometrischen Merkmale geeinigt hat, sollte man zunächst mal dankbar sein, dass man sich geeinigt hat, auf was auch immer. Es sei denn, Sie sagen das Ergebnis ist unerträglich. Dann müsste man es noch mal überprüfen. Aber bei mir ist bisher nicht angekommen, dass das Ergebnis unerträglich sei. Vielleicht kann man darauf noch in den Arbeiten eingehen, die mir zugehen.

Peter Schaar:

Wir werden unser möglichstes tun, Sie zu sensibilisieren. Frau Piltz bitte.

Gisela Piltz:

Wissen Sie Herr Uhl, dass wir Sie als Opposition der letzten Jahre nicht sensibilisiert hätten, kann man uns wirklich nicht vorwerfen. Aber ich kann mich erinnern, dass ich vor zweieinhalb Jahren die erste Anfrage zur RFID im Deutschen Bundes-

tag gestellt habe, die überhaupt gestellt worden ist. Und die damalige Bundesregierung äußerte, ihr seien keine Sicherheitsprobleme bekannt und sie sähe auch keine. Daraufhin habe ich befunden, dass sich mit dem Thema dann noch niemand beschäftigt haben kann. Wenn man anfängt, sich mit dem Thema zu beschäftigen, dann weiß man, dass es Sicherheitsprobleme gibt. Es stellen sich die Fragen, wer kann das auslesen, in welcher Entfernung kann dass ausgelesen werden, wie sieht es mit unbefugtem Zugriff aus und und und ? Das ist eine völlig neue Qualität, die aus unserer Sicht mit diesen RFID-Chips in das Thema Datenschutz kommt. Spätestens mit dem Antrag der FDP-Fraktion vom 8. März 2006 in dem auf die Sicherheitslücken bei biometrischen Pässen hingewiesen und gefordert wird, sie zu beseitigen, haben wir versucht, Sie für das Thema zu sensibilisieren. Wir fordern den Deutschen Bundestag auf, zu beschließen, die Ausstellung dieser Reisepässe so lange auszusetzen, bis diese Sicherheitslücken beseitigt sind. Wenn man gewollt hätte, hätte man für dieses Thema sensibilisiert sein können. Wir sind es jedenfalls und ...

Dr. Hans-Peter Uhl:

Sind die Lücken nur behauptet oder sind die bewiesen ?

Gisela Piltz:

Soweit ich das beurteilen kann, sind sie durch das Bundesamt für Sicherheit in der Informationstechnik bewiesen. Auch in den Niederlanden hat es große Probleme mit dem neuen Pass gegeben. Die FDP-Fraktion sieht hinsichtlich des ePasses große Probleme. Und wir halten es für ein eben so großes Problem, so genannte ePersonalausweise auch noch einzuführen.

Peter Schaar:

Das Thema ePersonalausweis würde ich gerne noch mal getrennt behandeln. Vielleicht können Sie, Frau Pau, noch etwas zum zweiten biometrischen Merkmal oder der Moratoriumsfrage sagen.

Petra Pau:

Sicherlich wäre ein Moratorium erstmal das Vernünftigste. Vielleicht kann man auch nachträglich klüger werden. Und ich glaube, es steht uns auch ganz gut an, wenn wir auch als Politikerin und Politiker - ganz egal, ob jemand dafür oder dagegen war - gestehen könnten, dass man neuen Erkenntnissen aufgeschlossen gegenübersteht und einmal getroffene Entscheidungen überprüft. Aber ich möchte einen Widerspruch anmelden. Wir reden jetzt im Moment über das Thema Biometrie und biometrische Merkmale. Herr Uhl hat aber eben schon ein bemerkenswertes Bekenntnis abgelegt, als Sicherheitsexperte. Er sagte, möglichst viele Daten schaffen Sicherheit. Und genau das ist mein Problem. Wir reden eben nicht isoliert über ein oder zwei biometrische Merkmale oder über dies oder jenes. Ich war gerade mit einer Delegation des Innenausschusses in den USA. Dort waren Vertreter aller Fraktionen anwesend und wir haben fraktionsübergreifend, überall wo wir waren - in Sicherheitsbehörden, im Parlament, in Ministerien - die Frage gestellt, inwieweit denn dieses Zusammenführen von Daten, welches dort inzwischen ganz andere Ausmaße angenommen hat, in irgendeiner Weise mehr Sicherheit geschaffen hat. Das konnte man uns nicht nachweisen. Aber von Institution zu Institution wurde die Liste der Probleme länger. Probleme hinsichtlich der Verwechslung, der unrechtmäßigen Aufnahme auf Fahndungslisten, weil plötzlich ein oder zwei Merkmale zusammenkamen, die einen Verdacht begründeten. Diese Liste wurde länger wegen der Fehlerquote gerade durch das ungezügelte Sammeln und Zusammenführen von Daten. Und dann kam noch hinzu, inwieweit werden bestimmte Daten durch Private für die entsprechenden Sicherheitsinstitutionen erhoben und bei der Gelegenheit dann an Dritte für andere Zwecke, auch für kommerzielle Zwecke, weitergegeben. Ich denke, man muss sich diesen Gefahren erstens stellen, und dann die Frage nach der Sinnhaftigkeit der Erhebung dieser Daten zur Herstellung von Sicherheit noch mal neu beantworten. Diese Debatte kommt mir viel zu kurz.

Peter Schaar:

Frau Stokar.

Silke Stokar von Neuforn:

Ich möchte auf das Sicherheitsrisiko noch einmal hinweisen. Wenn wir staatlich verpflichtet werden, unseren Fingerabdruck abzugeben, geben wir unseren persönlichen Fingerabdruck in die Hand des Staates. Der Staat bringt diesen in einen Chip

ein. Der holländische Pass wurde bereits geknackt. Also soviel zur Sicherheit. Und deshalb habe ich natürlich die Befürchtung, dass die Frage von Identitätsdiebstählen auf uns zukommen wird. Zu Recht wurde auf die Kriminalstatistik hingewiesen, wonach wir, auch aus dem internationalen Bereich, ganz neue Kriminalitätsformen bekommen. Und dazu gehört dann natürlich auch, dass im Bereich der Organisierten Kriminalität ein Interesse daran besteht, viele Fingerabdrücke zu stehlen, die möglicherweise dann auch noch Klarnamen zuzuordnen sind. Ich sehe hier also ein ganz, ganz hohes Risiko. Die andere Gefahr, die ich sehe ist, dass ich nicht möchte, wenn ich ins Ausland reise, dass in Staaten ohne Datenschutzstandard, insbesondere in Staaten, die teilweise ja überhaupt keine staatlichen Garantien abgeben können, bei jeder Einreise bei jeder x-beliebigen Grenzkontrolle mein Fingerabdruck aus meinem Pass herausgenommen wird. Ich verliere dann jede Möglichkeit, zu erfahren, was geschieht eigentlich weiter mit diesem Fingerabdruck. Die Risiken sind meiner Meinung nach viel höher als der versprochene Sicherheitsgewinn. So ist dieses ganze Theater mit RFID- Chips zur Fußball-WM ein einziges Desaster. Es ist die größte Lachnummer, die je produziert worden ist. Die Identitäten in den Stadien werden nicht festgestellt, weil das ganze System gar nicht funktioniert und die Aggressionen in den Warteschlangen viel zu groß werden. Das führt jetzt dazu, dass wir mehr Schwarzmarkt haben und dass mehr Leute mit ungeklärten Identitäten in den Stadien sind, als wenn wir ein herkömmliches Verfahren hatten, bei denen ein Ordner die Personen ansieht und nachsieht, ob die Karte gültig ist und diese anschließend zerreißt. Also so viel zur Sicherheitsversprechung durch neue Technologien.

Peter Schaar:

Die Frage, die sich daran natürlich anschließt ist: Inwieweit reichen diese Verwendungsbeschränkungen für die Pässe aus, die wir bisher haben? Wir haben ja in den Gesetzen bestimmte Begrenzungen der Lesebefugnisse auf staatliche Stellen für bestimmte Zwecke. Wir haben auch noch die Grundsatzentscheidung des Deutschen Bundestages gegen zentrale Dateien aus den Gründen, die Herr Prof. Roßnagel auf Rückfrage genannt hat. Auch ist das mit den zentralen Dateien vielleicht ein bisschen unglücklich formuliert. Aber es war natürlich der Wille des Gesetzgebers, mit dieser Formulierung externe Dateien zu verhindern. Das war ziemlich klar und eine Speicherung sollte bloß in den Dokumenten selbst vorgenommen werden. Soll es dabei bleiben oder sollen die biometrischen Merkmale auch in Datenbanken wandern? Sollen z.B. Private die Möglichkeit erhalten, auf diese Daten zuzugreifen? Wie sehen Sie das?

Herr Dr. Uhl.

Dr. Hans-Peter Uhl:

Eine Bemerkung muss ich noch schnell loswerden. Wenn Sie Bedenken haben bei der Einreise in irgendwelche Staaten, weil Sie dann sich nicht dem dortigen Grenzregime unterwerfen wollen. Da kann ich nur sagen, dann bleiben Sie halt zu Hause.

Silke Stokar von Neuforn:

Ich nehme aber meine Reisefreiheit wahr. Das ist ein Grundrecht.

Dr. Hans-Peter Uhl:

Wenn Sie mit den Grenzkontrollen in Angola nicht zurecht kommen sollten, oder in Kuba oder in Albanien, dann müssen Sie eben in ein anderes Land reisen. Das wollte ich damit sagen.

Wir sind doch hier in Deutschland. Wir können doch nur die deutschen Gesetze beeinflussen, doch nicht den Grenzbeamten in Angola oder sonstwo.

Wenn holländische Jugendliche irgendwas geknackt haben, dann muss man halt unsere Fachleute befragen, ob bei der Technologie, die wir anzuwenden gedenken, deutsche oder andere Jugendliche das auch knacken können. Und wenn unsere Fachleute ja sagen, dann sollten wir das lieber lassen. Und wenn sie sagen nein, dann ist es doch gut so.

Aber Sie haben noch eine ganz andere Frage gestellt, Herr Schaar. Die Frage ist für mich erstmal ganz banal. In einem Staat gibt es ein Staatsgebiet. Auf dem lebt ein Staatsvolk und es gibt sich eine Staatsgewalt. Das sind die ehernen Prinzipien jedes Staats. Also muss doch eigentlich jeder Staat ein Interesse daran haben, zu wissen, wie groß das Staatsvolk ist. Er muss wissen, wer ist ein Deutscher und hat deswegen einen deutschen Personalausweis. Und dann wird die Liste angelegt, in der sie alle drinstehen. Diese Liste der Deutschen haben wir nicht. Da frage ich mich, was soll das eigentlich. Ich bin noch nicht bei den biometrischen Daten und zugleich gar nicht bei der Verwendung derselben. Ich bin noch bei der Liste der Deutschen. Ich

will wissen, wie viel haben wir von der Sorte. Dann haben wir Namen, Vorname, Nachname, Adresse, Geburtsdatum und damit auch einen Zugang zu dem jeweiligen lokalen Melderegister, wo das biometrische Datum in Form des Foto drin ist, noch nicht das digitalisierte. Und jetzt sagen Sie, wenn Sie den nächsten Schritt gehen würden, dieses biometrisch zu erfassen, nicht nur lokal, sondern zusammenzufassen in einem zentralen Speicher, wäre das verfassungswidrig. Dieser Gedanke erschließt sich mir noch nicht. Ich rede zunächst noch nicht von der Verwendung der Daten, sondern nur von deren Erfassung. Dass natürlich auch Missbrauch getrieben werden kann, dass die Daten in falsche Hände kommen können, dass auch ein Zugriff möglich ist, der dann vielleicht wiederum rechtswidrig ist, das ist eine ganz andere Frage. Aber die blanke Verwendung, die blanke Zusammenfassung in einem zentralen oder vernetzt dezentralen Speicher - ich verstehe nicht, warum das verfassungswidrig sein soll. Weil das ein Eingriff in die Selbstbestimmung des Einzelnen wäre ?

Peter Schaar:

Bisher steht im Passgesetz genauso wie Personalausweisgesetz, dass es keine zentralen Dateien mit biometrischen Daten geben soll. Die Frage ist doch, soll es bei der Beschlussfassung des Deutschen Bundestages bleiben oder sollte man die Dateien letztlich doch für Sicherheitszwecke öffnen?

Dr. Hans-Peter Uhl:

Wenn man mir überzeugend darlegt, dass eine zentrale Zusammenlegung verfassungswidrig wäre, nicht unnütz oder ungeeignet oder unverhältnismäßig, sondern sogar verfassungswidrig, dann dürfen wir es nicht machen. Aber das hat mir noch niemand erklären können.

Peter Schaar:

Wenn es nicht verfassungswidrig wäre, sollte man es machen oder nicht ?

Dr. Hans-Peter Uhl:

Dann schauen wir mal, ob das nützlich ist. Ich könnte mir vorstellen, dass es nützlich ist. Und zwar aus folgendem Aspekt: Max Meier aus München holt sich einen

Personalausweis in München, und erhält ihn mit seinen biometrischen Daten, Fingerabdrücken, Lichtbild. Dann zieht er nach Düsseldorf um und will einen Zweitpass oder zweiten Personalausweis. Aber diesmal nicht auf Max Meier, sondern auf Manfred Müller ausgestellt. Gehen wir weiter davon aus, dass ihm dies gelingt und in Düsseldorf wird ihm vom Einwohnermeldeamt ein Personalausweis mit den gleichen biometrischen Daten - logischerweise auf Manfred Müller - ausgestellt. Dann haben wir zwei Personalausweise mit den identischen biometrischen Daten. D.h. wo immer diese Person auftritt, legt er einen Ausweis vor mit identischen Daten, aber ausgestellt auf unterschiedliche Namen. Die Verifizierung zeigt, es ist Manfred Müller aus Düsseldorf bzw. Max Meier aus München. Ein zentrales Speichern würde dies verhindern, weil es sofort zeigen würde, die Daten, die kennen wir schon. Diese Person ist aus München und nicht aus Düsseldorf.

Peter Schaar:

Ich möchte die Damen um ihre Meinung bitten. Ich denke, dass wir jetzt noch eine Runde hier machen, dass wir dann Ihnen auch die Gelegenheit geben, aus dem Publikum Fragen zu stellen.

Gisela Piltz:

Auf Ihre Frage eine ganz klare Antwort: ich möchte keine zentrale Speicherung und ehrlich gesagt finde ich es auch gar nicht so wichtig, ob das verfassungswidrig ist oder nicht. Ich habe dafür vielmehr einen politischen Grund. Ich finde, dass man nicht alles tun muss, was man tun kann. Und ich warte erst recht nicht darauf, ob mir das Verfassungsgericht sagt, dass meine Politik schlecht ist oder nicht. Ich habe einfach einen eigenen inneren Kompass was den Datenschutz angeht und dieser sagt mir, das muss nicht sein. Es ist für mich auch nicht nur eine Frage von Erfassung und Verwendung. Ich habe nämlich in der Zeit, in der ich mich mit Datenschutz beschäftige, eines gelernt: Alles was erfasst wird, wird früher oder später auch verwendet. Wie oft haben wir es in der Politik schon erlebt. Dann heißt es, wir machen das nur für die Terrorismusbekämpfung. Ich sage nur Kontenabfrage. Heute wird das bei jedem von Ihnen gemacht. Ein anderes Beispiel ist die Autobahn-Maut, deren Daten nur für die Erhebung der Maut dienen sollen. Jetzt stellt die CDU-Fraktion den Antrag, dass diese Daten auch für die Verfolgung von ganz schweren Straftaten herangezogen werden sollen. Ich habe gelernt, Sie müssen den ersten Schritt verhindern, weil sonst wird alles verwendet, was da ist - früher oder später.

Deshalb ist mein Bestreben immer zu sagen, ich will gar nicht erst, dass es erfasst wird. Es kann dann in einem weiteren Schritt nicht verwendet werden.

Auch heute können Sie schon mit einer neuen oder falschen Identität ausgestattet werden - das ist gar nicht so schwer wie ich mal geglaubt habe. Ich habe das mir einmal erklären lassen, wie man sich eine neue Identität, einen neuen Personalausweis besorgt. Wenn es darum gehen würde, dass wir das verhindern, dann müssen wir heute schon dies erschweren und nicht deswegen die Daten aller Bürger in eine Datenbank packen.

Peter Schaar:

Frau Pau, möchten Sie auch etwas dazu zu sagen.

Petra Pau:

Das was die Frau Piltz gesagt hat, unterschreibe ich sofort. Auch den Grundsatz, nicht alles, was technisch möglich und was denkbar ist in Ausnutzung von technischen Möglichkeiten, müssen wir umsetzen. Ich denke, unser Ausgangspunkt muss ein anderer sein. Nämlich tatsächlich das Selbstbestimmungsrecht von vorneherein zu sichern und dann zu schauen, was ist notwendig, um den entsprechenden Erfordernissen nachzukommen. Aber ich halte diese Erfassung - also den Schritt vor der zentralen Erfassung, den Herr Uhl beschrieben hat - schon nicht für sinnvoll. Dann kommen wir nämlich relativ bald tatsächlich zu dem universellen Chip, den jeder mit sich herumträgt. Wir haben in dieser Woche gerade wieder eine Debatte zum Thema Gesundheitskarte und was alles auf diesem Chip gespeichert werden soll. Hier stellt sich wieder die Frage der Auslesbarkeit des Chips und des Zusammenführens von Daten, die nicht zusammengehören.

Peter Schaar:

Frau Stokar.

Silke Stokar von Neuforn:

Ich würde gerne das Dilemma der Politik beschreiben. Wir haben damals versucht, im Personalausweisgesetz und Passgesetz Hürden einzubauen und Grenzen zu ziehen. Das Ergebnis habe ich ja geschildert. Ich glaube, die Debatte über den EU-Pass ist mehr oder weniger gelaufen. Es gibt eine Europäische Verordnung und diese ist unmittelbar bindendes nationales Recht, ganz gleich, ob der Bundestag sich damit befasst hat oder nicht. Das ist Europa und da können wir nicht viel machen. Ich stehe konkret vor einem Problem: Ich möchte eigentlich keinen biometrischen Personalausweis, in dem meine Fingerabdrücke gespeichert werden, der eine elektronische Signaturfunktion hat und der möglicherweise auch mit dem Führerschein gekoppelt wird. Andererseits sehe ich die globale Entwicklung. Estland hat genau dieses verpflichtend für alle Bürger eingeführt. Der andere berühmte Staat ist Bahrain, also ein arabischer Staat. Ich muss mich also entscheiden und das müssen wir das als Opposition sehr schnell tun - auch, ob wir den Fachverstand dieses heutigen Symposiums nutzen wollen, um parlamentarisch in das Verfahren zum Personalausweisgesetz einzugreifen. Ein Entwurf ist in Bearbeitung der Großen Koalition. Schnell entscheiden müssen wir auch, ob wir hier Änderungsanträge entwickeln und so das Schlimmste verhindern und damit den biometrischen Personalausweis mitgestalten oder ob wir als Opposition sagen, wir wollen das nicht. Wenn wir nicht schnell entscheiden - das Ergebnis kenne ich aus praktischer Erfahrung - führt dies dazu, dass - ohne dass unsere detaillierten Gegenargumente überhaupt in der parlamentarischen Debatte mit aufgenommen werden - die Innenminister unter sich ausmachen, wie der zukünftige biometrische Personalausweis in Deutschland aussieht. Dass er in irgendeiner Form kommen wird, davon bin ich überzeugt. Deshalb plädiere ich dafür, dass wir die Vorschläge machen. Ich möchte z.B. keine hoheitlichen und private Funktionen, also keine Kopplung mit einer Signatur. Aber wir sollten in die Detaildebatte einsteigen und anfangen, Paragraph für Paragraph zu entwickeln. Die Entscheidung zum elektronischen Pass und zum elektronischen Personalausweis ist in meiner Fraktion noch nicht entgültig gefallen. Wenn wir zu Herrn Uhl sagen, wir wollen das Ding nicht, wird er uns sagen, dass ist uns völlig egal, die Große Koalition wird ihn machen. Dann können wir das beklagen oder wir fangen an, eigene konkrete Vorschläge zu machen, unter welchen gesetzlichen Bedingungen wir das mittragen würden. Das ist eine der spannenden Debatten, die wir im Herbst sehr schnell führen müssen.

Peter Schaar:

Herr Dr. Uhl, ehe ich Ihnen das Wort gebe, möchte ich da direkt anknüpfen auch. Ich möchte Ihnen eigentlich nicht die Frage stellen, sind Sie für den Biometrie gestützten Personalausweis. Dies wird wahrscheinlich relativ schnell mit ja beantwortet. Sondern ich möchte Sie nach dem Prozedere der Entscheidung fragen, die da dann zu treffen ist. Wir sind ja in einer anderen Situation als bei den Pässen. Bei den Pässen gab es keine oder kaum eine Interventionsmöglichkeit, nachdem auf europäischer Ebene der Zug abgefahren war. Würden Sie sich denn dafür einsetzen, dass jetzt, wenn wir über die Einführung biometriegestützter Personalausweise sprechen, alles gründlicher vorbereitet wird. Und dass dann auch eine breite - auch durch die Bundesregierung organisierte - öffentliche Debatte kommt?

Dr. Hans-Peter Uhl:

Gern, denn natürlich muss man so was Grundsätzliches gründlich bearbeiten. Das ist mir vollkommen klar und ich möchte Bedenken ernst nehmen, insbesondere wenn es heißt, derartige Ausweisdokumente kann man knacken, damit kann man Missbrauch betreiben. Man muss ein Gesetz gründlich vorbereiten vorbereiten. Und möchte auch das Gesetze nachgebessert werden. Z.B. dürfen nach dem Autobahn-Mautgesetz die Maut-Daten außer zu Maut-Zwecken nicht verwendet werden. Das war so nachgebessert worden durch eine Altparteienkoalition, vermutlich durch Sie, Herr Schaar, ausgelöst. Ich habe den Koalitionsparteien gesagt, das muss korrigiert werden. Ich sage auch warum: Der Zufall will es, dass in meinem Wahlkreis in München das Ende einer Schleusungsfahrt mit einem LKW aus Griechenland war, der u.a. mit Irakis in der Sommerhitze vor 2 Jahren über Italien nach München führte. Dieser Schleuser hat beim Öffnen des LKWs in München festgestellt, dass ein 21jähriger Iraki an Hitze in dem Lastwagen ums Leben gekommen. Der Schleuser hat den toten Körper einfach weggeworfen. Weil eine Kamera das ganze aufgenommen hatte, wusste man zufällig, es handelt sich um einen blauen LKW von dem und dem Typ. Die Polizei, die eine Fahndung nach dem Schleuser ausgelöst hatte, sagt, wenn wir die Maut-Daten von diesem Autobahnabschnitt in München haben dürften, könnten wir sofort feststellen, wer der Halter ist und könnten diesen Schleuserkreis aufbrechen. Dann stellt sich mit dem Blick ins Gesetz heraus, das geht nur, wenn man den vorher den Schleuser befragt, ob man die Maut-Daten für Fahndungszwecke erheben darf. Und da hört der Spaß auf. Ich möchte, dass so widerwärtige eiskalte Menschenhändler, die bereit sind, Menschenleben zu opfern, das Handwerk gelegt wird. Es kann nicht sein, dass das Mautgesetz dies verhindert. Das kann nicht sein. In diesen Fällen muss man das im Gesetz eben ändern. Schluss aus.

Das heißt aber noch lange nicht zu jedem Bußgeldbescheid Maut-Daten verwenden darf. Soweit soll es natürlich nicht gehen. Es muss sich vielmehr um schwerste Verbrechen handeln und dann will ich die Daten haben.

Peter Schaar:

Lassen Sie mich hier erstmal einen vorläufigen Punkt machen und zur Publikumsfragerunde kommen.

Publikumsfragerunde

Peter Schaar:

Ich möchte jetzt Ihnen noch mal die Gelegenheit geben, zu fragen oder Stellung zu nehmen. Bitte sagen Sie auch Ihren Namen, damit wir das dann richtig in dem Tagungsband vermerken können.

Jan Krissler, Chaos Computer Club Berlin:

Ich wollte noch kurz auf die Stellungnahme von Ihnen eingehen, dass die Passbilder in dem neuen ePass die gleichen sind wie im alten. Das ist natürlich totaler Blödsinn, weil auf dem neuen Pass sind sie in Frontalansicht und nicht im Halbprofil. Das mag auf den ersten Blick kein Problem sein. Aber wenn man sieht, dass für die Grenzbeamten bei der manuellen Kontrolle der Passbilder die Ohrform ein sehr wichtiges Merkmal war, dann wird auch klar, dass das fehlende Ohr in einem Frontalbild die Sicherheit verringert. Und zweitens Ihr Max-Meier-Beispiel: Bei einer Falschakzeptanzrate von 0,1 %, was bei Biometrie als derzeit normaler Prozentsatz angesehen wird, trifft das auf 80.000 Bürger in Deutschland zu; 80.000 potentielle Kriminelle.

Peter Schaar:

Wir sammeln jetzt hier erst noch mal. Gehen Sie dann auch bitte zum Mikrofon. Und danach gibt es noch mal die Gelegenheit, darauf abschließend im einzelnen einzugehen.

Prof. Alexander Roßnagel:

Herr Dr. Uhl, Sie hatten mich gefragt, warum eine zentrale Speicherung von Biometriedaten verfassungswidrig sein kann. Das will ich in aller Kürze versuchen zu beantworten.

Es ist ein Eingriff in das informationelle Selbstbestimmungsrecht. Dass es bisher auf gesetzlicher Grundlage schon das Passbild gibt, verhindert nicht die Feststellung, dass eine digitale Speicherung dieses Bildes ganz andere Auswertungsmöglichkeiten eröffnet und dass dies noch ein weiterer, tiefer gehender Eingriff in die informationelle Selbstbestimmung ist. Dieser zusätzliche Eingriff ist nur zulässig, wenn er verhältnismäßig ist, d.h. wenn er geeignet, erforderlich und zumutbar ist. Hier gibt es Zweifel an der Erforderlichkeit. Bisher haben andere Mittel ausgereicht, um zu verhindern, dass mehrere Pässe an Personen ausgegeben wurden. Das deutsche Passwesen hat mit den konventionellen Mitteln, die man bisher hatte, eine sehr hohe Zuverlässigkeit erreicht, so dass sich die Frage stellt, ob diese Verfahren nicht auch geeignet sind und dabei aber weniger Grundrechtseingriffe mit sich bringen. Und der letzte Punkt ist, der Eingriff muss zumutbar sein, objektiv zumutbar – bezogen auf das Ziel, das man damit verfolgt. Würde man nur das Ziel verfolgen, die Vergabe von Pässen noch sicherer zu machen, dann ist das kein Ziel, das rechtfertigt, biometrische Daten aller Bundesbürger an zentraler Stelle zu speichern und ihre Grundrechte damit einem sehr, sehr hohen Missbrauchsrisiko auszusetzen. Hier besteht einmal das Missbrauchsrisiko, dass irgendwelche Unberechtigten auf die Daten zugreifen können – da könnte der Vorredner vom Chaos-Computer-Club sicher das eine oder andere erzählen, was da möglich ist. Und das zweite – in meinen Augen viel größere – Risiko ist das der Zweckentfremdung dieser Daten. Dieses große Risiko für alle unbescholtenen Bundesbürger ist für das Ziel, das Sie damit verfolgen, unzumutbar. Ich vermute, dass mir das Bundesverfassungsgericht an dieser Stelle Recht gibt. Berücksichtigen Sie bitte das Urteil zur DNA-Speicherung von Straffälligen. Bereits für diese Personen wurden Grenzen gezogen und um so mehr sind diese Grenzen zu ziehen gegenüber unbescholtenen deutschen Bürgern, die nicht den geringsten Anlass gegeben haben, ihre Biometriedaten in so einer zentralen Datenbank zu speichern und dann zusätzlichen Risiken auszusetzen.

Peter Schaar:

So, es gibt noch eine Frage, die ich aus Zeitgründen noch zulassen kann.

Norbert Warga, Datenschutzbeauftragter Bundesvorstand ver.di.

Ergänzend frage ich mit dem Focus auf dass, was in den Betrieben und Verwaltungen in dem Zusammenhang passiert. Nämlich, in Kenntnis dessen, dass in der Gesundheitskarte das Verfahren derart gewählt wird, dass Teil der Daten in der Karte selber gespeichert werden. In anderen Verfahren, wie z.B. beim Job-Card-Verfahren

Daten aus Beschäftigungsverhältnissen oder bei Lohnersatzfunktionen an einer zentralen Speicherstelle gespeichert werden. Wir darüber hinaus vielfältige Datenerfassungen haben, d.h., wir kommen zu einer Mischung, wo für die Vielzahl der Bevölkerung, diejenigen, die nämlich entweder Einkommen aus einer Tätigkeit beziehen oder Lohnersatzleistungen beziehen, Daten umfangreich verwaltet und gespeichert werden. Wenn ich jetzt die Frage der biometrischen Nutzung dabei sehe und den Hinweis vorhin im Vortrag bezüglich der Mitbestimmungsrechte wahrgenommen habe Die Menschen sind nicht allein gelassen sondern werden durch Betriebsräte vertreten, die in der Frage der biometrischen Nutzung das Direktionsrecht der Arbeitgeber beschränken. Dann sehe ich dies insbesondere für den öffentlichen Dienst eigentlich nicht und hier finde ich, steht der Gesetzgeber auch in besonderer Verantwortung. Zur Ankündigung der Novellierung des Bundespersonalvertretungsgesetzes, marschieren die Länder vorne vor. Gerade z.Zt. ihr Heimatland Bayern, das insbesondere in den entscheidenden Beteilungsrechten, nämlich Ordnung in der Dienststelle und Verhalten der Angehörigen der Dienststelle, bzw. Leistungs- und Verhaltenskontrolle, die Mitbestimmungs- und Beteiligungsrechte auf Null zurückführt. Von daher ist die Frage, Persönlichkeitsrecht sowohl im Gesetzgebungsverfahren bezüglich der Biometrie als auch in den Randbereichen der Wirtschaft und öffentlichen Verwaltung, im Zusammenhang zu sehen und es wäre begrüßenswert, wenn die Persönlichkeitsrechte auch von Beschäftigten dabei nicht völlig untern Tisch fallen.

Nur eine persönliche Bemerkung: Ich dachte immer, Sigi Zimmerschmid wäre ein Kabarettist. Ich wusste nicht Herr Dr. Uhl, dass Sie ihm die Steilvorlagen liefern, so nach dem Motto, Kopf ab und dann Rua is.

Peter Schaar:

Vielen Dank. Frau Stokar.

Silke Stokar von Neuforn:

Zwei kurze Hinweise zum Schluss: Ich glaube, dass die Weiterentwicklung im gesamten IT-Bereich - dazu gehören auch Scoring-Verfahren und die Themen RFID und Biometrie - geradezu danach ruft, dass wir an eine Nachbesserung des Bundesdatenschutzgesetzes herangehen. Ich weiß sehr wohl, dass Rot-Grün das nicht geschafft hat. Gerade wir Abgeordneten haben uns nicht durchgesetzt, wir haben auch keine Verhandlungstermine mit dem zuständigen Ministerium bekommen. Das liegt

dort wie ein Brocken und meine Befürchtung ist natürlich, ob eine „Modernisierung“ des Datenschutzrechts in der Großen Koalition auch zu einer Verbesserung und Stärkung sowie zu mehr Datenschutz führt. Unabhängig davon bin ich der Meinung, dass wir tatsächlich die Debatte um die Struktur und um eine Modernisierung des Bundesdatenschutzgesetzes aufnehmen müssen und besonders hier im Bereich der mobilen Speicherung klarere Regelungen brauchen. Der Hinweis, dass Biometriedaten besonders schützenswerte Daten sind, der muss gesetzlich verankert werden. Hierzu muss es im Parlament eine Debatte geben. Zum Schluss möchte ich noch einen witzigen Hinweis geben, wozu Biometrie auch führt. Ich weiß zwar gar nicht, ob ich dass sagen darf, aber ich sage es trotzdem. Die Geheimdienste sind in einer sehr schwierigen Situation. Sie haben nämlich nicht mehr die Möglichkeit mit gefälschten Ausweispapieren zu arbeiten und damit in andere Länder zu fahren, weil die Gefahr, dass sie auffliegen, sehr groß sind. Das ist jetzt für uns nicht witzig. Der deutsche Geheimdienst - insbesondere der BND - überlegt intensiv, ob er nicht ähnlich wie andere Geheimdienste mit Klaridentitäten - das war mal eine Erfindung der Gegenseite – arbeiten sollte. Das heißt, ein Geheimnisdienstler bedient sich der Identität eines real existierenden Bundesbürger. Die arme Person, die es erwischt und die dann möglicherweise auch in die USA fährt. Nur soviel zu der ganz neuen Sicherheitsdebatte und wozu das Ganze noch führt. Wir werden das noch sehr intensiv und in alle Richtungen diskutieren müssen.

Dr. Hans-Peter Uhl:

Ich glaube, dass Sie da nicht gefährdet sind.

Peter Schaar:

Frau Pau, möchten Sie noch abschließend ein paar Worte sagen?

Petra Pau:

Nach diesem Geheimnisverrat bleibt mir eigentlich nur das Bekenntnis, dass ich mich immer fürchte, wenn jemand von Nachbesserung redet oder auch das Wort Reform in den Mund nimmt. Weil dann im allgemeinen die Anpassung der Gesetzeslage oder der Norm an die Bedürfnisse der Sicherheitskräfte und nicht so sehr die Anpassung gemeint ist, mit der man neue technische Möglichkeiten mit Schranken versieht. Wenn wir uns an die Nachbesserung machen, dann eher in der Richtung, in

dem wir die technischen Möglichkeiten, die es heute gibt, analysieren und verstehen. Wir sollten dann den verfassungsmäßigen Zustand und damit auch den Datenschutz wieder herstellen. Das sollte das Ziel sein und nicht die Ausweitung der Möglichkeiten.

Gisela Piltz:

Angesichts der Mehrheitsverhältnisse im Deutschen Bundestag haben wir nur dann eine Chance, gehört zu werden, wenn wir von einer interessierten Öffentlichkeit weit und breit und vor allen Dingen laut begleitet werden. Sie wären heute nicht hier, wenn Sie sich für das Thema nicht interessieren würden. Deshalb mein herzlicher Dank. Aber ich habe auch eine Bitte: trommeln Sie laut für den Datenschutz. Zum Abschluss noch mein persönlicher Ansatz im Datenschutz, es geht nicht nur darum zu schauen, welche weiteren Rechte soll der Staat erhalten? Wenn der Staat etwas von mir wissen will, muss er das rechtfertigen. Nicht ich muss mich rechtfertigen, wenn er was von mir will. Das ist ja auch eine Frage, welches Staatsverständnis man hat. Es geht mir darüber hinaus auch darum, zu schauen, ob es auch Eingriffe von Privaten gibt. Ich finde, nicht nur Eingriffe in das informationelle Selbstbestimmungsrecht durch den Staat sind wichtig, sondern auch die Eingriffe von Privaten wird sicherlich ebenfalls ein immer wichtigeres Thema.

Peter Schaar:

Herr Dr. Uhl.

Dr. Hans-Peter Uhl:

Also, „Nine Eleven“ war sicher der Auslöser für viele Maßnahmen. Und die Anschläge, die danach kamen – in Madrid, in London - werden auch nicht die letzten sein. Wir werden auch nicht verschont bleiben auf lange Sicht, obwohl es für die unmittelbare Zukunft keinerlei konkrete Hinweise gibt. Aber wenn wir diesen Kampf gegen den Terrorismus ernst nehmen, dann müssen wir technisch aufrüsten und dazu gehören auch die biometrischen Daten. Zweitens möchte ich feststellen, dass ich nicht alles was auf dem Gebiet aus Amerika kommt, für vorbildlich halte. Ich war jetzt auch dort und nicht nur, dass die auch nur mit Wasser kochen, sondern da wird auch viel überzogen. Deswegen muss jedes Land in seinem Rahmen - bei uns auch im Rahmen der EU natürlich - seine eigenen Gesetze machen. Was immer

wir gesetzlich machen, muss verhältnismäßig sein, d.h. es muss geeignet, es muss erforderlich und es muss zumutbar sein. Und deswegen werden wir sowohl die Datenerfassung, als auch die Datenspeicherung und dann die Datenverwendung nach diesen Spielregeln jeweils von Fall zu Fall prüfen. Wir sind sensibel für Datenschutzanforderungen, aber eben Datenschutz ist nicht über allem, sondern Sicherheit gibt es auch noch und vielleicht ist das noch wichtiger als Datenschutz. All diese Spannungsverhältnisse werden wir lösen.

Kurz und gut, ich halte es für richtig, dass wir biometrische Daten bei den Pässen und Personalausweisen einführen und alles weitere wird sich dann zeigen. Aber wir sollten das Gespräch fortsetzen. Herr Schaar war ja schon bei mir und wird auch noch wiederkommen, davon bin ich überzeugt. Diese Gespräche werden wir fortsetzen und Kollege Wiefelspütz wird auch die SPD-Meinung mit einbringen und dann schauen wir mal, ob die Große Koalition auf dem Gebiet das Gleiche zustande bringt.

Das wir keinen Applaus zu erwarten haben, insbesondere von den anwesenden drei Damen, die die drei Oppositionsparteien vertreten, gehört zu den demokratischen Spielregeln dazu. Sie müssen kritisieren.

Gisela Piltz:

Ach wissen Sie, ich habe in Nordrhein-Westfalen den Innen- und Rechtsteil mit Ihrer Schwesterpartei verhandelt und das ist auch ganz gut gegangen.

Schlusswort

Peter Schaar:

Zum Abschluss der Podiumsdiskussion bedanke mich bei den Podiumsgästen . Ich bedanke mich aber auch bei Ihnen, die Sie im Publikum so geduldig zugehört und sich auch beteiligt haben. Es war nicht das Ziel, hier irgendwelche unterschiedlichen Meinungen einzuebnen, sondern die Debatte voranzubringen. Ich glaube, das ist ein Stück gelungen. Es wird nicht die letzte Debatte zum Thema Biometrie im allgemeine und auch nicht die letzte Debatte über die angesprochenen Fragen im Zusammenhang mit dem Datenschutz sein. Als Konsens möchte ich heute feststellen, dass es nicht darum geht, Daten um ihrer selbst willen zu sammeln, sondern in jedem Fall zu prüfen, ob dies erforderlich, sinnvoll und verhältnismäßig ist. Dass wir bei der Beurteilung der einzelnen Speicherung dann zu unterschiedlichen Ergebnissen kommen, ist völlig normal und gehört zum demokratischen Prozess. Ich wünsche mir, dass die Gesellschaft dieses Thema auch insgesamt stärker diskutiert, stelle aber auch fest, dass es noch nicht in dem erforderlichen Maße geschieht. Wir Datenschützer versuchen gleichwohl unser Bestes beizutragen.

Noch mal besonders herzlichen Dank an die Damen und Herren, die hier entweder durch Ihren Vortrag oder ihre Beiträge zum Gelingen der Veranstaltung beigetragen haben.