



Lothar Binding  
Mitglied des Deutschen Bundestages

## Der digitale Ausweis aus politischer Sicht

Lothar Binding  
Mitglied des Deutschen Bundestages  
Vorstand der SPD Heidelberg

Koautorin: **Sina K. Frank, Dipl. Pol.**

**Heidelberg, August 2004**

**Berliner Büro**  
Platz der Republik 1  
11011 Berlin  
Tel: (030) 227 -73144  
Fax: (030) 227 -76435

**Bürgerbüro Heidelberg**  
Bergheimer Straße 88  
69115 Heidelberg  
Tel: (06221) 18 29 28  
Fax: (06221) 61 60 40

**Bürgerbüro Weinheim**  
Hauptstraße 122  
69469 Weinheim  
Tel: (06201) 60 22 12  
Fax: (06201) 60 22 13

eMail Berlin:  
[lothar.binding@bundestag.de](mailto:lothar.binding@bundestag.de)

eMail Heidelberg und Weinheim:  
[lothar.binding@wk.bundestag.de](mailto:lothar.binding@wk.bundestag.de)

**Homepage:** [www.lothar-binding.de](http://www.lothar-binding.de)

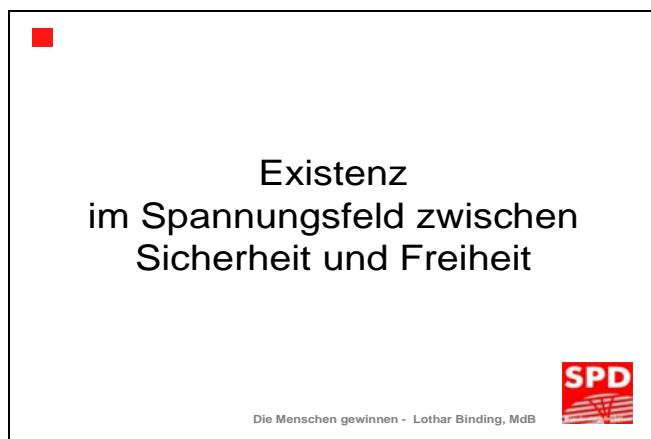
# Inhaltsverzeichnis

<b>EINLEITUNG</b> .....	<b>3</b>
<b>DER EINSTIEG IN EINE GLOBALE BIOMETRIEGESTÜTZTE SICHERHEITSINFRASTRUKTUR</b>	<b>4</b>
TERMINOLOGIE .....	4
ENTSCHEIDUNG FÜR „SMART BORDERS“ – BIOMETRISCHE „VIRTUELLE GRENZEN“ .....	4
<b>DER DIGITALE PERSONALAUSWEIS</b> .....	<b>5</b>
BIOMETRISCHE MERKMALE .....	6
<i>Iriserkennung</i> .....	7
<i>Fingerabdruck</i> .....	7
<i>Gesichtserkennung, Gesichtsproportionen</i> .....	8
<i>Stimme und Sprachverhalten</i> .....	8
<i>Gangerkennung</i> .....	8
<i>Handgeometrie</i> .....	9
<i>Andere biometrische Technologien</i> .....	9
BETRIEBSARTEN .....	9
VERIFIKATION .....	10
IDENTIFIKATION .....	10
ES IST NICHT ALLES GOLD WAS GLÄNZT .....	10
<b>DATENSCHUTZGERECHTER EINSATZ</b> .....	<b>10</b>
<b>IN DEUTSCHLAND MAßSTÄBE SETZEN</b> .....	<b>14</b>

## Einleitung

Rasterfahndung, Bewegungsprofile, Ausleuchtung der Privatsphäre – wer erschreckt eigentlich noch angesichts dieser Begriffe? In den 80er Jahren gab es durch die geplante Volkszählung in Deutschland eine umfangreiche Datenschutzdiskussion. In vielen Städten fanden Demonstrationen statt, viele Bürger fühlten sich an George Orwells Buch „1984“ erinnert. Wie dort dargestellt, wurde befürchtet, dass die öffentliche Verwaltung als eine Art „Großer Bruder“ die Daten der Bürger beliebig speichern, zusammenfügen und auswerten könnte und dadurch der „gläserner Bürger“ geschaffen würde. Hintergrund dieser Bedenken war die Sorge, dass unbescholtene Bürger vorschnell unter Verdacht geraten könnten und ihre Daten – einmal gespeichert – unkontrolliert in Datenbanken konserviert werden könnten. Mit den Erfahrungen in den 70er Jahren, anlässlich der ersten groß angelegten Rasterfahndungen zur Terrorismusbekämpfung gab es eine hohe Sensibilität gegenüber den Gefahren, nicht etwa durch den Terrorismus, sondern durch den Staatsreflex auf terroristische Kriminalität.

Anders heute: Die Hintergründe des Volkszählungsboykotts sind vergessen. Seitdem der Angriff am 11. September 2001 die modernen „westlichen“ Gesellschaften mit einer bislang unbekanntem Bedrohung konfrontiert, scheint Sicherheit für die Gesellschaft das höchste Ziel geworden zu sein. Musste sich damals derjenige rechtfertigen, der Daten erheben oder sammeln wollte, ist es im Alltag heute umgekehrt. Wer auf den Schutz persönlicher Daten drängt, gerät in den Verdacht, etwas verheimlichen zu wollen. Die Sensibilität für den Umgang mit persönlichen Daten ist heutzutage erschreckend gering. Jede Einzelhandels- und Baumarktkette gewährt Kundenkarten, das elektronische Zahlungssystem ist Normalität, selbst Homebanking ist in weiten Teilen eingeführt. Möglichen Datensammlungen, -analysen und -vertrieb wird von Verbrauchern nicht als Bedrohung empfunden. Der Gewöhnungsprozess ist vorprogrammiert.



*„Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden noch die Frucht derselben zu genießen; denn ohne Sicherheit ist keine Freiheit.“ (Wilhelm von Humboldt)*

Sicherheit, die innere wie auch die äußere, ist zu einem Leitwort geworden, dessen Konjunktur bis heute anhält. Sicherheit und die Besorgnis darüber, ist allgegenwärtig. Und das Resultat? Es gibt ein allgemeines Gefühl von Unsicherheit, wir haben Angst vor Bedrohungen, die wir nicht abwehren und vor Tätern, die wir nicht fassen können. Das Ringen um eine Reduzierung der Verletzlichkeit unserer Zivilisation prägt das Lebensgefühl der Menschen. Viele Bürgerinnen und Bürger sind plötzlich bereit zu akzeptieren, dass in ihre

Freiheitsrechte eingegriffen wird, dass stetig mehr Daten über sie gesammelt werden. Damit wird die Illusion verbunden, dass sie sicherer seien. Die Strategie des Terrorismus stellt die Kultur des demokratischen Miteinanders auf eine harte Probe. Die Balance zwischen den Staatszielen Sicherheit und Freiheit scheint aus dem Gleichgewicht geraten zu sein. Die Kernfrage in der aktuellen Sicherheitsdebatte lautet: Was bringt den demokratischen Rechtsstaat mehr in Gefahr - der Terror oder dessen Bekämpfung? Beschwört der Reflex auf den neuen internationalen Terrorismus gerade jenen Überwachungsstaat herauf, den wir aus Orwells Buch „1984“ kennen?

## Der Einstieg in eine globale biometriegestützte Sicherheitsinfrastruktur

Eines ist sicher: Das Zeitalter uneingeschränkter Sicherung der Persönlichkeitsrechte ist vorbei. Die Chance auf Anonymität und Datenschutz werden in Zukunft nicht mehr an erster Stelle des gesellschaftlichen Wertesystems stehen. Das macht den Weg frei für den Einstieg in eine globale biometriegestützte Sicherheitsinfrastruktur.

### Terminologie

Der Begriff „*Biometrie*“ leitet sich von den griechischen Wörtern „*bios*“ für Leben, und „*metros*“ für Maß ab. Im Brockhaus ist Biometrie als „*die Anwendung von Methoden der mathematischen Statistik auf die Erfassung und Bearbeitung von Daten in Bereichen der Biologie, Medizin, Landwirtschaft u. a.; in der Informatik die Verarbeitung bioelektrischer Körpersignale für Erkennungs- und Sicherheitsverfahren.*“ definiert<sup>1</sup>. Unter Biometrik wird „*das automatisierte Messen eines oder mehrerer spezifischer Merkmale eines Lebewesens*“<sup>2</sup> verstanden. Häufig wird der Begriff „*Biometrie*“ abkürzend für die eigentlich genauere Bezeichnung „*Biometrische Identifikation*“ verwendet, bei der es darum geht eine „*Biometriespezifizierte Person von anderen unterscheidbar zu machen*“<sup>3</sup>

## Entscheidung für „*smart borders*“ – biometrische „*virtuelle Grenzen*“

In vielen Staaten sind mit Tests, Pilotprojekten und Machbarkeitsstudien, zunehmend auch mit Gesetzen und Verordnungen erste Grundlagen für eine biometrische Ausstattung von Ausweisdokumenten und biometrische Grenzkontrollen gelegt worden.

Seit Anfang des Jahres werden beispielsweise Einreisende in die USA mit Fingerabdruck und Gesichtsbild erfasst; der neueste Zeitplan sieht vor, bis Oktober 2006 von Einreisenden aus Deutschland, Großbritannien, Japan und 24 weiteren Staaten digital lesbare Reisedokumente mit biometrischen Erkennungsmerkmalen digitale Fingerabdrücke und verschlüsselte Angaben zu Gesichtsmarkmalen zu fordern („*Visa Entry Reform Act 2002*“).

Auch die EU treibt die Entwicklung und Umsetzung einer abgestimmten Strategie bei biometrischen Ausweisdokumenten voran. Es liegen einigungsfähige Vorschläge für Visa,

---

<sup>1</sup> *Der Brockhaus, Band. 9.*, vollständig überarbeitete und aktualisierte Auflage. Mannheim: Bibliographisches Institut & F.A. Brockhaus 2002

<sup>2</sup> Micheal Behrens, Richard Roth (Hrsg.): „*Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven*“ DuD-Fachbeiträge, Vieweg, 2001, S.10

<sup>3</sup> Micheal Behrens, Richard Roth (Hrsg.): „*Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven*“ DuD-Fachbeiträge, Vieweg, 2001, S.10

Aufenthaltstitel für Nicht-EU-Bürger und Pässe für EU-Bürger vor. Außerdem gibt es den festen Willen, innerhalb der nächsten Jahre schrittweise neue Ausweisdokumente und biometriegestützte Ausweiskontrollen einzuführen. Da die EU in diesem Bereich die Gesetzgebungskompetenzen hat, wird sich das auch auf deutsche Staatsbürger auswirken.

In *Deutschland* sind bereits das Pass- und Personalausweisgesetz und das Ausländergesetz geändert worden: Eine Einbringung zusätzlicher biometrischer Merkmale – Gesicht, Finger oder Hand – in Ausweisdokumente für Bundesbürger und Ausländer kann jetzt vorgenommen werden. Es bedarf aber weiterer konkreter Modalitäten und Einzelheiten durch den Gesetz- und Verordnungsgeber.


Die G8-Staaten unterstützen die *International Civil Aviation Organization (ICAO)* und deren Bemühungen zur Standardisierung biometrischer Verfahren. Die ICAO – eine Sonderorganisation der Vereinten Nationen – hat nach längerer Vorarbeit die Empfehlung ausgesprochen, in internationalen Reisedokumenten das Gesichtsbild als erstes – für die Mitgliedsstaaten verbindliches – Merkmal aufzunehmen. Für Staaten, die mit Hilfe der Biometrie Datenbankabgleiche vornehmen wollen, wird optional Fingerabdruck und/oder Iris genannt.

## Der digitale Personalausweis

Den Personalausweis kann man verlieren, die PIN-Nummer der EC-Karte vergessen, Reisepässe und Unterschriften können gefälscht und Daten können manipuliert werden – spezifische Merkmale des Körpers aber bleiben den Menschen ihr Leben lang erhalten. Fazit: Warum also nicht den Körper als Ausweis nehmen, als Beweis dafür, dass man der ist, für den man sich ausgibt?

■ **Die Entscheidung über den neuen Ausweis ist getroffen**

- bio-metrische Merkmale im Chip  
– orientiert am Reisepass  
(Entscheidung des BMI über die Gesamtstrategie Biometrie vom 30. Juni 2003).
- der Chip hat Bürgerkartenfunktion  
– ermöglicht elektronische Identifizierung, etwa im Internet,  
(Entscheidung des BMI vom 1. Oktober 2003)



8 Die Menschen gewinnen - Lothar Binding, MdB

Die Entscheidung über Biometrie und Bürgerkartenfunktion im Ausweis ist in Deutschland getroffen:

- Der neue Personalausweis soll biometrische Merkmale im Chip enthalten, die sich an denen des Reisepasses orientieren werden.
- Darüber hinaus soll der Chip auch eine Bürgerkartenfunktion wahrnehmen, d.h. dem Inhaber eine elektronische Identifizierung, etwa im Internet, ermöglichen.

## ■ Biometrische Merkmale machen Mut

- Pässe werden sicherer
- Pässe der Bürger werden vor Fälschung geschützt, schützen die Bürger
- Ausgabe von Visa wird vereinfacht
- Biometrische M. ergänzen die digitale Signatur im elektronischen Rechtsverkehr
- Verbrechensbekämpfung wird verbessert



12

Die Menschen gewinnen - Lothar Binding, MdB

Fingerabdruck, Iris- oder Gesichtserkennung – welches biometrische Merkmal in Zukunft neben Lichtbild und Unterschrift digital auf Pässen und Personalausweisen von Bundesbürgern sowie in „Ausländerausweisen“ abgespeichert werden soll, hatte das im Januar 2002 in Kraft getretene „*Terrorismusbekämpfungsgesetz*“ noch nicht festgelegt.

## ■ Biometrische Methoden



PC-Tastatur mit Sensorfeld für Fingerabdruck



Iriserkennung



Gesichtserkennung mit Hilfe von Streifenrastern

(Alle Bilder BSI-Jahresbericht 2003)

Die Menschen gewinnen - Lothar Binding, MdB



Im „*Zweiten Sachstandsbericht*“ zum Thema „*Biometrie und Ausweisdokumente*“ kam das Büro für Technikfolgenabschätzung (TAB) beim Deutschen Bundestag zu dem Befund, dass die Finger-, Gesichts-, und Irisabdruck-Erkennung eine annähernd vergleichbare technische Leistungsfähigkeit besitzen. Demgegenüber fällt die Handgeometrie-Erkennung bei insgesamt durchschnittlichen Evaluationsergebnissen durch eine hohe Falschakzeptanzrate ab.

Am Frankfurter Flughafen laufen zurzeit zwei Tests zur automatischen Personenerkennung durch biometrische Merkmale. Zum einen werden 2000 Mitarbeiter für den Zugang zu Sicherheitsbereichen anhand von Gesichtsform, Augeniris und Fingerabdrücken überprüft. Bei einer zweiten Versuchsreihe lassen sich Fluggäste beim Bundesgrenzschutz registrieren, um bei Grenzkontrollen mit Hilfe der computergestützten Iris-Prüfung schneller abgefertigt zu werden.

## Biometrische Merkmale

„ Mittlerweile existieren eine ganze Reihe von biometrischen Merkmalen, die von einem Computer ausgewertet werden können. Üblicherweise unterteilt man sie in so genannte aktive Merkmale, basierend auf verhaltenstypischen Merkmalen, und passive Merkmale, die sich auf physiologische Merkmale beziehen.“<sup>4</sup> In der nachfolgenden Tabelle sind die wichtigsten biometrischen Merkmale zusammengestellt:

Die wichtigsten passiven und aktiven biometrischen Merkmale	
Passive Merkmale	Aktive Merkmale
Irismuster	Unterschriftendynamik
Fingerbildererkennung	Lippenbewegung beim Sprechen
Gesichtserkennung	Stimmerkennung
Retinamuster	Anschlagsdynamik auf Tastaturen
Handgeometrie	Bewegung (Gangartzyklus)
Venenmuster	DNS
Thermogramm	
Form des Ohres	
Geruch	

Quelle: Digitale Fachbibliothek ‚Das innovative Unternehmen‘ Produkte – Prozesse – Dienstleistungen (CD Rom) Hrsg.: Barske, Gerybadze, Hünninghausen, Sommerlatte, Digitale Fachbibliothek

Im folgenden Abschnitt sollen die wichtigsten biometrischen Technologien kurz beschrieben werden.

### Iriskennung

Die Iriskennung stützt sich auf die Tatsache, dass die Retina jedes einzelnen Individuums einmalig ist. Da sich die Oberfläche der Iris aus einem Kranz, Fäden, Vertiefungen, Flecken, Gruben, ringförmig angeordneten Rillen und Wellen zusammensetzt, die in unendlich vielen verschiedenen Variationen auftreten und in ebenso vielen Arten miteinander kombiniert sind, besitzt die Iris massenhaft typische Erkennungsmerkmale. Die Iriskennung (Iris-Scanning) gilt daher als extrem genaue Identifizierungstechnologie. Zudem ist das Verfahren, das nicht länger als ein bis zwei Sekunden in Anspruch nimmt, relativ schnell. All diese Eigenschaften haben die Iriskennung zu einer attraktiven Technologie im Einsatz für Sicherheitsanwendungen gemacht.

### Fingerabdruck

Die Vorteile liegen regelrecht auf der Hand. Genauer: Auf den Fingern. „ Die Fingerabdruckererkennung beruht auf der Tatsache, dass die Einzigartigkeit eines Fingerabdruckes durch die Analyse winziger Merkmale wie Schweißdrüsen, Rillenabstände

<sup>4</sup> Veronika Nolde: Who is who? Einsatzmöglichkeiten biometrischer Verfahren, in: Digitale Fachbibliothek ‚Das innovative Unternehmen‘. Produkte – Prozesse – Dienstleistungen (CD-Rom) Hrsg.: Barske, Gerybadze, Hünninghausen, Sommerlatte, Digitale Fachbibliothek

und Verzweigungen definiert werden kann. Die Wahrscheinlichkeit, dass zwei Individuen den gleichen Fingerabdruck haben, wird auf weniger als eins zu einer Milliarde geschätzt.“<sup>5</sup> Ungenauigkeiten, die durch fettige, verschmutzte oder rissige Haut auftraten, stellten Wissenschaftler bisher vor große Probleme. Dieses Hindernis wurde vor kurzem durch die Entwicklung eines Gerätes gelöst, das es ermöglicht, die spezifischen Eigenschaften eines Fingerabdrucks ohne direkten Hautkontakt aufzuzeichnen, zu digitalisieren und in ein digitales Bild umzuwandeln.<sup>6</sup>

### **Gesichtserkennung, Gesichtsproportionen**

*„Um eine andere Person zu erkennen, blicken wir ihr zumeist ins Gesicht, da die sichtbaren Unterscheidungsmerkmale im Gesicht konzentriert auftreten. Insbesondere die Augen scheinen nicht nur darüber Auskunft zu geben, wer jemand ist, sondern auch wie sich diese Person fühlt, worauf ihre Aufmerksamkeit gerichtet ist usw. Will jemand seine Identität oder die Sichtbarkeit innerer Vorgänge verbergen, so muss er sich maskieren. Daher kann die Gesichtserkennung als eine Art elektronischer Demaskierung bezeichnet werden.“<sup>7</sup>*

### **Stimme und Sprachverhalten**

Die Stimmerkennung tanzt immer Unterschied zu all den anderen Technologien aus der Reihe, da sie auf nichtvisuelle Eigenschaften des menschlichen Körpers verzichtet. Tonvibrationen in der Stimme eines Menschen werden hierzu gemessen und mit vorhandenen Proben verglichen. Die zu identifizierende Person muss dazu meist ein bestimmtes Erkennungswort oder einen vollständigen Erkennungssatz aussprechen, die den Verifizierungsprozess unterstützen. Diese Methode funktioniert sogar am Telefon – hat aber einen großen Schwachpunkt, nämlich die Empfindlichkeit gegen Hintergrundgeräusche und Interferenzen.

### **Gangerkennung**

Die Identität einer Person kann jedoch nicht nur anhand äußerlicher Merkmale oder der Stimme festgelegt werden. Auch die Gangart kann einen Menschen identifizieren. Im Gegensatz zu den bereits besser ausgereiften biometrischen Technologien, bei denen Körperteile Gegenstand der Untersuchung sind, unterliegt die Erkennung der Gangart der zusätzlichen Problematik, Bewegungen als Muster aufzuzeichnen und zu identifizieren. *„Wissenschaftler der Universität Southampton haben ein Modell entwickelt, das die Beinbewegungen als Pendelbewegungen wahrnimmt und die Hüftneigung als Variable definiert.“<sup>8</sup> Bei einem anderen Modell werden Länge und Form der Beine zusätzlich zur Geschwindigkeit der Gelenkbewegungen gemessen. Ziel der Forscher ist es, beide Modelle zusammenzuführen. Damit würde die Identifizierung anhand der Gangart zu einer voll einsatzfähigen biometrischen Technologie werden. Die Anwendung dieser Technologie auf bewegliche Subjekte macht sie als Überwachungstechnologie besonders interessant. So wird an der University of Leeds an Computermodellen gearbeitet, die es ermöglichen, auffällige Bewegungsabläufe von Menschen zu erkennen: etwa die eines potenziellen Autodiebs auf einem Parkplatz.“<sup>9</sup> Weibliche Ladendiebe, die sich als Schwangere tarnen und so die Beute*

---

<sup>5</sup> Biomterie, in: Konrad Becker: Die Politik der Infosphäre. World-Information.org. BpB, Schriftenreihe (Bd. 386), [http://www.bpb.de/publikationen/7KIVBA,0,0,5\\_3\\_Biometrie.html](http://www.bpb.de/publikationen/7KIVBA,0,0,5_3_Biometrie.html)

<sup>6</sup> Vgl.: [www.ddsi-cpc.com](http://www.ddsi-cpc.com)

<sup>7</sup> Biomterie, in: Konrad Becker: Die Politik der Infosphäre. World-Information.org, BpB, Schriftenreihe (Bd. 386), [http://www.bpb.de/publikationen/7KIVBA,0,0,5\\_3\\_Biometrie.html](http://www.bpb.de/publikationen/7KIVBA,0,0,5_3_Biometrie.html)

<sup>8</sup> Vgl.: [www.isis.ecs.soton.ac.uk/image/gait/](http://www.isis.ecs.soton.ac.uk/image/gait/)

<sup>9</sup> Vgl.: [www.comp.leeds.ac.uk/vision/imv/index.html](http://www.comp.leeds.ac.uk/vision/imv/index.html)

*verstecken, können aufgedeckt werden, da tatsächlich Schwangere anhand ihres Ganges vom System erkannt werden können.“<sup>10</sup>*

## **Handgeometrie**

Bei der Handerkennung wird ein dreidimensionales Bild der Hand erstellt und mit einem entsprechenden gespeicherten Bild verglichen. Im Gegensatz zu den Geräten zur Vermessung von Fingerabdrücken oder der Iris sind die Apparate zur Handerkennung relativ groß und sperrig, können aber umfassende Identifizierungsvorgänge in kürzester Zeit durchführen. Sie kommen daher vorwiegend an Orte wie Flughäfen, wo es darauf ankommt, viele Menschen in kurzer Zeit abzufertigen bieten daher einen idealen Einsatzort.

## **Andere biometrische Technologien**

Andere biometrische Technologien, die hier nicht im Detail besprochen werden, beruhen auf besonderen Merkmalen von Unterschrift, Tastaturanschlag, Ohr, Venenmuster, Retina, Körpergerüchen oder DNA. Diese Technologien befinden sich entweder noch in frühen Entwicklungsphasen oder finden nur in hoch spezialisierten und daher eingeschränkten Bereichen Anwendung.

Für die Tauglichkeit im praktischen Einsatz müssen biometrische Technologien jedoch bestimmte Voraussetzungen erfüllen:

- Universalität – Jede Person muss das betreffende Merkmal aufweisen.
- Einzigartigkeit – Das Merkmal unterscheidet sich von Person zu Person.
- Beständigkeit – Das Merkmal verändert sich im Lauf der Zeit nur geringfügig.
- Erfassbarkeit – Das Merkmal ist technisch messbar.<sup>11</sup>

Laut Peter Bittner<sup>12</sup> können sich auf einer Breiten Basis nur Verfahren durchsetzen, die folgende weitere, weichere Kriterien erfüllen:

- Akzeptanz – Kulturelle Vorbehalte werden berücksichtigt.
- Nutzerfreundlichkeit – Die Erfassung verläuft einfach, schnell und schmerzfrei.
- Robustheit – Das Verfahren weist eine hohe Überwindungsresistenz auf.
- Ökonomie – Die Kosten für die Erfassung übersteigen nicht den Rahmen.

Keines der heute verfügbaren Verfahren kann jede dieser Voraussetzungen vollständig erfüllen.

## **Betriebsarten**

Bevor biometrische Daten verarbeitet werden können, müssen sie erfasst werden. Dazu wird zuerst das betreffende Merkmal mittels eines Sensors aufgenommen und digitalisiert. Je nach Art des Merkmals kommen hierfür verschiedene Technologien in Frage. Aus den vom Sensor gelieferten Rohdaten gewinnt ein meist programmatisch implementierter Merkmals-

---

<sup>10</sup> Biometrie, in: Konrad Becker: Die Politik der Infosphäre. World-Information.org, BpB, Schriftenreihe (Bd. 386), [http://www.bpb.de/publikationen/7KIVBA,0,0,5\\_3\\_Biometrie.html](http://www.bpb.de/publikationen/7KIVBA,0,0,5_3_Biometrie.html)

<sup>11</sup> A. K. Jain, R. Bolle, S. Pankanti (Eds.): "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, 1999, S.4

<sup>12</sup> Peter Bittner: "e-Identity - wenn der Körper vermessen zur Information wird", Arbeitsgruppe 3, 19. IfF Jahrestagung, 2003

Extraktions-Algorithmus die „*Parameter eines mathematischen Modells der Rohdaten*“<sup>13</sup>, - im Fachjargon Template (Schablone) genannt. Dies sind zum Beispiel geometrische Bemaßungen der Hand oder charakteristische Frequenzen der Stimme, die sehr Platz sparend gespeichert werden können. Es ist nicht möglich, anhand des Templates die Rohdaten erneut zu gewinnen. Trotzdem handelt es sich hier nicht um eine Einwegfunktion, da sich sehr leicht Rohdaten erzeugen lassen, die zu einem identischen Template führen. Die Referenzdaten werden bei der so genannten Ersterfassung (Enrolment) erhoben, in der unter kontrollierten Bedingungen alle benötigten Merkmale mehrfach eingelernt werden, bis eine optimale Template-Qualität garantiert ist. Dem Vorgang des Enrolment kommt insofern eine besondere Bedeutung zu, als dass er die Grundlage für eine spätere gute Erkennungsrate bildet. Nur wenn das Enrolment sorgfältig durchgeführt wird, lassen sich genügend Daten des körpereigenen Merkmals erfassen, damit für eine spätere Erkennung auch bei einem schlechten aktuellen Muster noch hinreichend Übereinstimmungen vorhanden sind.

Die gewonnenen Daten können nun beliebig oft zur Identifikation oder Verifikation von Personen herangezogen werden:

### **Verifikation**

Bei der Verifikation wird festgestellt, ob eine Person, die ein Dokument vorlegt, dessen berechtigter Inhaber ist. Dazu reicht es aus, wenn die biometrischen Daten nur auf dem Ausweispapier gespeichert sind. (*eins zu eins Vergleich*)

### **Identifikation**

Für eine Identifikation müssen die persönlichen Daten hingegen zusätzlich in einem zentralen Register gespeichert sein. Mit diesem lässt sich beispielsweise überprüfen, ob ein Mensch, dessen Gesicht von einem Erkennungsgerät erfasst wurde, in einer Fahndungsdatenbank registriert ist. (*eins zu viele Vergleich*)

### **Es ist nicht alles Gold was glänzt**

Die hier unter technischen Gesichtspunkten beinahe begeistert klingende Beschreibung biometrischer Merkmale und deren Erfassung, darf nicht darüber hinwegtäuschen, dass es gleichwohl in jeglicher konkreten Anwendung stets einen Restzweifel gibt, ob die Erfassung korrekt war, ob es sich nicht doch um eine Fälschung handelt und *last but not least*, ob die datenschutzrechtlichen Belange wirklich auf Dauer gesichert werden können und gesichert werden. In diesem Zusammenhang sei auf die kritischen Beiträge der DFN-Tagung des letzten Jahres hingewiesen.

### **Datenschutzgerechter Einsatz**

Unter dem Gesichtspunkt Datenschutz sehe ich vor allem in der zuvor genannten Identifikation ein Risiko, denn dessen Dimensionen sind kaum abzuschätzen. Hinsichtlich der Ausweispapiere für Bundesbürger hat die Regierung geregelt, dass die biometrischen Merkmale nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwendet werden dürfen, so dass dem aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteten Zweckbindungsgrundsatz ausreichend Rechnung getragen ist.

---

<sup>13</sup> Unabhängiges Landeszentrum für Datenschutz: „Positionspapier zum Antiterrorgesetz der Bundesregierung“, Kiel, 7. Dezember 2001, S.14

Anders ist der Bereich der „Ausländerausweise“ zu beurteilen. Hier ist die Aufnahme biometrischer Merkmale geregelt, es fehlt aber vollständig eine ausreichend bestimmte Zwecksetzung. § 5 Abs. 7 AuslG enthält eine pauschale Verarbeitungsbefugnis für alle Stellen im Rahmen ihrer gesetzlichen Aufgaben. Dies ist mit den verfassungsrechtlichen Vorgaben zur Zweckbindung und dem Bestimmtheitsgebot nicht in Einklang zu bringen.

Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger ist zurzeit gesetzlich ausgeschlossen. Eine Speicherung auf dem Ausweisdokument genügt, um den gesetzlichen Zweck zu erreichen. Die Einrichtung zentraler Referenzdateien für Ausländer ist gesetzlich nicht ausgeschlossen. Eine zentrale Datenspeicherung bei öffentlichen Stellen und ohne strenge Zweckbindung ist jedoch aus Gründen der Ungleichbehandlung im Sinne des Art. 3 GG und des Prinzips der Verhältnismäßigkeit problematisch. Eine dezentrale Speicherung der Daten in einem Register würde z.B. die Verwendung zu strafrechtlichen Ermittlungszwecken oder zur „Rasterfahndung“ ermöglichen. Die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, birgt jedoch die Gefahr einer Zweckentfremdung und ist datenschutzrechtlich problematisch.

Entgegen meiner Auffassung, wäre die *„Speicherung der biometrischen Merkmale von Ausländern im Lichte des Grundrechts auf informationelle Selbstbestimmung außerhalb des Ausweisdokumentes bei einer dezentralen oder zentralen Ausländerbehörde vertretbar, wobei eine ausschließliche Bindung an Zwecke der Datensicherung gesetzlich vorgesehen werden müsste“*.<sup>14</sup>

*„ Das im Januar 2002 in Kraft getretene Gesetz zur Bekämpfung des internationalen Terrorismus („Terrorismusbekämpfungsgesetz“) enthält als ein wichtiges Element die Regelung der Aufnahme biometrischer Merkmale in Pässe und Personalausweise von Deutschen sowie in Ausweisdokumente für Ausländer. Das Gesetz sieht vor, dass neben dem Lichtbild und der Unterschrift weitere Merkmale in den Pass und Personalausweis – auch in verschlüsselter Form – aufgenommen werden dürfen. Gleichzeitig wird durch neue Vorschriften die Aufnahme derartiger biometrischer Merkmale auch in die Identifikationspapiere von Ausländern und Asylbewerbern ermöglicht. Die Arten der biometrischen Merkmale, ihre Einzelheiten, die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung sollten durch ein noch zu erlassendes Ausführungsgesetz bzw. eine Rechtsverordnung gesondert geregelt werden. Damit beabsichtigt der Gesetzgeber, die Möglichkeiten zur computergestützten Identifizierung von Personen auf der Grundlage der Ausweisdokumente zu verbessern, u.a. um zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen. Zur augenblicklichen gesetzlichen Grundlage ist folgendes anzumerken (Kap. V):*

- *Hinsichtlich der Ausweispapiere für Bundesbürger hat der Gesetzgeber geregelt, dass die biometrischen Merkmale nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung ausgelesen und verwendet werden dürfen, so dass dem aus dem Grundrecht auf informationelle Selbstbestimmung hergeleiteten Zweckbindungsgrundsatz ausreichend Rechnung getragen ist. Anders ist der Bereich der „Ausländerausweise“ zu beurteilen. Hier ist die Aufnahme biometrischer Merkmale geregelt, es fehlt aber*

---

<sup>14</sup> TAB Arbeitsbericht Nr. 93, Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung, Zweiter Sachstandsbericht, Thomas Petermann, Constanze Scherz, Arnold Sauter.

vollständig eine ausreichend bestimmte Zwecksetzung. § 5 Abs. 7 AuslG enthält eine pauschale Verarbeitungsbefugnis für alle Stellen im Rahmen ihrer gesetzlichen Aufgaben. Dies ist mit den verfassungsrechtlichen Vorgaben zur Zweckbindung und dem Bestimmtheitsgebot nicht in Einklang zu bringen.

- Der Gesetzgeber hat eine Beschränkung der in Betracht kommenden biometrischen Merkmale auf solche von „Fingern oder Händen oder Gesicht“ vorgenommen. Damit sind nicht nur andere, sondern ist auch die Kombination mehrerer Merkmale ausgeschlossen. Diese Einschränkung ist nach heutigem technischem Kenntnisstand problematisch, da hierdurch u.U. die Leistungsfähigkeit biometrischer Systeme nicht auszuschöpfen ist.
- Hinsichtlich der Auswahl der einzelnen in Betracht kommenden biometrischen Merkmale ist zu berücksichtigen, dass bei der Anwendung biometrischer Verfahren sensible, persönlichkeitsbezogene Zusatzinformationen anfallen können. Deshalb ist es notwendig, die mit der Aufnahme der biometrischen Merkmale verbundenen Risiken zu begrenzen. In Betracht kommt hierfür vor allem ein Verzicht auf die Speicherung von Rohdaten.
- Die vom Gesetzgeber – ohne nähere Vorgaben – geschaffene Befugnis, die Merkmale und Angaben auch in verschlüsselter Form in das jeweilige Dokument zu integrieren, macht eine genaue Regelung der Frage erforderlich, in welcher Weise eine Verschlüsselung vorzunehmen ist bzw. die biometrischen Daten mit einer elektronischen Signatur zu signieren sind. Angesichts der hierfür erforderlichen Sicherheitsumgebung erscheint eine zentrale Erstellung der Dokumente vorzugswürdig.
- Eine Speicherung der Daten in einem zentralen Register ist für Bundesbürger zurzeit gesetzlich ausgeschlossen. Eine Speicherung auf dem Ausweisdokument genügt, um den gesetzlichen Zweck zu erreichen. Die Einrichtung zentraler Referenzdateien für Ausländer ist gesetzlich nicht ausgeschlossen. Eine zentrale Datenspeicherung bei öffentlichen Stellen und ohne strenge Zweckbindung ist jedoch aus Gründen der Ungleichbehandlung im Sinne des Art. 3 GG und des Prinzips der Verhältnismäßigkeit problematisch. Eine dezentrale Speicherung der Daten in einem Register würde z.B. die Verwendung zu strafrechtlichen Ermittlungszwecken oder zur „Rasterfahndung“ ermöglichen. Die Speicherung biometrischer Merkmale in einem Datenbestand, der nicht der alleinigen Verfügungsgewalt des Betroffenen unterliegt, birgt die Gefahr einer Zweckentfremdung und ist datenschutzrechtlich problematisch.

Für die Speicherung der biometrischen Merkmale von Ausländern wäre im Lichte des Grundrechts auf informationelle Selbstbestimmung eine Speicherung außerhalb des Ausweisdokumentes bei einer dezentralen oder zentralen Ausländerbehörde aber vertretbar, wobei eine ausschließliche Bindung an Zwecke der Datensicherung gesetzlich vorgesehen werden müsste.<sup>15</sup>

---

<sup>15</sup> TAB Arbeitsbericht Nr. 93, Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung, Zweiter Sachstandsbericht von Thomas Petermann, Constanze Scherz, Arnold Sauter.

## ■ Biometrische Merkmale machen Angst

- Automatische Überwachung mit biometrischen Daten – Kameras mit Gesichtserkennung allüberall
- Unkontrollierte Zusammenführung aller Daten – Datenbanken bilden Persönlichkeitsprofile, scannen die Existenz



14

Die Menschen gewinnen - Lothar Binding, MdB


Doch wer kann garantieren, dass niemand die Sammlung der sensiblen biometrischen Daten unbefugt, auch z.B. im Ausland, übernimmt? Das Prinzip der zentralen Speicherung bekommt hier globalen Charakter. Ich habe große Bedenken gegen unterschiedliche Regelungen für Ausländer und Inländer in Deutschland. Gerade im Zusammenhang mit Pässen wirken Regelungen international und Sonderrechte für Inländer verkehren sich im Ausland schnell in Sonderrechte von Ausländern. Wäre eine zentrale Speicherung biometrischer Merkmale für Inländer verboten, für Ausländer aber erlaubt, so wäre plausibel nicht zu begründen, warum im Ausland nicht auch die entsprechenden Merkmale Deutscher Staatsbürger zentral gespeichert werden.

In den USA war die Sozialversicherungsnummer ausdrücklich nicht zur Identifikation vorgesehen, heute wird sie praktisch überall als Personenkennziffer genutzt. Ebenso ist anzunehmen, dass mit solchen Daten auch privater Handel betrieben wird, ähnlich wie dies bereits mit Email- und Postadressen geschieht. Besonders Kaufhäuser mit ihren umfassenden Kameraüberwachungssystemen und Kundenkartensystemen könnten starkes Interesse daran zeigen. Ungeahnte Möglichkeiten eröffnen sich auch in Kombination mit der aufkommenden Radio Frequenz Identifikation (RFID). Der winzig kleine, gerade einmal drei Quadratmillimeter große Chip, der in sämtliche Materialien eingearbeitet werden könnte – sogar in die menschliche Haut kann er implantiert werden – funktioniert wie ein kleiner Peilsender. Spezielle Lesegeräte funken ein Erkennungssignal an die Antennen der Chips, die dann die bekannten Daten ausspuckt. Mithilfe von Datenbanken ist dann jeder Gegenstand und jedes Lebewesen eindeutig zu identifizieren und sämtliche Informationen über den Träger können sprichwörtlich im Vorbeigehen gespeichert werden. Dies wird ein Horrorszenario für den Datenschutz.

Sollte die Digitalisierung des Körpers mittels biometrischer Technologien tatsächlich so weite Verbreitung finden, wie es ihre Befürworter erwarten, so könnte sich ein neues, elektronisches feudales System entwickeln. In diesem System würden die Menschen als Datenkörper erfasst.


Die Freiheit, sich zu bewegen, zu handeln, zu kommunizieren wird dadurch begrenzt, dass es Kontrollinstanzen gibt, die über jede Bewegung, über jeden Austausch wachen. Die Bürger würden zu „digitalen Untertanen“, die Macht an sich bleibt im Verborgenen. Eine Situation, die manch einen an die vorausschauende Mahnung George Orwells vor einer fast perfekten Überwachungsgesellschaft erinnern mag. Die „Telescreens“, die die Mitteilungen der „Gedankenpolizei“ von Ozeanien verbreiteten, konnten zugleich sehen und

hören, und „man ging davon aus, dass jedes Geräusch gehört wurde und, wenn es nicht dunkel war, jede Bewegung studiert.“<sup>16</sup>



**Politik  
zwischen  
Angst haben und Mut machen**

Biometrische Merkmale machen  
uns nur so sicher, wie das  
politische System stabil ist.



Die Menschen gewinnen - Lothar Binding, MdB

## **In Deutschland Maßstäbe setzen**

Biometrische Merkmale unterstützen unsere Sicherheit also nur insoweit, wie unser politisches System so demokratisch ist, dass verlässliche Verfahren durch gesellschaftliche Kontrolle Missbrauchsmöglichkeiten hinreichend eingrenzen; deshalb lohnt es sich mit der Einführung in Deutschland nicht zu warten, bis andere Staaten die Maßstäbe gesetzt haben – auch die Steigerung unserer Sensibilität gegenüber der Einführung der neuen Techniken ist nicht nur unter rechtspolitischen Gesichtspunkten eine lohnende Aufgabe. Biometrische Merkmale sind etwas sehr Persönliches.

---

<sup>16</sup> Vgl.: [www.k-1.com/Orwell](http://www.k-1.com/Orwell)