

# Datenschutzrechtliche Aspekte bei der Aufnahme biometrischer Merkmale in Ausweispapiere

Frank Markus Abbühl

16. April 2004

Betreuung: Prof. Dr. Marie-Theres Tinnefeld,  
Dipl.-Inform. Peter Klaus Bittner

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>2</b>
1.1	Sichere neue Welt . . . . .	2
1.2	Überblick . . . . .	2
<b>2</b>	<b>Biometrische Verfahren</b>	<b>3</b>
2.1	Terminologie . . . . .	3
2.2	Betriebsarten . . . . .	3
2.3	Praktisch angewandte Verfahren . . . . .	5
2.4	Diskussion der Zuverlässigkeit . . . . .	6
2.5	Zusammenfassung . . . . .	7
<b>3</b>	<b>Recht und Ordnung</b>	<b>8</b>
3.1	Interessenlage . . . . .	8
3.2	Einordnung biometrischer Daten . . . . .	9
3.3	Terrorismusbekämpfung per Gesetz . . . . .	10
3.4	Rechtslage . . . . .	11
3.5	Zweckbestimmung . . . . .	11
3.6	Verhältnismäßigkeit . . . . .	12
3.7	Datenschutzgerechter Einsatz . . . . .	12
<b>4</b>	<b>Ausblick</b>	<b>13</b>

# 1 Einleitung

Bereits im Januar 2002 trat das Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz, TBG) in Kraft, das nach den Terroranschlägen am 11. September 2001 in einem Eilverfahren vom Deutschen Bundestag verabschiedet worden war. Es handelt sich um ein Artikelgesetz, das zahlreiche Änderungen an bestehenden Gesetzen vorsieht. In der Folge wurden sowohl im Pass- als auch im Personalausweisgesetz die rechtlichen Grundlagen für den Einsatz biometrischer Verfahren zur Identitätssicherung geschaffen.

## 1.1 Sichere neue Welt

Vor einigen Jahren noch besetzten Anbieter von biometrischen Lösungen eine Marktnische bei der Zugangskontrolle von Hochsicherheitsbereichen. Iris-Scanner und Fingerabdruck-Datenbanken kannte man bestenfalls aus Spionage- und Kriminalfilmen. Das gesteigerte Wachstum dieser Branche ist laut [Gerbich, 2002] untrennbar verknüpft mit dem erhöhten Verlangen nach Sicherheit seitdem der internationale Terrorismus in den Mittelpunkt des medialen Interesses gerückt ist.

[Jodda, 2003] berichtet, das Kanadier auf Ihren Paßfotos nicht mehr lächeln dürfen, um eine bessere Erkennungsleistung beim Abgleich mit einer internationalen Datenbank gesuchter Verbrecher zu gewährleisten. Gemäß [Union, 2003] reichen im Londoner Stadtviertel Newham flächendeckend installierte Kameraüberwachungssysteme verdächtige Personen nahtlos von einem Überwachungsbereich zum nächsten weiter, in Florida wurde ein ganzes Footballstadien mit Hilfe von Gesichtserkennungssystemen (erfolglos) nach Terroristen durchsucht und die EU-Kommission arbeitet laut [Zerbst, 2003] an der Einführung biometrischer Visa und Reisepässe. Bemühungen um eine weltweite Standardisierung biometrischer Verfahren werden von Regierungen und internationalen Organisationen wie der International Civil Aviation Organization<sup>1</sup> (ICAO) mit Hochdruck vorangetrieben.

## 1.2 Überblick

Anhand der Thematik der Arbeitsgruppe "e-Identity – wenn der Körper vermessen zur Information wird" auf der 19. Jahrestagung des FIF<sup>2</sup> unter der Leitung von Peter Bittner möchte ich in dieser Arbeit die aktuelle Diskussion in Deutschland um die Rahmenbedingungen bei der Aufnahme von biometrischen Daten in Ausweispapiere aufgreifen.

Nach einer allgemeinen Einführung in die Begriffswelt der Biometrik werde ich kurz auf die praktisch angewandten Verfahrensweisen bei der Erfassung, Verifikation und Identifikation von Personen sowie die Vielfalt biometrischer Merkmale eingehen und diesen

---

<sup>1</sup><http://www.icao.int>

<sup>2</sup>Forum InformatikerInnen für Frieden

Abschnitt mit einer Diskussion der Zuverlässigkeit und Überwindungssicherheit abschließen. Der nachfolgende Abschnitt beschäftigt sich dann eingehend mit den datenschutzrechtlichen Aspekten, die es bei der Einführung dieser Technologie in Ausweise und Pässe zu beachten gilt.

## 2 Biometrische Verfahren

Herkömmliche Authentisierungsverfahren beruhen entweder auf dem *Wissen* eines Geheimnisses (Paßwort, PIN) oder dem *Besitz* eines Gegenstandes (Schlüssel, Chipkarte). Beides kann weitergegeben, gestohlen oder verloren werden. Biometrische Verfahren hingegen beruhen laut [Lukas Gundermann, 1999] auf "physiologischen oder verhaltenstypischen Besonderheiten einer Person".

### 2.1 Terminologie

Das Lexikon definiert *Biometrie*<sup>3</sup> als "die Übertragung mathematischer Methoden [der Statistik] zur zahlenmäßigen Erfassung, Planung und Auswertung von Experimenten auf Objekte der Biologie, Medizin und Landwirtschaft" [Werner Digel, 1990]. Unter *Biometrik* versteht man "das automatisierte Messen eines oder mehrerer spezifischer Merkmale eines Lebewesens" [Micheal Behrens, 2001, S. 10].

In der einschlägigen Literatur wird der Biometrie-Begriff in einem sehr viel enger definierten Sinn verwendet, nämlich abkürzend für *biometrische Verifikation* oder *biometrische Identifikation*. Bei der Ersteren wird geprüft, ob ein Individuum seine behauptete Identität besitzt, bei der Letzteren geht es darum, "eine mittels Biometrie spezifizierte Person von anderen unterscheidbar zu machen" [Micheal Behrens, 2001, S. 10]. Wie biometrische Verfahren diese Ziele umsetzen, beschreibt der folgende Abschnitt.

### 2.2 Betriebsarten

Bevor biometrische Daten verarbeitet werden können, müssen sie erfaßt werden. Dazu wird zuerst das betreffende Merkmal mittels eines an die Charakteristik anzupassenden *Sensors* aufgenommen und digitalisiert. Ein *Merkmals-Extraktions-Algorithmus* leitet daraus die "Parameter eines mathematischen Modells der Rohdaten" [ULD, 2001, S. 14] ab, das sogenannte *Template*. Dieses dient als Referenzdatensatz für den biometrischen Vergleich. Im Gegensatz zu den Rohdaten können Templatedaten sehr platzsparend gespeichert werden, für die geometrische Bemaßung der Hand beispielsweise reichen schon wenige Byte aus.

---

<sup>3</sup> *griechisch*: bios = Leben, metrein = messen

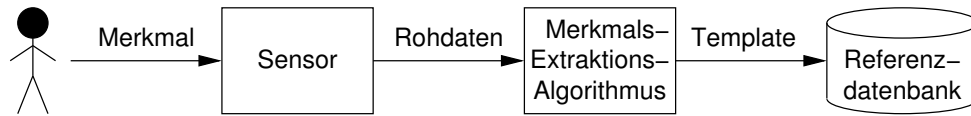


Abbildung 1: Erfassen und Einlernen der Biometriedaten

Es ist nicht möglich, anhand von Templatedaten wieder exakt auf die originalen Rohdaten zu schließen. Trotzdem stellt ein Merkmals-Extraktions-Algorithmus keine Einwegfunktion dar, denn aus dem Template lassen sich sehr leicht praktisch beliebige Rohdaten erzeugen, die bei einem neuerlichen Meßvorgang zu einer ausreichenden Übereinstimmung führen.

Die *Referenzdaten* werden bei der sogenannten *Ersterfassung*<sup>4</sup> erhoben, in der unter kontrollierten Bedingungen alle benötigten Merkmale mindestens einmal oder auch mehrfach eingelernt werden, bis eine gute Template-Qualität gewährleistet ist. Adaptive Systeme benutzen nachfolgende Messungen zur kontinuierlichen Anpassung der Referenzdaten, um beispielsweise alterungsbedingte Veränderungen eines Merkmals zu berücksichtigen.

Nun wird bei jedem Verifikationsvorgang das betreffende Merkmal erneut sensorisch erfaßt und zu Templatedaten verarbeitet. Ein *Merkmals-Vergleichs-Algorithmus* berechnet den Grad der Übereinstimmung dieser Daten mit den gespeicherten Referenzdaten. Da die gemessenen Daten nur mit dem angegebenen Referenzdatensatz verglichen werden, spricht man von einem 1 : 1 Vergleich.

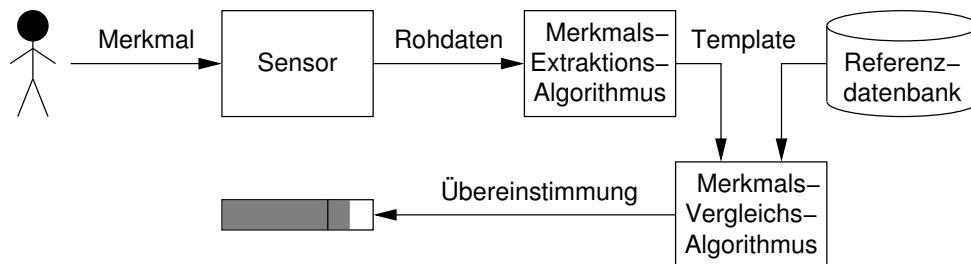


Abbildung 2: Datenfluß bei der Verifikation

Derselbe Mechanismus kann auch zur Identifikation von Personen eingesetzt werden. Hierbei werden die gemessenen Daten der Reihe nach mit einigen oder allen Referenzdatensätzen verglichen, man spricht hier daher auch von einem 1 :  $n$  Vergleich. Der Datensatz mit der besten Übereinstimmung wird der erfaßten Person zugeordnet.

<sup>4</sup> engl.: enrolment

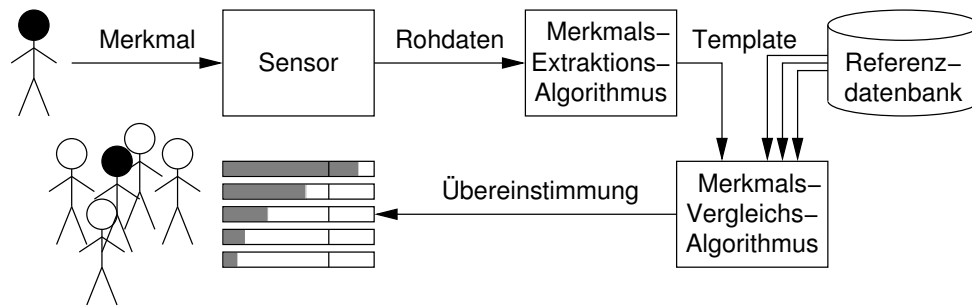


Abbildung 3: Datenfluß bei der Identifikation

### 2.3 Praktisch angewandte Verfahren

Theoretisch lassen sich die unterschiedlichsten Körpermerkmale für biometrisch erfassen, damit sie für den praktischen Einsatz in biometrischen Verfahren taugen, müssen Merkmale jedoch den folgenden in [A. K. Jain, 1999, S. 4] genannten Kriterien standhalten:

- *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.

Auf einer breiten Basis durchsetzen können sich aber nur Verfahren, die von den Benutzern tatsächlich akzeptiert werden. [Bittner, 2003] beschreibt hier zahlreiche weitere Rahmenbedingungen. Die *technische Umsetzung* eines Verfahrens muß schnell und zuverlässig arbeiten und kompatibel zu anderen Systemen sein. Die Sensoreinrichtungen müssen robust ausgelegt sein, um den Wartungsaufwand zu minimieren, und trotzdem empfindlich genug, um genaue Meßwerte zu liefern und damit die nötige Sicherheit und *Überwindungsresistenz* zu gewährleisten. Darüberhinaus muß die Realisierung für den Betreiber *ökonomisch machbar* sein und darf keine unangemessen hohen Kosten verursachen. Nicht zu vergessen die *Nutzerfreundlichkeit*, die Erfassung sollte einfach, schnell und hygienisch einwandfrei verlaufen und eventuelle Kulturelle Vorbehalte der Benutzer berücksichtigen.

Keines der heute verfügbaren Verfahren kann jede dieser Voraussetzungen vollständig erfüllen. Die in der folgenden Tabelle aus [Veronika Nolde, 2002] zusammengefaßten Merkmale und Verfahren haben sich jedoch in der Vergangenheit für unterschiedliche Einsatzgebiete bewährt. Alle zahlenmäßigen Angaben sind als grobe Schätzungen zu verstehen, da diese Werte abhängig von den Randbedingungen sehr stark variieren.

Es existiert eine unübersichtliche Vielfalt weiterer Merkmale und Verfahren, die nicht mehr in der Tabelle aufgeführt sind. Zum Beispiel wären hier die Erkennung anhand der Ohrform, der Gangart, des Körpergeruchs und der Lippenbewegung zu nennen. Diese

Merkmal	Sensorprinzip	Templategröße in Byte	Fehlerrate	Überwindungs- resistenz
Fingerabdruck	Optisch, Kapazitativ	100 - 2000	1 - 10%	gering
Gesicht	Kamera	500 - 2000	1 - 50%	gering
Iris	Spezialkamera	200 - 500	gering	hoch
Retina	Infratotkamera	100	gering	sehr hoch
Hand	Kamera	9 - 100	0.1%	mittel
Thermogramm	Infratotkamera	2000 - 4000	gering	hoch
Unterschrift	Drucksensor, Stift	300 - 2000	hoch	gering
Stimme	Mikrofon	100	1 - 5%	gering
Tastaturanschlag	Tastatur, nebenläufig	100	0.17%	hoch

Tabelle 1: Häufig eingesetzte Merkmale und Verfahren

befinden sich zum Teil noch in der Entwicklung oder wurden noch nicht in größerem Umfang eingesetzt, so daß ich keine näheren Angaben finden konnte.

Auch die an sich einfache Erfassung des Erbguts<sup>5</sup>, das eine ultimative Identifizierbarkeit verspricht und in der Kriminalistik mit großem Erfolg eingesetzt wird, eignet sich aufgrund des hohen Zeitaufwandes bei der genetischen Analyse nur schlecht. Der technische Fortschritt wird jedoch auch auf diesem Gebiet nicht halt machen.

## 2.4 Diskussion der Zuverlässigkeit

Zwei Messungen eines Merkmals liefern niemals exakt identische Ergebnisse, die Erkennung beruht immer auf einem statistischen Vergleich. Die Messergebnisse hängen ab von veränderten *Umweltbedingungen* wie Licht- oder Temperaturverhältnissen, veränderten, abgeschwächten oder fehlenden *Merkmalsausprägungen* etwa durch Brille, Bart, Mimik, Gestik, oder Verletzung sowie vom Verhalten des Benutzers wie unterschiedlichem Anpressdruck bei der Abnahme von Fingerabdrücken oder unsachgemäßer Verwendung des Sensors. Hinzu kommen mögliche Systemprobleme mit der Sonorik oder den Algorithmen.

Der Merkmals-Vergleichs-Algorithmus kann nur ein Maß für die Ähnlichkeit zwischen Referenzdaten und aktuellen Messdaten liefern. Den Wert für die Abweichung, bei der eine Person noch als identifiziert gilt, nennt man *Toleranzschwelle*.

Die relative Häufigkeit, mit der Personen fälschlicherweise vom System erkannt werden wird als *Falschakzeptanzrate*<sup>6</sup> bezeichnet, die Häufigkeit, mit der Personen irrtümlich abgewiesen werden heißt *Falschrückweisungsrate*<sup>7</sup>. Das Verhältnis beider Fehlerraten

<sup>5</sup>Desoxiribonukleinsäure (DNS)

<sup>6</sup>engl.: false acceptance rate, FAR

<sup>7</sup>engl.: false rejection rate, FRR

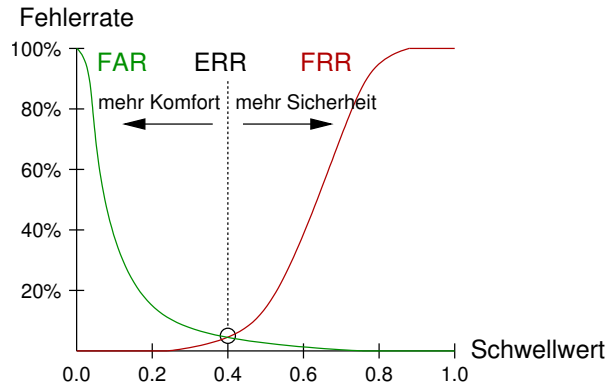


Abbildung 4: Kalibrierung der Toleranzschwelle

wird über die Toleranzschwelle eingestellt. Je niedriger die Schwelle, desto seltener kommt es zwar zu Falschakzeptanzen, aber dafür umso häufiger zu Falschabweisungen. Erschwerend kommt hinzu, daß sich die Werte nur experimentell bestimmen lassen.

Die Angaben über die Fehlerrate in der Tabelle 1 sollen lediglich einen Eindruck über die gewaltigen Schwankungsbreiten geben, sie gelten dabei jeweils für eine optimale Kalibrierung. Die optimistischen Herstellerangaben beruhen vermutlich auf Tests in kleinen Personengruppen unter bestmöglichen Bedingungen, wohingegen breit angelegte Feldversuche zu eher ernüchternden Ergebnissen kommen, wie ein vom Bundesamt für Sicherheit in der Informationstechnik<sup>8</sup> (BSI) initiiertes Vergleich von Gesichtserkennungssystemen zeigt [Busch, 2003].

Ein weiterer Aspekt der Zuverlässigkeit von biometrischen Systemen ist die *Überwindungsresistenz*. Billige Fingererkennungssysteme lassen sich schon durch einen mit Klebeband von der Tasse abgenommenen Fingerabdruck täuschen und so manches Gesichtserkennungssystem fällt auf ein vor den Kopf gehaltenes Foto herein. Daher verfügen ernstzunehmende Systeme auch immer über eine *Lebenderkennung*, indem Sie zum Beispiel die Körpertemperatur, den elektrischen Widerstand der Haut messen oder den Augenreflex abprüfen.

Durch Kombination verschiedener Verfahren kann die Falschakzeptanzrate dramatisch gesenkt werden. Gute Ergebnisse sind jedoch nur unter kontrollierten und möglichst konstanten Bedingungen erzielen. Doch sowohl Menschen als auch Maschinen lassen sich täuschen, absolute Sicherheit gibt es nicht.

## 2.5 Zusammenfassung

Dieser Abschnitt bot eine knappe Einführung in die Grundlagen der Biometrik, welche Schritte bei der Erfassung der Daten erfolgen und wie diese zur Verifikation und Identi-

<sup>8</sup><http://www.bsi.de/>

fikation von Personen herangezogen werden. Nach einem Überblick über die wichtigsten praxistauglichen Verfahren und die dabei herangezogenen Körpermerkmale folgte die Diskussion der Zuverlässigkeit, die durch Kombination und Sorgfalt durchaus ein für die meisten Anwendungsgebiete ausreichendes Niveau erreichen kann.

Biometrische Verfahren haben das Potential, in vielen Bereichen PIN, Paßwort und Chipkarte abzulösen, bieten sie doch gleichzeitig ein wesentlich höheres Maß an Bequemlichkeit und Sicherheit für den Verbraucher. Über kurz oder lang werden sie auch helfen, Personalausweise, Reisepässe und Visa fälschungssicherer zu machen, die entsprechenden Gesetzesänderungen sind bereits vollzogen.

### 3 Recht und Ordnung

In staatlichen Händen stellt der Einsatz biometrischer Verfahren ein mächtiges Instrument zur Überwachung und Kontrolle der Bürger dar. Die Euphorie über die zu erwartende Verbesserung der Sicherheitslage wird getrübt durch den bitteren Beigeschmack eines nicht unerheblichen Mißbrauchspotentials.

In diesem Abschnitt wird die Problematik bei einer gesetzeskonformen Ausgestaltung der neuen Personalausweis- und Paßgesetze behandelt. Nach einer knappen Erläuterung der Position der verschiedenen Interessengruppen und einer Darstellung der aktuellen Situation nach Umsetzung des Terrorismusbekämpfungsgesetzes folgt zunächst eine datenschutzrechtliche Einordnung von biometrischen Daten. Anschließend wird, ausgehend vom Grundgesetz und dem Persönlichkeitsrecht bis über dessen konkrete Ausgestaltung im Bundesdatenschutzgesetz, eine für alle Beteiligten tragbare Lösung nachvollzogen.

#### 3.1 Interessenlage

Mindestens drei verschiedene Interessengruppen lassen sich ausmachen: Strafverfolger, Datenschützer und Verbraucher.

Das primäre Ziel der *Strafverfolger* ist die Aufrechterhaltung von Recht und Ordnung<sup>9</sup>. So fordert beispielsweise der Bund Deutscher Kriminalbeamter [BDK, 2002] die Einführung einer zentralen Fingerabdruck-Datenbank zur effektiveren Verbrechensbekämpfung. Eine weiteres Ziel ist die Verhinderung des Mißbrauchs staatlicher Leistungen wie Kindergeld und Sozialhilfe und von Ausweis-Doppelausstellungen, wie dies im Asylbereich mit Hilfe des Ausländerzentralregisters (AZR) und dem Automatisierten Fingerabdruck-Identifikationssystem (AFIS) bereits heute praktiziert wird [ULD, 2001, S. 19]. Diese Gruppe arbeitet auch eng mit den Standardisierungsgremien zusammen.

Die *Datenschützer* hingegen fürchten um die zunehmende Einschränkung von Freiheitsrechten. Biometrische Daten lassen sich nämlich auch als Personenkennziffer verwenden

---

<sup>9</sup> engl: Law and Order

[ULD, 2001, S. 17], [Veronika Nolde, 2002, S. 120]. Gesammelte Daten können so zu lückenlosen Bewegungs- und Verhaltensprofilen zusammengeführt werden, was dem Recht auf informationelle Selbstbestimmung entgegensteht und schnell Begehrlichkeiten auf eine umfassende Überwachung der Bürger weckt.

Die Mehrheit der *Verbraucher* steht einem Einsatz biometrischer Verfahren eher unkritisch gegenüber, nach einer repräsentativen Meinungsumfrage im Auftrag von [Frank Diering, 2004] "würden 87 Prozent den Fingerabdruck im Ausweis und Reisepass akzeptieren; 74 Prozent hätten nichts gegen eine elektronische Kontrolle der Iris des Auges, und 66 Prozent würden sich [...] auch das Gesicht scannen lassen". Trotz dieser deutlichen Zahlen stoßen derlei Maßnahmen immer noch bei sehr vielen Menschen auf eine geringe Akzeptanz, da sie zum Beispiel die Entnahme von Fingerabdrücken mit der Behandlung von Kriminellen assoziieren oder die Gesichtserkennung Orwell'sche Überwachungsszenarien heraufbeschwört. Einige Personengruppen haben auch gesundheitliche<sup>10</sup> oder hygienische Bedenken<sup>11</sup>.

### 3.2 Einordnung biometrischer Daten

Ohne zusätzliche Informationen wie zum Beispiel Name und Geburtsdatum der betreffenden Person können Biometrische Daten auch als nicht-personenbezogen angesehen werden [Thomas Petermann, 2002, S. 87]. Sobald sich jedoch auf irgendeine Art dieser Bezug herstellen läßt sind "biometrische Daten eindeutig mit einer Person verknüpft [und] nicht nur personenbezogen sondern dauerhaft personengebunden" [Veronika Nolde, 2002, S. 117]. Eine Person kann zwar ihre Adresse und sogar ihren Namen wechseln, nicht jedoch ihren Körper.

Bei "Angaben über rassische und ethnische Herkunft, über politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben" handelt es sich nach §3 Abs. 9 BDSG um "besondere Arten personenbezogener Daten", die einem erhöhten Schutz unterliegen. Einen solchen "unerwünschten Zusatzgehalt" enthalten biometrische Rohdaten. Bilder vom Gesicht einer Person lassen beispielsweise Rückschlüsse auf Alter und ethnische Herkunft zu, Aufnahmen vom Augenhintergrund werden auch zur medizinischen Diagnose von Krankheiten wie Arteriosklerose, Diabetes oder Bluthochdruck eingesetzt [Veronika Nolde, 2002, S. 118], Fingerabdruck und Handgeometrie scheinen statistisch mit dem Auftreten von Leukämie und Brustkrebs zu korrelieren, auch von einem eventuellen Zusammenhang mit Homosexualität ist die Rede [ULD, 2001, S. 16]. Zwar werden die Rohdaten üblicherweise nicht dauerhaft gespeichert, dennoch werden sie sowohl bei der Ersterfassung als auch bei jedem Verifikations- oder Identifikationsvorgang erhoben und möglicherweise auch zur Auswertung an andere Stellen übermittelt.

---

<sup>10</sup>beispielsweise die fälschliche Annahme, daß die Iris per Laser abgetastet wird

<sup>11</sup>Statistisch ist bei Japanern diese Empfindung besonders ausgeprägt [Veronika Nolde, 2002, S. 40]

Templatedaten sind nach derzeitigem Wissensstand frei von derlei Zusatzgehalt, andererseits wurden aber auch noch keine ausreichend großen Datenmengen statistisch ausgewertet um dies zu beweisen oder zu widerlegen. Im Zusammenhang mit Ausweisdokumenten kann man davon ausgehen, daß man es mit personenbezogenen Daten im Sinne des §3 Abs. 1 BDSG zu tun hat.

### 3.3 Terrorismusbekämpfung per Gesetz

Von den Gesetzesänderungen in Folge des Terrorismusbekämpfungsgesetzes (TBG) sind unter anderem die §§ 4 und 16 des Passgesetzes (PassG) und gleichlautend die §§ 1 und 3 des Personalausweisgesetzes (PersAuswG) betroffen:

”Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. [...]

Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form [...] sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet.”

[...] ”Im Pass enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden. Auf Verlangen hat die Passbehörde dem Passinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen.”

Trotz dieser auf den ersten Blick datenschutzrechtlich einwandfreien Regelungen läßt dieses Gesetz noch große Spielräume bei der konkreten Ausgestaltung zu. Es fehlt eine genauere Spezifikation, welches Merkmal verwendet wird und ob lediglich Templates oder auch Rohdaten gespeichert werden sollen. Das erwähnte Bundesgesetz wurde bisher noch nicht erlassen. Das BSI empfiehlt Gesichtserkennung, Fingerabdruck und Irisscan, letztere wird merkwürdigerweise durch die Formulierung des Gesetzestextes ausgeschlossen.

Zugutehalten muß man dem Gesetz, daß eine zentrale Speicherung von Daten explizit nicht vorgesehen ist – auch wenn sich dezentrale Datenbestände zum Beispiel im Rahmen einer Rasterfahndung zusammenführen lassen – und daß der genaue Zweck genannt wird: die Prüfung der Echtheit des Dokuments und der Identität<sup>12</sup> des Inhabers. Weiterhin steht dem Ausweisinhaber ein Auskunftsrecht zu.

---

<sup>12</sup>Gemeint ist die Authentizität

### 3.4 Rechtslage

Mit dem neuen Paß- und Personalausweisgesetz hat der Gesetzgeber "die Rechtsgrundlage für die Aufnahme biometrischer Merkmale in Pässe und Personalausweise geschaffen" [Laßman, 2002, S. 38]. Damit entfällt bei der praktischen Umsetzung dieses Vorhabens zwar die Notwendigkeit der Einwilligung des Betroffenen, der Gesetzgeber muß aber weiterhin Aspekte der Menschenwürde und Verhältnismäßigkeit beachten.

Im Volkszählungsurteil [BVerfGE 65, 1] wird sehr genau beschrieben, wann bei einer Datenerhebung Persönlichkeitsrechte verletzt werden, nämlich erst wenn die Möglichkeit besteht, Datenbestände zu einem Persönlichkeitsprofil zusammenzuführen. Das Büro für Technikfolgen-Abschätzung<sup>13</sup> (TAB) kommt daher zu dem Schluß, daß "die Erhebung und Verarbeitung eines einzelnen, isolierten biometrischen Merkmals keinen Verstoß gegen die Menschenwürde darstellt" [Thomas Petermann, 2002, S. 89]. Gleichzeitig verbietet sich damit aber auch eine zentrale Speicherung, da genau diese Art der Zusammenführung bei Verwendung der biometrischen Daten im Sinne einer Personenkennziffer möglich wäre.

Problematisch sind weiterhin Verfahren wie die Gesichts- oder Bewegungserkennung, die keine aktive Mitwirkung der zu erfassenden Person benötigen. Solche Daten dürfen nach §4 Abs. 1 BDSG nur mit Rechtsgrundlage oder unter sehr speziellen Voraussetzungen erhoben werden. Solange keine weitergehenden "Überwachungsgesetze" verabschiedet werden – was auch nicht zu erwarten ist – kommen nur Verfahren in Frage, "die einen Körperkontakt oder eine spezielle Haltung des Körpers erfordern" [ULD, 2001, S. 10]. Andererseits könnte man die Menschenwürde gerade dann als verletzt ansehen, wenn "der Einzelne gezwungen [ist], seinen Körper in einer vorgegebenen Weise einzusetzen" [Lukas Gundermann, 1999, S. 6], weil er dadurch zum Objekt degradiert würde.

### 3.5 Zweckbestimmung

Im Sinne des in §3a BDSG geregelten Grundsatzes der Datenvermeidung und Datensparsamkeit dürfen ausschließlich Daten gespeichert werden, die dem im Pass- und Personalausweisgesetz festgelegten Zweck der "Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers" erfüllen. Damit kommt auch eine Speicherung der ohnehin sehr sensiblen Rohdaten aufgrund deren möglichen Zusatzgehaltes [Veronika Nolde, 2002, S. 119] nicht in Frage, zumal sämtliche biometrische Verfahren mit den reinen Templatedaten als Referenz funktionieren. Die bei jeder Erfassung angefallenen Rohdaten müssen sofort nach der Verarbeitung durch den Merkmals-Extraktions-Algorithmus gelöscht werden.

Biometrische Verfahren eignen sich per Definition zu Zwecken der Identitätssicherung im Sinne der oben beschriebenen Verifikation. Allerdings bieten sie erst bei der Kombination unterschiedlicher Merkmale eine ausreichende Erkennungsleistung. Der Gesetztestext in

---

<sup>13</sup><http://www.tab.fzk.de>

seiner aktuellen Formulierung schließt jedoch genau diese Kombination aus, ebenso wie weitere brauchbare Verfahren wie zum Beispiel die Iriserkennung. "Das Gebot der Geeignetheit verlangt [...] den Einsatz solcher Mittel, mit denen der gewünschte Erfolg am ehesten gefördert werden kann" [Thomas Petermann, 2003, S. 95].

Der Einsatz kryptographischer Verfahren, insbesondere der digitalen Signatur, eignet sich zum Zwecke der Echtheitsprüfung der Ausweisdokumente sowie zur Wahrung der Vertraulichkeit der gespeicherten Daten. Die dadurch verlorengegangene Transparenz für den Inhaber wird durch ein explizit genanntes Auskunftsrecht ausgeglichen. Als problematisch erweisen könnte sich die gesetzliche Beschränkung des Gültigkeitszeitraumes digitaler Signaturen auf 5 Jahre [Thomas Petermann, 2003, S. 100] bei einer Gültigkeitsdauer der Ausweise von 10 Jahren bei Erwachsenen ab dem 26. Lebensjahr.

### **3.6 Verhältnismäßigkeit**

Der Grundsatz der Verhältnismäßigkeit wird genau dann gewährleistet, wenn die Mittel geeignet sind, kein milderes Mittel existiert und das Übermaßverbot eingehalten wird [Lukas Gundermann, 1999, S. 7]. Die Geeignetheit wurde bereits im obenstehenden Abschnitt diskutiert.

Die nötige Milde der Mittel erfüllen alle Verfahren, die die weiter oben genannten Bedingungen genügen. Der Einsatz von Gesichtserkennung verstößt meines Erachtens gegen das Gebot der Direkterhebung, da keine aktive Mitwirkung der zu erfassenden Person notwendig ist. Seltsam erscheint auch hier, daß der Gesetzgeber nicht den Irisscan mit einbezogen hat, der in dieser Hinsicht sogar besser geeignet ist als die der Fingerabdruck, den jeder Mensch unbemerkt hinterläßt.

Die von vorneherein ausgeschlossene Möglichkeit zur zentralen Speicherung hingegen würde durch die sich daraus ergebende Möglichkeit zur Identifikation von Personen eine krasse Überschreitung des Übermaßverbotes darstellen. Dies stünde in keinem angemessenen Verhältnis zum Gesetzeszweck.

### **3.7 Datenschutzgerechter Einsatz**

Die Aufnahme biometrischer Daten in Ausweise und Pässe ist trotz der Bedenken von Datenschützern nicht mehr abzuwenden, doch damit mit Hilfe dieser sensiblen Daten keine Persönlichkeitsrechte verletzt werden können, bedarf es besonderer Umsicht. Eine zentrale Speicherung der Daten aller Bürger kommt keinesfalls in Frage, ebensowenig die Auswertung unbemerkt zu erfassender Merkmale. Zum Zwecke der Fälschungs- und Identitätssicherung genügt die Speicherung von Templatedaten auf dem Ausweispapier selbst, so daß die Daten in der Verfügungsgewalt des Inhabers verbleiben und somit dem Grundsatz der informationellen Selbstbestimmung entsprechen.

Auf der Ebene des technischen Datenschutzes sind sogar Chipkarten realisierbar, "auf denen die gesamte biometrische Datenverarbeitung abläuft und die vollständigen Referenzdaten gespeichert sind" [Marit Köhntopp, 1999, S. 10]. Mit Hilfe kryptographischer Verfahren wie der digitalen Signatur kann die Authentizität der Karte gewährleistet werden. Damit entfielen auch die besondere Problematik bei der Verarbeitung der Rohdaten. Richtig angewendet muß die "Biometrie nicht als Feind der [informationellen Selbstbestimmung]<sup>14</sup>, sondern als deren Freund angesehen werden" [Lukas Gundermann, 1999, S. 3].

## 4 Ausblick

Nachdem nun sowohl die unterschiedlichen Anwendungsmöglichkeiten und Probleme als auch die rechtlichen Aspekte bei der Verwendung biometrischer Verfahren zur Sicherung von Ausweispapieren bekannt sind möchte ich zum Schluß noch einen Blick in die Zukunft wagen.

Aus der von Woodward und anderen erhofften Balkanisierung<sup>15</sup> der Verfahren ist nach [Lukas Gundermann, 1999] nichts geworden. Im Gegenteil, die G8-Staaten und Industrieverbände treiben eine internationale Standardisierung der Verfahren im Rahmen des BioAPI Consortium<sup>16</sup> mit Hochdruck voran. [Thomas Petermann, 2002, S. 48]. Die logische Konsequenz dieser Standardisierung ist die Bildung eines weltweiten Verbundes zur noch effektiveren Bekämpfung des internationalen Terrorismus [ULD, 2001, S. 19]. Doch wer kann da noch garantieren, daß niemand im Ausland die Sammlung der sensiblen biometrischen Daten übernimmt? Der Begriff der zentralen Speicherung bekommt hier globalen Charakter.

Dagegen wirkt das Phänomen des *Information Creep* geradezu harmlos. In den USA war die Sozialversicherungsnummer<sup>17</sup> ausdrücklich nicht zur Identifikation vorgesehen, heute wird sie praktisch überall als Personenkennziffer genutzt [Veronika Nolde, 2002, S. 131]. Ebenso ist anzunehmen, daß mit solche Daten auch privater Handel betrieben wird, ähnlich wie dies bereits mit Email- und Postadressen geschieht. Besonders Kaufhäuser mit ihren umfassenden Kamerüberwachungssystemen und Kundenkartensystemen könnten besonderes Interesse daran zeigen.

Wunderbare Möglichkeiten eröffnen sich auch in Kombination mit der aufkommenden *Radio Frequenz Identifikation* (RFID). Die als Nachfolger des Strichcode gehandelten Miniatur-Transponder bieten bereits heute genügend Speicherkapazität, um biometrische Templates zu speichern und sprichwörtlich im Vorbeigehen auszulesen. "In Visa

---

<sup>14</sup> *engl.*: privacy

<sup>15</sup> Viele proprietäre Einzellösungen

<sup>16</sup> <http://www.bioapi.com>

<sup>17</sup> *engl.*: social security number

und Pässen soll RFID noch in diesem Jahr ausprobiert werden. Das wird ein Mega-Thema für den Datenschutz” [Zeidler, 2004].<sup>18</sup>

## Literatur

S. Pankanti (Eds.) A. K. Jain, R. Bolle. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1999.

BDK. Bdk fordert zentrale erfassung von fingerabdrücken, Aug 2002. URL <http://www.bdk.de>.

Peter Bittner. 19. jahrestagung. In *e-Identity - wenn der Körper vermessen zur Information wird*. FIFF e.V., Okt 2003.

Detlef Borchers. Reisepass mit rfid-chip. *Newsticker*, 03 2004. URL <http://www.heise.de/newsticker/meldung/45780>.

Christoph Busch. Bioface - vergleichende untersuchung von gesichtserkennungssystemen. Technical report, Bundesamt für Sicherheit in der Informationstechnik (BSI), Jun 2003. URL <http://www.bsi.bund.de/fachthem/BioFace/BioFaceIIBericht.pdf>.

BVerfGE 65, 1. Volkszählungsurteil, Dez 1983.

Hans-Jürgen Leersch Frank Diering. Bereit zur kontrolle. *Die Welt*, Mär 2004.

Sandra Gerbich. Das große daumendrücken. *Information Week*, Jan 2002.

Bettina Jodda. Bitte nicht lächeln! - wir sind kanadier. *Telepolis*, Sep 2003.

Dr. G. Laßman. Bewertungskriterien zur vergleichbarkeit biometrischer verfahren. Technical report, TeleTrust Deutschland e.V., Jul 2002. URL [http://www.teletrust.de/down/kritkat\\_2-0.zip](http://www.teletrust.de/down/kritkat_2-0.zip).

Marit Köhntopp Lukas Gundermann. Biometrie zwischen bond und big brother - technische möglichkeiten und rechtliche grenzen. *Datenschutz und Datensicherheit (DuD)*, 1999. URL <http://www.koehntopp.de> FIXME.

Patrick Horster Marit Köhntopp. *Sicherheitsinfrastrukturen*, chapter Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren. Viewig, 1999.

Richard Roth Micheal Behrens. *Biometrische Identifikation - Grundlagen, Verfahren, Perspektiven*. Vieweg, 2001.

---

<sup>18</sup>Nachtrag: Die Bundesdruckerei ”hat auf der CeBIT (Halle 17, Stand C36) den Reisepass mit eingearbeitetem RFID-Chip vorgestellt sowie die entsprechenden Lesegeräte und Prüfanlagen” [Borchers, 2004].

- Arnold Sauter Thomas Petermann. Biometrische identifikationssysteme, sachstandsbericht. Technical Report 76, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Feb 2002. URL <http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf>.
- Arnold Sauter Thomas Petermann, Constanze Scherz. Biometrie und ausweisdokumente. leistungsfähigkeit, politische rahmenbedingungen, rechtliche ausgestaltung, sachstandsbericht 2. Technical Report 93, Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Dez 2003. URL <http://www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf>.
- ULD. Positionspapier zum antiterrorgesetz der bundesregierung, Dez 2001. URL <http://www.datenschutzzentrum.de/material/themen/divers/antiterr.pdf>.
- Humanistische Union. Mehr sicherheit durch biometrie. *Reader zur Fachanhörung Bündnis 90/Die Grünen*, Mai 2003. URL <http://files.humanistische-union.de/2003/2003-05,biometrie,reader.pdf>.
- Lothar Leger Veronika Nolde. *Biometrische Verfahren. Körpermerkmale als Passwort. Grundlagen, Sicherheit und Einsatzgebiete biometrischer Verfahren*. Deutscher Wirtschaftsdienst, 2002.
- Gerhard Kwiatkowski Werner Digel. *Meyers großes Taschenlexikon*, chapter Biometrie. B.I.-Taschenbuchverlag, 3. auflage edition, 1990.
- Markus Zeidler. Rfid: Der schnüffel-chip im joghurtbecher. *MONITOR*, 513, Jan 2004. URL [http://www.wdr.de/tv/monitor/pdf.phtml?myP=040108f\\_rfid.pdf](http://www.wdr.de/tv/monitor/pdf.phtml?myP=040108f_rfid.pdf).
- Johannes Zerbst. Europäer sollen biometrisch erfasst werden. *Telepolis*, Jun 2003. URL <http://www.heise.de/tp/deutsch/inhalt/te/14959/1.html>.