

HUMBOLDT-UNIVERSITÄT ZU BERLIN
Institut für Informatik
Rudower Chaussee 25
12489 Berlin

Elisa Jasinska

BIOMETRIE UND DATENSCHUTZ

Proseminar Informationelle Selbstbestimmung
bei Peter Bittner



Berlin, den 23.05.2005

Inhaltsverzeichnis

1	Biometrie	3
1.1	Biometrische Merkmale	3
1.1.1	Eigenschaften	3
1.2	Anforderungen an biometrische Systeme	4
1.2.1	Technische Umsetzbarkeit	5
1.2.2	Robustheit	5
1.2.3	Ökonomische Machbarkeit	6
1.2.4	Nutzerfreundlichkeit	6
1.3	Grundbegriffe biometrischer Systeme	7
1.3.1	Enrollment und Template	7
1.3.2	Verifikation – 1 : 1 Vergleich	7
1.3.3	Identifikation – 1 : n Vergleich	8
1.3.4	Fehlerraten	8
1.4	Beispiele biometrischer Merkmale	10
1.4.1	Fingerbild	10
1.4.2	Gesicht	11
1.4.3	Iris	11
1.5	Biometrie in der Praxis	12
1.5.1	Zugangssicherung	12
1.5.2	Personenidentifikation	12
1.5.3	Gerätezugangskontrolle	13
1.5.4	Zugang zu Informationen und Dienstleistungen	13
1.5.5	Conveniencebereich	13
2	Datenschutz	13
2.1	Personenbezogene Daten	14
2.1.1	Biometrische Daten als personenbezogene Daten	14

2.1.2	Rechtliche Konsequenzen	15
2.1.3	Sensitive Daten	16
2.2	Datenerhebung	17
2.2.1	Gewinnung von Daten unter Mitwirkung des Betroffenen	17
2.2.2	Gewinnung von Daten mit Wissen des Betroffenen . . .	17
2.2.3	Gewinnung von Daten ohne Kenntnis des Betroffenen .	17
2.3	Datensparsamkeit und Datenspeicherung	18
2.4	Systemdatenschutz	19
2.4.1	Anonymisierte und pseudonymisierte Biometrie	19
2.5	Sicherheit und Zuverlässigkeit	20
2.5.1	Lebenderkennung	20
2.5.2	Überwindung	21
3	Fazit	21

1 Biometrie

Biometrie ist die Vermessung von Lebewesen und ihren Eigenschaften. Das Wort Biometrie ist aus dem griechischen abgeleitet, *bios* Leben und *metron* Maß.

„Aus einzelnen oder einer Kombination von biometrischen Daten wird auf eine Person geschlossen. Diese kann sich authentifizieren (aus einem definierten Personenkreis), etwa gegenüber Zugangsbeschränkungen, oder sie wird identifiziert (aus einem undefinierten Personenkreis).“ (vgl. [Wiki])

1.1 Biometrische Merkmale

Biometrische Merkmale stellen Eigenschaften eines Menschen dar, die vermessen werden können. Diese Merkmale kann man in zwei Gruppen unterteilen. Zum einen passive, die durch physiologische Eigenschaften bestimmt werden, zum anderen die verhaltensabhängigen, bei denen der Mensch aktiv werden muß.

Zur biometrischen Erfassung geeignete passive Eigenschaften sind zum Beispiel das Gesicht, die Iris und Retina des menschlichen Auges. Weiterhin gehören Fingerabdrücke und die Handgeometrie zu den physiologischen Merkmalen.

Aktive Merkmale beruhen auf der Analyse von Bewegungen und Verhaltensmustern. Beispiele für aktive Merkmale sind Unterschrift, Gestik und Gang. Auch das Tippverhalten und die Stimme zählen zu den verhaltensabhängigen Größen.

1.1.1 Eigenschaften

Die biometrischen Merkmale müssen zahlreiche Anforderungen erfüllen, um eine optimale Nutzbarkeit im Rahmen des biometrischen Verfahren zu gewährleisten. (vgl. [TAB02] S. 18, nach A. Jain 1999)

- **Universalität**
Das jeweilige Merkmal muß bei jedem Menschen vorhanden sein, damit durch das System eine möglichst große Gruppe erfaßt werden kann. Das Fehlen eines Merkmals bei Einzelnen würde die weitreichende Nutzung unmöglich machen.
- **Einzigartigkeit**
Weiterhin muß die gemessene Merkmalsausprägung einzigartig sein, um auch in einer sehr großen Gruppe die Individuen deutlich voneinander unterscheiden zu können.
- **Beständigkeit**
Da die umfassende Tauglichkeit des Verfahrens stark beeinträchtigt wird, wenn sich das Merkmal ändert, muß eine gewisse Beständigkeit gefordert werden, um den Aufwand des wiederholten *Enrollments* (siehe Kapitel 1.3.1.) zu minimieren.
- **Erfaßbarkeit**
Das auszuwertende Merkmal muß durch ein technisches System meßbar sein, um die biometrische Erfassung überhaupt möglich zu machen.

1.2 Anforderungen an biometrische Systeme

Ein biometrisches System besteht in der Regel aus einem Sensor, einer Verarbeitungseinheit, einem Vergleicher, einer Ausgabereinheit sowie ggf. einer Datenbank.

Der Sensor dient zur Aufnahme des Merkmals, zum Beispiel kapazitive oder optische Sensoren zur Fingerabdruckerkennung oder Kameras zur Gesichtserfassung. Die Verarbeitungseinheit bekommt das Bild vom Sensor, führt Filteroperationen aus und extrahiert die Merkmale, um sie an den Vergleicher zu senden. Der Vergleicher überprüft die aufgearbeiteten Sensordaten mit den Datenbankeinträgen und leitet das Ergebnis des Vergleichs an die Ausgabereinheit weiter.

Ein System für die Personenerkennung mittels biometrischer Merkmale hat in der Praxis einige Kriterien zu erfüllen, nach denen sich die Alltagstauglichkeit beurteilen läßt. (vgl. [TAB02] S. 18, nach Behrens/Roth 2001)

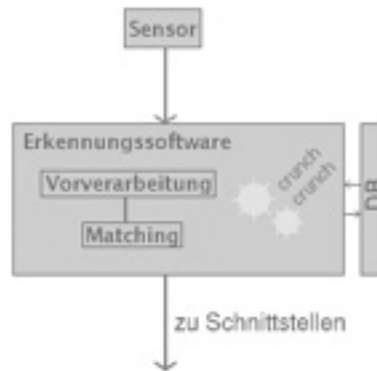


Abbildung 1: Aufbau biometrischer Systeme [FifF04]

1.2.1 Technische Umsetzbarkeit

Eine der zentralen Anforderungen ist selbstverständlich die technische Umsetzbarkeit. Insbesondere sind hier die Erfassungsgeschwindigkeit und die Kompatibilität von Bedeutung. Wenn ein System eine sehr niedrige Erfassungsgeschwindigkeit vorweist, ist eine komfortable Verwendung des Systems im Alltagsbetrieb ausgeschlossen, da es zu unzumutbaren Verzögerungen bei der Identifizierungsprozedur kommt. Die Kompatibilität der Teilkomponenten des Systems und der existierend Infrastruktur ist ein weiterer wichtiger Aspekt bei der Praxisumsetzung. Hierfür ist es von Vorteil, daß die Komponenten alle auf der Basis von offenen Standards zusammenarbeiten.

1.2.2 Robustheit

Ein weit einsetzbares System zur biometrischen Erfassung und Identifikation muß, wie alle komplexeren technischen Systeme, eine gewisse Robustheit aufweisen, um sich für den täglichen Einsatz zu eignen. Ein robustes System sollte einen geringen Wartungsaufwand genauso mitbringen wie eine geringe Empfindlichkeit gegen Umwelteinflüsse und Schäden, die durch den alltäglichen Gebrauch entstehen können. Gleichzeitig muß die Sensorik des Systems aber auch empfindlich genug sein, um eine für den Datenvergleich geeignete und möglichst fehlerfreie Erkennung zu liefern. In direktem Zusam-

menhang mit der Erkennungsgenauigkeit ist auch die Überwindungsresistenz zu sehen. Das meint hier die Überwindungssicherheit gegen Angriffe mit unrechtmäßig erlangten Merkmalen, wie abgetrennten Fingern (dies musste ein malaysischer S-Klasse Fahrer kürzlich erleben (vgl. [SKLASSE])), mit nachgeahmten Merkmalen (durch Beschaffung des Fingerabdrucks) oder Angriffe auf den technischen Unterbau und das *Backend* der Systeme.

1.2.3 Ökonomische Machbarkeit

Für einen umfangreichen Einsatz eines biometrischen Systems ist der ökonomische Faktor von entscheidender Bedeutung. Ein System, dessen Anschaffung aber das Budget der meisten Organisationen übersteigt, wird genauso wenig praktische Anwendung finden wie ein System, dessen Erkennung fragwürdig ist. In welchem Rahmen sich die Kosten der Anschaffung und Unterhaltung eines Systems bewegen, ist sowohl von der Aufgabe des Systems bzw. dem damit zusammenhängenden Schutzbedürfnis verbunden, als auch mit der Anzahl der Systeme, die angeschafft werden sollen.

1.2.4 Nutzerfreundlichkeit

Die allgemeine Akzeptanz der biometrischen Identifikationssysteme seitens der Nutzer ist ganz entscheidend von der Benutzerfreundlichkeit der Systeme abhängig. Um eine möglichst hohe Nutzerakzeptanz zu erreichen, muß das System vor allem einfach zu bedienen und gesundheitlich unbedenklich sein. Ein komplexes System führt dazu, daß ein großer Aufwand nötig ist, um neue Nutzer mit dem System bzw. der Anwendungsprozedur vertraut zu machen. Bei kontaktbehafteten Systemen kommt die Sensorik mit einer großen Zahl an Menschen in kurzer Zeit in direkten Kontakt. Daher ist Hygiene ein wichtiger Faktor eines solchen Systems. Dies wird umso wichtiger, je mehr Menschen mit dem System in Kontakt kommen.

1.3 Grundbegriffe biometrischer Systeme

Wesentliche Begriffe wie Enrollment, Template, Verifikation, Identifikation und Fehlerraten spielen eine zentrale Rolle bei biometrischen Systemen. Im folgenden Teil werden diese Begriffe genauer erläutert.

1.3.1 Enrollment und Template

Enrollment ist das erstmalige Aufnehmen des biometrischen Merkmals der zukünftigen Nutzer in das System. Dabei entstehen zunächst die *Rohdaten*. Diese werden, unter anderem aus Kapazitätsgründen, auf die für die biometrische Erkennung relevanten Daten reduziert; bei diesem Vorgang entsteht der komprimierte *Referenzdatensatz*. Die generierten *Referenzdatensätze* werden als *Templates* bezeichnet, welche die für das verwendete System und die von diesem verwendeten Merkmale relevanten Informationen enthalten. (vgl. [TAB02] S. 19) Daher kann zum Beispiel aus dem *Template* eines Fingerabdruckes kein vollständiger Abdruck rekonstruiert werden. (vgl. [TAB02] S. 23)

Vor allem muss dabei darauf geachtet werden, dass verschiedene *Rohdaten* auch verschiedene *Templates* erzeugen. Bei der Ohrmuschelerkennung von Inarelli mit 4 Werten an 12 Messpunkten lassen sich zum Beispiel nur 4^{12} (ca. 16,7 Mio.) verschiedene *Templates* beschreiben. Somit gibt es Menschen mit höchstwahrscheinlich verschiedenen Ohrmuscheln, allerdings mit identischen *Templates*. (vgl. [TABGA01] S.11)

1.3.2 Verifikation – 1 : 1 Vergleich

Die Daten des Nutzers werden von der Sensorik des Systems erfasst und verarbeitet, um mit dem Datensatz dieser Person verglichen zu werden, die Identität wird *verifiziert*. Es findet ein direkter 1:1 Vergleich statt. Ein vorstellbarer Anwendungsbereich ist die Identitätsüberprüfung anhand von Ausweisdokumenten. Der Vorteil der *Verifikation* liegt in der Möglichkeit der dezentralen Speicherung des Templates in der Verfügungsgewalt des Nutzers, wobei keine eventuell datenschutzrechtlich bedenklichen Datenbanken

entstehen. (vgl. [TAB02] S. 20)

1.3.3 Identifikation – 1 : n Vergleich

Eine Person wird im System erfaßt und seine Daten mit einer Datenbank von Templates verglichen. Damit wird die *Identität* des Nutzers festgestellt, sofern sich ein Template des entsprechenden Merkmals in der Systemdatenbank befindet. Ist dies nicht der Fall, wird der Nutzer abgewiesen. Es findet ein 1:n Vergleich statt, welcher je nach Anordnung der Daten in der Datenbank, einen höheren Zeitaufwand bei der *Identifikation* bedeuten könnte, als bei der Verifikation. (vgl. [TAB02] S. 20)

1.3.4 Fehlerraten

Idealerweise sollte der Datensatz eines biometrischen Systems immer einzigartig für die vermessene Person sein. Durch verschiedene Einflüsse kann dieses ideale Ergebnis jedoch nie erreicht werden.

Bei den Messungen herrschen niemals dieselben Bedingungen. So unterliegen, durch äußere Einflüsse wie zum Beispiel unterschiedliche Positionen des Fingers, verschiedene Wetterbedingungen oder Verunreinigungen des Sensors, die Meßdaten Schwankungen. Weiterhin werden aus Kapazitätsgründen schon bei der Speicherung des Templates viele Informationen weggelassen.

Somit findet immer ein statistischer Vergleich des Templates mit den Daten statt, die in der aktuellen Messung ermittelt wurden. Das Ergebnis dieses Vergleichs ist ein Prozentsatz an Übereinstimmung.

Daher muß für jedes biometrische System eine Toleranzschwelle festgelegt werden, ab welcher der Authentifizierungsversuch akzeptiert bzw. abgelehnt wird (so wird z. B. bei 95% Übereinstimmung der Messung mit dem Template akzeptiert). Diese Toleranzschwelle hat maßgeblichen Einfluß, wie viele Nutzer fälschlicherweise akzeptiert werden oder aber fälschlicherweise zurückgewiesen werden. (vgl. [TAB02] S. 21)

- **False Rejection Rate (FRR)**

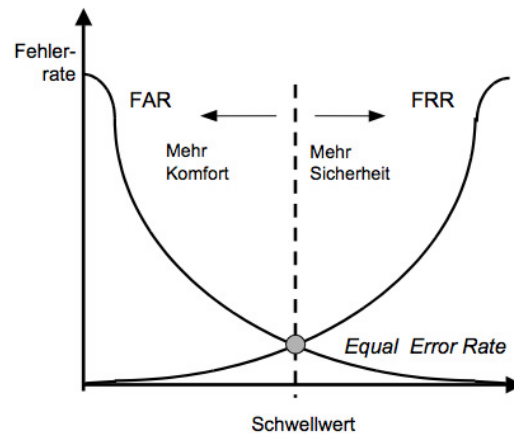


Abbildung 2: FAR und FRR in Abhängigkeit [KritKat] S. 14

Je kleiner die Rate falscher Ablehnungen ist, desto höher ist der Komfort für den Nutzer, da er nicht mehrmals versuchen muß, in dem System erkannt zu werden. Eine geringe FRR hilft auch, damit die Nutzer Vertrauen in das System entwickeln können.

- **False Acceptance Rate (FAR)**

Die Rate falscher Akzeptanz ist für die Sicherheit, die ein biometrisches System liefern kann, von entscheidender Bedeutung. Jede zu unrecht akzeptierte Person kompromittiert die Sicherheit des Systems.

Die FAR und FRR beeinflussen sich gegenseitig, eine Absenkung der falschen Akzeptanz hat eine Erhöhung der falschen Zurückweisung zur Folge. (siehe Abbildung 2)

- **Equal Error Rate (EER)**

Wenn False Rejection Rate (FRR) und False Acceptance Rate (FAR) gleich sind, spricht man von einer Equal Error Rate. In diesem Fall ist die Balance zwischen Sicherheit und Komfort ausgewogen (kleinster gemeinsamer Fehler). Allerdings kann es für bestimmte Anwendungen (z.B. solche mit sehr hohen Sicherheitsanforderungen) nötig sein, die Balance zu einer Seite zu verschieben; mit den damit verbundenen Nachteilen.

- **False Enrollment Rate (FER)**

Die Rate fehlerhafter Enrollmentversuche, d. h. die Menge an Personen, die nicht vermessen werden können, da die erfaßten Merkmale nicht stark genug ausgeprägt bzw. nicht vorhanden sind. Eine zu hohe FER verhindert möglicherweise vollständig den Einsatz eines Systems, da den Nutzern, für die kein Template erstellt werden kann, eine alternative Form der Authentifizierung angeboten werden muß.

1.4 Beispiele biometrischer Merkmale

Das Paß- und Personalausweisgesetz sowie das Ausländergesetz wurden dahingehend geändert, daß die Einbringung zusätzlicher biometrischer Merkmale in Ausweisdokumente vorgenommen werden kann. Aufgrund dieser Änderungen werde ich im Folgenden die drei Merkmale beschreiben, die in diesem Zusammenhang politisch diskutiert wurden. (vgl. [TAB03] S. 76)

1.4.1 Fingerbild

Beim Fingerabdruck handelt es sich um ein einzigartiges Merkmal, daß sogar bei eineiigen Zwillingen unterschiedlich ist. (vgl. [TAB02] S. 22) Verglichen werden die Oberflächenmerkmale des Fingers, sog. Minutien, also die Punkte an denen Linien auf der Haut des Fingers zusammenlaufen.

Bei der kriminaltechnischen Erfassung der Fingerabdrücke werden große Gesamtbilder erfaßt, bei denen es sich um hochwertige Schwarzweiß-Bilder mit etwa 250 KByte pro Finger handelt. In der Templateerstellung bei der Biometrie müssen - u. a. wegen des hohen Speicherbedarfs - die Daten komprimiert werden. Daher werden im Template nur die zur Unterscheidung nötigen Merkmale gespeichert, die 250- bis 1000-mal weniger Daten enthalten als bei der kriminalistischen Methode üblich ist. Das führt auch dazu, daß der Fingerabdruck aus dem gespeicherten Template nicht vollständig rekonstruierbar ist. (vgl. [TAB02] S. 23)

Bei der Verwendung des Fingerabdrucks gibt es allerdings ein Problem, welches das Enrollment schwierig macht. Der Fingerabdruck ist bei rund 2% der

Weltbevölkerung nicht stark genug ausgeprägt für die Verwendung bei biometrischen Systemen. (vgl. [TAB03] S. 62) Zusätzlich kann durch Verletzungen, welche am Finger besonders leicht entstehen, die erfolgreiche Authentifizierung behindert werden, auch wenn der Nutzer berechtigt ist und das System normal funktioniert.

Zudem wird die Erfassung von Fingerabdrücken von den meisten Menschen mit der Strafverfolgung in Verbindung gebracht und daher auch als Einschränkung der persönlichen Freiheit empfunden. Somit gibt es ein nicht zu unterschätzendes Akzeptanzproblem bei der breiten Anwendung von Fingerabdruckererkennung als biometrisches Identifikationssystem.

1.4.2 Gesicht

Das Gesicht wird unter anderem durch Knochen, Muskulatur und Behaarung charakterisiert. Es weist eine gute Unterscheidungsrate auf, allerdings ist diese abhängig von äußerlichen Merkmalen, wie z.B. Behaarung oder Brille, die sich sehr schnell ändern lassen. Unterschiedliche Gesichtspositionen, verschiedene Lichtverhältnisse und andere Umwelteinflüsse stellen auch eine Schwierigkeit für Gesichtserkennungssysteme dar. Findet das Enrollment z. B. bei künstlichem Licht statt, können Authentifizierungsversuche bei Tageslicht fehlschlagen.

1.4.3 Iris

Die Iris ist der farbige Gewebering, der die Pupille umschließt. Sie regelt, wie eine Blende, die Weite der Pupille und somit den Lichteinfall auf die Netzhaut. Die Iris ist ein einzigartiges Merkmal. Bei einem einzelnen Menschen unterscheiden sich sogar die Iriden der beiden Augen voneinander. (vgl. [TAB02] S. 27) Als Merkmale werden beim Enrollment die Fasern, Verflechtungen und Streifen herangezogen, die Farbe wird nicht verwendet. Die Aufnahmen werden von hochauflösenden Schwarzweiß-Kameras erstellt.

Ein großer Vorteil der Iriserkennung ist, daß es sich um ein kontakloses System handelt. Somit eignet sich dieses System auch für Anwendungen, bei denen Systeme mit Benutzerkontakt hygienisch zu bedenklich wären. Als

Lebenderkennung wird oft die Reflexreaktion der Iris auf Lichteinfall herangezogen, die recht schwer zu täuschen ist. Ein entscheidender Nachteil ist die Empfindlichkeit des Systems gegenüber von Krankheiten, bei denen die Hornhaut geschädigt wird, wie der weitverbreitete Astigmatismus (Hornhautverkrümmung).

1.5 Biometrie in der Praxis

Die Anwendungsgebiete für Biometrie sind vielfältiger, als es zunächst den Anschein hat. Daher hier eine kurze Übersicht über die üblichen Einsatzgebiete. (vgl. [TAB02] S. 61-73)

1.5.1 Zugangssicherung

Die wohl klassische Anwendung der Biometrie ist die Zugangssicherung. Diese wird meist bei Gebäuden oder Geländen, wie Krankenhausapotheken, Flughäfen, Regierungseinrichtungen, Forschungsabteilungen etc. genutzt. Für diese Art der Anwendung genügt die Verifikation von Personen zur Zugangsautorisierung. Es wird ein sehr hohes Sicherheitsniveau benötigt, was zu einer hohen Rate falscher Ablehnung führen kann und somit problematisch in der Nutzerakzeptanz ist. Allerdings kann dies, aufgrund der begrenzten Nutzerzahl, durch eine Ersatz-Autorisierung kompensiert werden.

1.5.2 Personenidentifikation

Bei der Personenidentifikation wird eine Person eindeutig identifiziert. Dies stellt im Vergleich zur Verifikation sehr höhere Anforderungen an das verwendete System. Es fallen weit aus größere Datenmengen an die gespeichert und verarbeitet werden müssen, so daß hier Fragen des Datenschutzes eine besondere Rolle spielen. Vor allem steht die Personenidentifikation im Zusammenhang mit der derzeitigen Frage, Biometrie als Identitäts- bzw. Legitimationsnachweis zu nutzen.

1.5.3 Gerätezugangskontrolle

Ein schon heute relativ verbreitetes Anwendungsgebiet von einfachen biometrischen Systemen ist die Gerätezugangskontrolle, z.B. für PDAs oder PCs, Geldautomaten oder auch Mobiltelefone. Genaugenommen ist die Gerätezugangskontrolle eine Form der Zugangssicherung.

1.5.4 Zugang zu Informationen und Dienstleistungen

Es besteht auch die Möglichkeit, biometrische Systeme zur Verifikation bei E-Commerce, Electronic Banking, E-Government oder Telefonsystemen zu verwenden, wenn zum Beispiel eine Hotline mit einer Stimmerkennung zusammenarbeitet. Allerdings ist insbesondere bei Internetanwendungen fraglich wie Enrollment, Datenübermittlung usw. bewerkstelligt werden sollen.

1.5.5 Conveniencebereich

Der Conveniencebereich hat wohl das größte Potential für biometrische Anwendungen, da hier meist nur mittlere Sicherheitsanforderungen gestellt werden. Die Identifizierung von Personen mittels Biometrie hat hier eine komforterhöhende Funktion im Alltag, z. B. bei Heizungs- oder Beleuchtungsanlagen, Unterhaltungselektronik und Kraftfahrzeugen, die sich je nach Benutzer automatisch konfigurieren.

2 Datenschutz

Der erste Abschnitt des Bundesdatenschutzgesetzes (BDSG) umfasst allgemeine Bestimmungen, die beim Umgang mit schutzwürdigen Daten zu beachten sind. Auf diese Bestimmungen werde ich im folgenden Teil eingehen.

Beim Einsatz biometrischer Verfahren in der Praxis ist aus datenschutzrechtlicher Sicht ausserdem zu beachten, ob die Daten von öffentlichen oder Privaten Stellen verarbeitet werden. Im privaten Bereich ist der 3. Abschnitt

des BDSG anwendbar, die Regelungen für den öffentlichen Bereich findet man in den Landesdatenschutzgesetzen bzw. im BDSG Abschnitt 2.

2.1 Personenbezogene Daten

Laut BDSG §3 Abs.1 werden Daten, die sich bestimmten natürlichen Personen zuordnen lassen, als personenbezogene Daten bezeichnet, und stehen unter einem besonderen Schutz.

„BDSG §3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).”

Bei der datenschutzrechtlichen Bewertung in der Biometrie kommt es sehr auf technische Details an, um die verarbeiteten Daten beurteilen zu können.

2.1.1 Biometrische Daten als personenbezogene Daten

Rohdaten stellen eine elektronische Repräsentation des Abbilds des entsprechenden Merkmals dar. Ein Gesicht z. B. ist eventuell direkt personifizierbar, falls man die Person kennt; der Finger kann erst mit einer Datenbank einen Personenbezug herstellen, es müssen also weitere Informationen zugefügt werden. Daher müssen Rohdaten nicht in jedem Fall personenbezogen sein. Personenbezug im Sinne des Datenschutzrechts liegt vor, wenn es sich um Rohdaten handelt, die in der gleichen Weise auch vom menschlichen Geist für die Wiedererkennung von Personen verwendet werden. Ausserdem ist der Personenbezug gegeben, wenn Rohdaten zum Beispiel mit den klassischen Adressierungsdaten einer Personen zusammengebracht werden können, was bei verschiedensten Institutionen *legal* der Fall sein kann.

Templates werden unter Verwendung von Rohdaten durch mathematische Funktionen erzeugt. Daher besteht keine Möglichkeit, nur unter Verwendung der Template-Daten festzustellen, von welcher Person die Rohdaten für die

Templates stammen. Sie werden entweder dadurch personenbezogen, dass sie wie oben mit zusätzlichen Identifizierungs- bzw. Adressierungsinformationen zusammengebracht werden oder die Algorithmen für die Erstellung der Templates lassen eine Rückrechnung auf die Rohdaten zu. (vgl. [TABGA01] ab S. 14)

2.1.2 Rechtliche Konsequenzen

Mit dem im Volkszählungsurteil anerkannten Grundrecht auf informationelle Selbstbestimmung wird jedem garantiert, selbst über Preisgabe und Verwendung seiner persönlichen Daten bestimmen zu können. Abgeleitet wird dieses Recht aus Art. 2 GG, dem Grundrecht auf freie Entfaltung der Persönlichkeit, in Verbindung mit Art. 1 I GG. Bei der Herleitung des Rechts auf informationelle Selbstbestimmung baut das BVerfG vor allem auf die vorangegangene Rechtsprechung des Bundesgerichtshofs in Zivilsachen zum allgemeinen Persönlichkeitsrecht auf, welches durch dieses Urteil ausgeweitet wurde. Dabei bezieht sich das Urteil auf die im BDSG §3 Abs.1 enthaltene Definition personenbezogener Daten. (vgl. [TABGA01] S.18)

„Handelt es sich bei den verarbeiteten biometrischen Daten um personenbezogene Daten, so ist damit auch klargestellt, dass das (staatliche) Erheben, Verarbeiten und Nutzen der Daten einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt.“ ([TABGA01] S.18)

Daher bedarf jeder Eingriff einer rechtlichen Regelung, wie es in BDSG §4 beschrieben ist.

„BDSG §4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

2.1.3 Sensitive Daten

Bestimmte Kategorien personenbezogener Daten werden nach Art. 8 Abs. 1 EG-Datenschutzrichtlinie einem weitergehenden Schutz unterstellt. Dies sind z.B. Daten, aus denen die ethnische Herkunft hervorgeht, sowie Daten über Gesundheit oder Sexualleben, auch *sensitive Daten* genannt.

Bei einigen biometrischen Systemen ist der ermittelbare Informationsgehalt einer Erfassung größer als die Informationen, die zur Identifikation einer Person notwendig sind. Gerade aus Rohdaten, die wesentlich mehr Informationen enthalten, können z. B. Rückschlüsse auf Personen gezogen werden, die sensitive Daten beinhalten. Bei Templates, die nur die wesentlichen, zur Identifikation notwendigen Daten enthalten, ist diese Gefahr geringer, aber dennoch gegeben.

Jedes Foto einer Person oder ihr Nachname kann Informationen über die ethnische Herkunft enthalten. Aufnahmen des Augenhintergrundes lassen u.U. Diagnosen auf Krankheiten wie Arteriosklerose, Diabetes oder Bluthochdruck zu. Bei Fingerabdrücken scheint es statistische Korrelationen von Fingerabdruckmustern und Krankheiten wie chronische Magen-Darm-Beschwerden (CIP), Leukämie und Brustkrebs zu geben. (vgl. [TABGA01] S. 19 Fussnoten: 39, 40, 41)

Sogar bei pseudonymisierten biometrischen Daten können unter Umständen durch Zusammenhänge zu anderen Daten Rückschlüsse gezogen werden. Wenn z. B. eine Person im Supermarkt pseudonymisiert mit einem Iris-Scanner erfaßt wird und beim Verlassen des Ladens mit der EC-Karte bezahlt, kann ein direkter Rückschluß der ermittelten Identität auf dem Namen der Kartenzahlung gezogen werden. Je nach Ausstattung eines Bereiches mit Erfassungsgeschäften kann es sogar zu einer „Templateverfolgung“ kommen.

Bei einigen Daten stellt sich die Frage, ob die Ausnahme vom erhöhten Schutzniveau nach Art. 8 Abs. 2 lit. e Fallgruppe EG-Datenschutzrichtlinie greifen kann. Das sind z. B. Daten, die die betroffene Person *offenkundig öffentlich* gemacht hat, wie ein unverhülltes Gesicht. Bei Fingerabdruck oder Augenhintergrund kann man beispielsweise davon ausgehen, dass diese Daten nicht öffentlich gemacht werden.

Wenn es allerdings darum geht, eine Datenbank mit ethnischen Zuordnungen anzulegen, welche *nur* den Namen einer Person und Angaben zur Ethnie enthält, so erscheint diese Ausnahme fraglich. (vgl. [TABGA01] S. 20) „Dies zeigt, dass das Art. 8 EG-Datenschutzrichtlinie zugrunde liegenden Konzept insgesamt zweifelhaft ist und seine Umsetzung in deutsches Datenschutzrecht noch zu erhebliche Abgrenzungsproblemen führen wird.“ ([TABGA01] S. 20)

2.2 Datenerhebung

Aus dem Datenschutzrecht ergibt sich die Pflicht, Daten unmittelbar bei den Betroffenen und mit deren Kenntnis zu erheben. Bei biometrischen Systemen ist dem Nutzer durch seine Mitwirkung bewusst, dass Daten erfasst werden. Allerdings gibt es auch Verfahren, bei denen eine unbemerkte Datenerfassung möglich ist. (vgl. [TABGA01] S. 22)

2.2.1 Gewinnung von Daten unter Mitwirkung des Betroffenen

Dies sind Verfahren, die eine unmittelbare Beteiligung des Betroffenen an der Aufnahme notwendig machen, zum Beispiel das Auflegen eines Fingers auf einen Fingerabdrucksensor oder das Nachsprechen eines Textes für eine Spracherkennung.

2.2.2 Gewinnung von Daten mit Wissen des Betroffenen

Beispiele hierfür wäre die Aufnahme und biometrische Verarbeitung durch offen sichtbare Kamerasysteme, wenn die Betroffenen auf die Verarbeitung mit biometrischen Verfahren hingewiesen wurden.

2.2.3 Gewinnung von Daten ohne Kenntnis des Betroffenen

Hier sind vor allem Verfahren zu nennen, die berührungslos Daten erheben, so dass der Nutzer keinerlei Aufwand betreiben muss, um von dem System

bearbeitet zu werden, und so davon nichts mitbekommt, zum Beispiel Kamerasysteme, die nicht auf die biometrische Verarbeitung hinweisen, und man ohne Kenntnis erfasst werden kann.

Der Grad der Mitwirkung hängt jedoch meist von der technischen Umsetzung der Systeme ab, so dass gerade bei der Installation solcher Systeme auf eine datenschutzgerechte Anpassung Wert gelegt werden sollte.

2.3 Datensparsamkeit und Datenspeicherung

„BDSG §3a Datenvermeidung und Datensparsamkeit
Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Wenn in der Biometrie von vornherein auf unnötige Datenerhebung bzw. Datenspeicherung verzichtet wird, entstehen erst keine großen Datensammlungen, die eventuell mißbraucht werden könnten. Zum Beispiel ist es bei der bloßen Feststellung der Identität meist nicht erforderlich, die einzelnen Identifikationsvorgänge zu speichern (also die genauen Angaben zur Zeit, Ort und Häufigkeit der Vorgänge).

Wird nicht auf die Speicherung von solchen Daten verzichtet, so muß durch Zweckbindung sichergestellt werden, daß nur Daten erhoben und gespeichert werden, die tatsächlich erforderlich sind. Darüber hinaus sollte auf Speicherung von Rohdaten auf Grund des überschüssigen Informationsgehaltes (siehe Kapitel 2.1.) vollkommen verzichtet werden.

Ausserdem sollte auf eine dezentrale Speicherung der Daten geachtet werden um keine grossen Datenbanken mit biometrischen Merkmalen entstehen zu lassen. Zum Beispiel könnten die Daten persönlich aufbewahrt werden, etwa auf einer Chipkarte, so dass der Nutzer die Kontrolle über seine Daten hat.

Da die Daten allerdings von einer ausgewiesenen Stelle erhoben werden, muss darauf geachtet werden, dass diese die Rohdaten lediglich verarbeitet und anschliessend wieder löscht. Somit verbleibt nur das Template auf dem Speicherchip des Nutzers. Sollte ein Nutzer seinen Datenträger jedoch verlieren bedeutet dies, dass ein komplett neuer Enrollmentvorgang durchgeführt werden muss.

2.4 Systemdatenschutz

Der Begriff *Systemdatenschutz* umschreibt technische und organisatorische Maßnahmen, die zum Schutz des Rechts auf informationelle Selbstbestimmung gegeben sind. Hierbei handelt es nicht nicht ausschließlich um Technische Mittel wie Verschlüsselung, sondern auch auch die Möglichkeit der Datensparsamkeit, Anonymisierung oder Pseudonymisierung von Daten oder Datenschutzaudits. (vgl. [SYS])

”BDSG §9 Technische und organisatorische Maßnahmen
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.”

2.4.1 Anonymisierte und pseudonymisierte Biometrie

Anonymisierte und pseudonymisierte Biometrie sind sogenannte templatefreie Verfahren. Ihre Besonderheit liegt darin, biometrische Daten einer Person indirekt zu speichern. (vgl. [TABGA01] S.17 und [ANON03])

Verfahren:

Ein Klartext wird mittels einem aus den biometrischen Daten erzeugtem Schlüssel verschlüsselt. Nur mit denselben biometrischen Daten kann aus

dem Chifftrat wieder ein Klartext erzeugt werden, welches ein Beweis für die Authentizität der Person ist. Dabei wird überhaupt kein Personenbezug hergestellt. (Anonymes Verfahren) Gekoppelt mit einem Benutzernamen (Pseudonym) kann ein Personenbezug hergestellt werden. (Pseudonymes Verfahren)

Aus datenschutzrechtlicher Sicht sind Verfahren dieser Art zu bevorzugen, da in ihnen die Forderung des Systemdatenschutzes nach Datensparsamkeit und Datenvermeidung erfüllt werden kann.

2.5 Sicherheit und Zuverlässigkeit

Biometrische Systeme müssen, um die ihnen gestellten Anforderungen zu erfüllen, zum Teil sehr hohen Sicherheitsanforderungen genügen. Ein Mißbrauch muß weitgehend ausgeschlossen werden. Auf dem derzeitigen Stand der Technik ist dies noch bei keinem System gegeben, was zum Teil an der verfügbaren Sensorik und Software als auch an der Biometrie prinzipiell liegt.

Zum einen besteht eine Gefährdung durch die Fehlerraten, da es sich immer um einen statistischen Vergleich der Daten handelt und somit nie ein vollständig korrektes Ergebniss erzielt wird. (siehe Kapitel 1.3.4) Zum anderen bieten Systeme durch ihre Komplexität viele technische Angriffsmöglichkeiten.

2.5.1 Lebenderkennung

In einige Systeme wird bereits eine sog. Lebenderkennung oder auch *Life-Test* eingebunden, der zusätzlich zur Merkmals erfassung eine Erkennung vornimmt, um die Überwindung der Systeme mit Attrappen zu vermeiden.

Hierbei wird z.B. beim Fingerabdruck auf eine Pulsmessung zurückgegriffen. Es ist aber nicht besonders schwierig, zum Beispiel in eine Attrappe eine Puls-simulation mit einzubauen, die diese oft recht primitiven Systeme überlistet. (vgl. [DS80]) Beim Irisscan kann der Irisreflex gemessen werden, der eine abrupte Kontraktion der Pupille auslöst. Die Gesichtserkennung überprüft Reaktionen wie Bewegungen des Kopfes oder Blinzeln.

Eine Lebenderkennung ist meist nur bei passiven Systemen nötig, da diese bei vielen aktiven Merkmalen in der Natur der Erkennung selbst liegt, eine nicht lebendige Person wird wohl kaum eine Unterschrift leisten können. Allerdings gibt es auch aktive Systeme, die sich leicht überwinden lassen, wie z. B. die Stimmenerkennung mit einer Aufzeichnung.

2.5.2 Überwindung

Die Überwindungssicherheit ist bei einigen Systemen sehr gering, zum Beispiel wenn die Merkmale leicht zugänglich sind.

Zunächst ist hier der Fingerabdruck zu nennen, der überall hinterlassen wird, sogar auf den Erkennungsgeräten selbst. Manchmal reicht das Anhauchen eines Sensors, wobei zusätzliche Feuchtigkeit die Fettrückstände anreichert und den Sensor reaktiviert. Aus einem auf einer Folie ausgedrucktem Fingerabdruck und etwas Gelatine läßt sich einfach eine Attrappe herstellen. Da man Gelatine zu einer relativ dünnen Schicht verarbeiten kann, ist es möglich die Attrappe direkt auf dem eigenen Finger zu plazieren, und somit auch einen Puls für die Lebenderkennung zu simulieren. (vgl. [DS80])

Das Gesicht kann überall unbemerkt aufgenommen werden, so kann jeder, auch unbemerkt, die benötigten Daten für die Authentifizierung erlangen. Gesichtserkennungssysteme könnten teilweise mit Fotos überwunden werden, bei Varianten mit Lebenderkennung reicht meist eine Bildsequenz die von einem Laptop-Monitor aus abgespielt wird. (vgl. [DS81])

Natürlich gibt es auch Systeme, die nicht mit solch simplen Methoden überwunden werden können, zu nennen wäre hier der Iris-Scan oder die Erfassung der Retina. Allerdings ist es bestimmt nur eine Frage der Zeit und der Mühe bis dies auch möglich ist.

3 Fazit

Abschließend läßt sich feststellen, daß biometrische Systeme auf ihrem derzeitigen Entwicklungsstand noch nicht für den breiten Einsatz geeignet sind.

Die Anforderungen an biometrische Systeme decken sich nicht mit ihren Fähigkeiten in der Realität.

Leider ist festzustellen, dass der Druck zur Einführung der Systeme sehr stark ist, was dazu führt, dass viele in einem technisch noch unausgereiften Zustand in den Betrieb übergehen werden. Dies wird zu vielen eigentlich vermeidbaren Problemen führen.

Literatur

- [TAB02] Petermann, T., Sauter, A., Biometrische Identifikationssysteme, Berlin: Buero fuer Technikfolgen-Abschaetzung beim Deutschen Bundestag, Arbeitsbericht Nr. 76, 2002.
- [TAB03] Petermann, T., Scherz, C., Sauter, A., Biometrie in Ausweisdokumenten, Berlin: Buero fuer Technikfolgen-Abschaetzung beim Deutschen Bundestag, Arbeitsbericht Nr. 93, 2003.
- [DS80] Krissler, Jan, Hacking Biometric Systems, in: Die Datenschleuder, Nr. 80, S. 14.
- [DS81] Krissler, Jan, Ueberwindbarkeit von Gesichtserkennungssoftware, in: Die Datenschleuder, Nr. 81, S. 23.
- [DS82] Krissler, Jan, Biometrie in Ausweisdokumenten, in: Die Datenschleuder, Nr. 82, S. 26.
- [KritKat] TeleTrusT (Deutschland e.V.), Kriterienkatalog - Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Arbeitsgruppe 6: Biometrische Identifikationsverfahren, Stand 10.07.2002, Erfurt.
- [FifF04] Krissler, Jan: Biometrie im Kontext. Vortrag auf der 20. FifF Jahrestagung, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 30. September bis 03. Oktober 2004, Berlin, Vortrag vom 02. Oktober 2004.
- [Wiki] <http://de.wikipedia.org/wiki/Biometrie>, 29.10.2004.
- [TABGA01] Baeumler, Dr. H., Gundermann, L., Probst, Dr. T., Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kiel: Unabhaengiges Landeszentrum fuer Datenschutz Schleswig Holstein, 2001.
- [ANON03] Martini, Dr. U., Beinlich, S., Virtual PIN - Biometric Encryption Using Coding Theory, Muenchen: Neue Technologien - Technologiecenter, Giesecke & Devrient, 2003.

- [SYS] <http://www.datenschutzzentrum.de/systemdatenschutz/>,
09.05.2005.
- [SKLASSE] <http://erdgeist.org/archive/46halbe/s-klasse9.jpg>, 09.05.2005.
- [BDSG] http://bundesrecht.juris.de/bundesrecht/bdsg_1990/inhalt.html,
09.05.2005.