UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD • Postfach 71 16 • 24171 Kiel

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Die Vorsitzende
Postfach 7121

24171 Kiel

Holstenstr. 98
D-24103 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
Ansprechpartner/in:
Frau Köster
Durchwahl: 988-1216

Aktenzeichen:
LD5-73.03/99.063

Kiel, 22. Januar 2004

L 215
26.1.

Aufnahme biometrischer Daten in Ausweispapiere, Drucksache 15/2887 (neu)
Ihr Schreiben vom 5. Januar 2004; Ihr Zeichen L 215

Sehr geehrte Frau Schwalm,

als Anlage übersende ich Ihnen wunschgemäß meine Stellungnahme zu dem in der 89. Sitzung des Innen- und Rechtsasschusses am 3. Dezember 2003 beratendenen Antrag der FDP-Fraktion, Aufnahme biometrischer Daten in Ausweispapiere, Drucksache 15/2887 (neu).

Mit freundlichen Grüßen

Dr. Helmut Bäumler

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Stellungnahme
des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein

zu dem
in der 89. Sitzung des Innen- und Rechtsausschusses
am 3. Dezember 2003 (TOP 5)
beratenen Antrag der Fraktion der FDP
(Aufnahme biometrischer Daten in Ausweispapiere,
Drucksache 15/2887, neu)

1) Einleitung

Bei biometrischen Merkmalen auf Pässen und Ausweispapieren geht es um die „automatische Vermessung des Körpers". Schon in heutigen Ausweisen sind biometrische Merkmale wie Körpergröße und Augenfarbe enthalten, damit der Ausweis dem Ausweisinhaber zugeordnet werden kann. Da es schon Dokumente gibt, die zur Identitätsfeststellung von Personen dienen, kann eine Verbesserung einer solchen Identitätsfeststellung nicht von vornherein unzulässig sein. Auch wenn Risiken und Gefahren beim Einsatz biometrischer Verfahren nicht zu leugnen sind, muss dies daher nicht zwangsläufig zum Verzicht auf biometrische Merkmale in Ausweisen führen. Wesentlich aus datenschutzrechtlicher Sicht ist, dass der biometrischen Erfassung und Auswertung klare Grenzen gezogen werden, damit sie einerseits beherrschbar bleiben und andererseits höchsten Sicherheitsanforderungen genügen.

2) Funktionsweise biometrischer Verfahren

Mit dem Begriff *Biometrie* oder *biometrische Verfahren* werden Verfahren zur automatisierten Erfassung und Auswertung der Körpermerkmale und des Verhaltens von Personen bezeichnet, um diese automatisiert (wieder)erkennen zu können. Zu den derzeit auswertbaren Merkmalen und Verhaltensweisen zählen u. a. Fingerabdruck, Handflächenabdruck, Handvenenmuster, Geometrie der Hand, Irismuster, Retinamuster, Gesichtsgeometrie, Stimme, Lippenbewegung, (Unter-)Schrift sowie das Tippverhalten auf einer Tastatur.

Die Erfassung biometrischer Merkmale erfolgt mit Hilfe von Kameras und Sensoren (z.B. Mikrofone, Fingerabdrucksensoren). Ein Teil der dabei erzeugten **Rohdaten** (Aufnahmen von Bildern, Tönen oder Sensormesswerten) erlaubt eine unmittelbare Wiedererkennung durch Menschen (z.B. Sprachaufnahmen oder Videoaufnahmen eines Gesichts), wenn die betreffende Person bekannt ist. Für eine weitere Gruppe von Rohdaten ist durch den Menschen nur eine *vergleichende* Identifizierung möglich, etwa beim manuellen Vergleich eines Fingerabdrucks mit einem Muster. Eine dritte Gruppe von Rohdaten kann nicht durch den Menschen mit einem Muster verglichen werden, z. B. Infrarot-Gesichtsaufnahmen oder die Sensordaten eines (Unter-) Schriftensensors, der Schreibdruck und die Schreibgeschwindigkeit erfasst.

Biometrische Verfahren zum automatisierten Vergleich erzeugen aus den Rohdaten ein sog. **Template**. Dies ist ein kleiner Datensatz, der Parameter eines mathematischen Modells der Rohdaten beinhaltet, beispielsweise Koordinaten von sog. Minutien (u.a. Verzweigungen oder Enden von Fingerabdrucklinien) bei Fingerabdrücken. Er enthält (in komprimierter Form) die für einen Vergleich notwendigen Daten, erlaubt aber üblicherweise keine unmittelbaren Rückschlüsse auf die Rohdaten der Person. Ein solches Template wird bei der erstmaligen Benutzung des Gerätes, dem **Einlernen (Enrollment)**, als Muster gespeichert. Bei allen weiteren Nutzungen werden wiederum Rohdaten erfasst und aus ihnen ein Template berechnet. Ein Vergleichsalgorithmus überprüft, ob dieses Template mit dem abgespeicherten übereinstimmt. Ist dies der Fall, meldet das Gerät ein positives Ergebnis.

Es gibt zwei grundsätzliche Betriebsarten, die stark mit der jeweiligen Anwendung zusammenhängen: **Verifikation** und **Identifikation**. Bei der *Verifikation* werden die biometrischen Daten einer lebenden Person mit denen auf dem Ausweis verglichen; hierfür genügt eine Speicherung auf dezentralgen Datenträgern (z. B. auf Chipkarten, Ausdruck eines Barcodes), die im Einflussbereich der Benutzer verbleiben können. Bei der *Identifikation* geht es hingegen um den Abgleich biometrischer Daten „unbekannter Personen" mit einem zentralen Datenbestand, um sie zu identifizieren.

3) Grundsätzliche datenschutzrechtliche Einordnung

Das ULD Schleswig-Holstein beschäftigt sich in der Erkenntnis, dass es sich um ein wichtiges **Zukunftsthema** handelt, bereits seit einigen Jahren mit dem Themenkomplex Biometrie, so. u. a. im Rahmen des in den Jahren 2000-2002 durchgeführten und vom Bundeswirtschaftsministerium geförderten Projektes „BioTrusT". Schwerpunkt war die Untersuchung biometrischer Anwendungen im Bereich von Banken. Die 2001/2002 und im August 2003 für den Deutschen Bundestag erstellten Gutachten („Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen", „Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen") gehen bzw. gingen jeweils als Grundlage in die Berichte des Büros für Technikfolgenabschätzung des Bundestages ein.[1] Schwerpunkt des zuletzt erstellten Gutachtens sind die daten-

[1] Beide Gutachten können beim ULD angefordert werden. Das Gutachten „Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen" ist auch auf der Webseite des ULD veröffentlicht (http://www.datenschutzzentrum.de/projekte/biometri/index.htm#tab).

schutzrechtlichen Anforderungen, die bei der Umsetzung der Vorgaben des Terrorismusbekämpfungsgesetzes hinsichtlich biometrischer Merkmale auf Ausweispapieren von Bundesbürgern und Ausländern zu beachten sind.

Das ULD betrachtet den Einsatz biometrischer Verfahren generell mit **skeptischer Offenheit**. Biometrie beinhaltet viele Chancen, Überprüfungsvorgänge im Alltag einfacher und kundenfreundlicher zu gestalten. Im Vergleich zu einem manuellen Abgleich biometrischer Daten (z. B. Passbild) oder anderen Zugangskontrollverfahren (PINs, Passwörter, Ausweise etc.) kann damit auch eine Erhöhung der Sicherheit einhergehen. Zu bedenken ist aber auch, dass es sich um eine mächtige Technologie handelt, die unter sicherheitstechnischen und grundrechtlichen Aspekten nur schwer zu beherrschen ist. Zu erwähnen sind in diesem Zusammenhang sowohl der Schutz vor der Verwendung von gefälschten biometrischen Merkmalen (z. B. Nachmachen einer Unterschrift, Silikonabgüsse von fremden Fingerabdrükken, Kontaktlinsen mit fremden Irismustern) als auch der technische Schutz der gespeicherten Vergleichsdaten vor Manipulation.

Auf Grund des hohen Mißbrauchspotentials und der Unabänderlichkeit der biometrischen Daten muss gewährleistet sein, dass die in Ausweisen und Reisepässen enthaltenen Daten in der **Verfügungsgewalt der Betroffenen** verbleiben. Eine darüber hinausgehende Speicherung in zentralen und dezentralen Registern ist nicht vom Gesetzeszweck gedeckt und wäre folglich unverhältnismäßig (siehe dazu auch Punkt 4).

4) Eckpunkte einer datenschutzgerechten Gestaltung

Aus datenschutzrechtlicher Sicht sind folgende Eckpunkte im Zusammenhang mit einem breiten Einsatz biometrischer Verfahren zu beachten:

- **Keine unbemerkte Erhebung biometrischer Daten**

Biometrische Verfahren für den Masseneinsatz müssen so konstruiert sein, dass sie die Daten nicht unbemerkt und heimlich erfassen. Daher ist auf die verdeckte Sprecher- oder Gesichtserkennung sowie auf die verdeckte biometrische Auswertung anderer Daten (z. B. Unterschriften) zu verzichten. Dies gebietet schon das allgemeine **Transparenzgebot** bei der Datenverarbeitung. Es sind deshalb Verfahren vorzuziehen, die eine **aktive Mitwirkung** erfordern, etwa einen Kör-

perkontakt oder eine spezielle Haltung des Körpers. Geeignet in dieser Hinsicht sind Hand- und Fingerabdruckverfahren, Handgeometrie oder Schriftdynamik.

- **Nebenwirkungsfreie Verfahren**

Es müssen Verfahren und Verfahrensgestaltungen gewählt werden, die **nebenwirkungsfrei** sind bzw. **Nebenwirkungen minimieren**. Dazu gehört der Verzicht auf die Speicherung solcher Rohdaten, die medizinische oder sonstige sensible Informationen enthalten können. Dazu gehört auch der Verzicht auf die Verwendung von Merkmalen, die für kriminalistische Zwecke genutzt werden können, um eine Vermischung dieser verschiedenen Anwendungszwecke von vornherein auszuschließen. Daraus folgt, dass biometrische Verfahren wie die Handgeometrie-, Handvenen- oder Iriserkennung der Verwendung von Finger-, Handlinien-, Gesichts- oder Sprecherkennungsverfahren vorzuziehen sind. Die Gewinnung von medizinischen oder sonstigen Zusatzinformationen bei der Durchführung von Identitätskontrollen sollte generell gesetzlich untersagt werden, da sich in Zukunft neue, heute nicht vorhersehbare Möglichkeiten ergeben werden, aus den biometrischen Daten zusätzliche Informationen zu gewinnen (etwa zur Gesundheit).

- **Rechtsfolgen**

Es muss beachtet werden, dass die Entscheidungen biometrischer Verfahren nur im Rahmen einer gewissen Schwankungsbreite korrekt sind. Mögliche fehlerhafte Ergebnisse werden danach unterschieden, ob eine fälschliche Erkennung einer unberechtigten Person (**Falschakzeptanz**) oder eine fehlerhafte Nicht-Erkennung eines Berechtigten (**Falschzurückweisung**) erfolgt. Prinzipbedingt kann eine Fehlerart nur zu Lasten der anderen Fehlerart gesenkt werden. Dies geschieht mit Hilfe der Parametereinstellung. Die Häufigkeit von Fehlern hängt vom biometrischen Merkmal, seiner Qualität, dem eingesetzten Produkt und von den Parametereinstellungen ab. Qualitätsaussagen über die Genauigkeit eines Verfahrens sind derzeit nur schwer und nur mit Hilfe umfangreicher statistischer Versuchsreihen zu ermitteln. Bei den besten Gesichtserkennungsverfahren liegen die Fehlerraten im Bereich von 1-10 %, bei Fingerabdruckverfahren im Bereich von 0,2-1%.[2] Bei mehreren Millionen Einreisevorgängen jährlich wären Hun-

[2] Einen Eindruck über die derzeitige Qualität von Gesichts- und Fingerabdruckerkennungsverfahren erlauben die internationalen Wettbewerbe „Face Recognition Vendor Test 2002" (http://www.frvt.org/FRVT2002) und „Fingerprint Verification Competion 2002, FVC2002." (http://bias.csr.unibo.it/fvc2002). Bei einer Falschakzeptanzrate von 1% (d.h. bei einer solchen Parametereinstellung, die 1% Nicht-Berechtigte fälschlicherweise erkennt)

derttausende von Fehlentscheidungen zu Lasten Reisender vorstellbar, während gleichzeitig ein gewisser Prozentsatz Unberechtigter die Grenzen unbehelligt passieren dürfte.

Es darf deshalb **kein blindes Vertrauen** in die biometrische Technik geben. Insbesondere müssen die Ergebnisse biometrischer Entscheidungen überprüft werden (können), wenn sich negative rechtliche Folgen (z. B. Verweigerung der Ein- oder Ausreise) anschließen sollen.

Bei der Erstellung der Ausweise ist zu beachten, dass sich biometrische Merkmale im Laufe der Jahre leicht verändern. Insbesondere bei den Gesichtserkennungsverfahren kann dies dazu führen, dass Berechtigte nicht (mehr) erkannt werden. Dies ist bei der Festlegung der Gültigkeitsdauer von Ausweisen zu berücksichtigen. Notwendig ist auch ein **Recht des Nutzers** auf die Überprüfung, ob es sich um *seine* Datensätze handelt. Anders als die in herkömmlichen Ausweisen verwendeten Daten (Name, Lichtbild, Unterschrift etc.) lassen sich biometrische Merkmale in den meisten Fällen nicht manuell überprüfen. Für eine wirksame Überprüfung durch den Nutzer müssen ihm deshalb genau die technischen Verfahren (mit gleichen Parametereinstellungen) zur Verfügung gestellt werden, die auch sonst bei der Identitätsüberprüfung eingesetzt werden.

- **Systemsicherheit und Revisionsmöglichkeiten**

Biometrische Verfahren müssen höchsten Sicherheitsanforderungen genügen, da ein Missbrauch biometrischer Daten für die Betroffenen fatale Folgen haben kann. Deshalb und weil biometrische Verfahren nicht automatisch sicher sind (ihre Sicherheit hängt zum einen von der Sicherheit des Gesamtsystems, aber auch entscheidend von der Parametereinstellung und der Konfiguration ab), sind **Revisionsmöglichkeiten** vorzusehen, um Manipulationen entdecken oder verhindern zu können.

---

wurden von den besten Geräten eines Gesichtserkennungsverfahrens bei einem 1:1-Vergleich (Verifikation) ca. 90% der Berechtigten erkannt und 10% abgewiesen. Die Ergebnisse beziehen sich auf einen Datensatz von Frontalaufnahmen bei Visa-Anträgen bei US-Behörden, die unter vergleichbaren Bedingungen aufgenommen wurden. Beim Vergleich von Innenaufnahmen des gleichen Tages betrug die Erkennungsrate bis zu 95% (bei 1% Falschakzeptanzrate); wurden Innen- und Außenaufnahmen gemischt, sank die Rate auf 50%. Im Bereich der Fingerabdruckverfahren lagen die besten Ergebnisse bei einer 1%igen FAR bei ca. 0,15% Falschzurückweisungen.

- **Rückfallpositionen und Auswege aus biometrischen Verfahren**

Es müssen sinnvolle Alternativen vorgesehen sein, wenn biometrische Verfahren nicht so wie vorgesehen funktionieren oder Fehlentscheidungen produzieren. Dazu gehören **Ausweichverfahren**, wenn einzelne biometrische Merkmale von Personen nicht erfassbar sind, aber auch Prozeduren, die mit Falscherkennungen und Fehlfunktionen der biometrischen Systeme umgehen. Generell müssen Systeme und Abläufe so gestaltet werden, dass Alternativen möglich sind, wenn sich eingeführte biometrische Verfahren als ungeeignet erweisen.

- **Keine Speicherung von Referenzdaten außerhalb der Verfügungsgewalt der Betroffenen**

Wegen des hohen **Missbrauchspotenzials** und der **Unabänderlichkeit** der biometrischen Daten sollten Referenzdaten weder zentral noch in einer anderen für Unbefugte zugänglichen Form gespeichert werden. Die jetzige Gesetzeslage nach dem 11. September 2001 sieht zwar ein Speicherverbot in zentralen oder vernetzten lokalen Registern vor und hat damit der Nutzung der biometrischen Daten für andere Zwecke als den der sicheren Zuordnung von Ausweispapieren eine Absage erteilt.

Um jeglichen Missbrauch auch tatsächlich wirksam auszuschließen, muss jedoch sichergestellt sein, **dass die Betroffenen die Verfügungsgewalt über ihre Daten behalten**. Die biometrischen Daten dürfen daher **ausschließlich** auf dem Personalausweis bzw. Reisepass, nicht aber in Registern oder als Kopie in Archivbeständen gespeichert werden. Dies beinhaltet auch den Verzicht auf dezentrale Register und Dateien (auch wenn sie zunächst nicht vernetzt sind; sie könnten technisch jederzeit problemlos zusammengeführt werden), aber auch auf Zwischenspeicherungen und Protokollierungen biometrischer Daten zu Kontrollzwecken. Anderenfalls besteht die Gefahr einer Zweckentfremdung dieses Datenbestandes. Da der Gesetzeszweck ausschließlich in der sicheren Zuordnung von Ausweisinhaber und Ausweispapier liegt, verstieße eine auf darüber hinausgehende Nutzungen zielende Verarbeitung der Daten, z. B. für Ermittlungs- und Fahndungszwecke, gegen den **Verhältnismäßigkeitsgrundsatz** des Grundgesetzes. Eine Speicherung biometrischer Daten bei Pass- und Ausweisbehörden (analog zu den Ausweisbildern) ist deshalb – nicht zuletzt wegen der mit der routinemäßigen Nutzung dieser Bilder inzwischen sogar in Ordnungswidrigkeitenverfahren gemachten Erfahrungen – abzulehnen.

Die Frage der Verfügungsgewalt bzw. die Diskussion darüber wird auch auf Seiten der Polizei geführt werden müssen. Klarer Trennstrich bei der Verarbeitung biometrischer Daten muss sein, ob es sich um **Tatverdächtige** handelt, die nach eindeutigen Rechtsvorschriften erkennungsdienstlich behandelt worden sind.

Das für das Büro für Technikfolgenabschätzung des Bundestages erstellte Gutachten von August vergangenen Jahres hat nachgewiesen, dass die Speicherung der biometrischen Merkmale im staatlichen Verfügungsbereich zur Erreichung des Zwecks der Erhöhung der Ausweissicherheit nicht erforderlich ist. Der verfassungsrechtliche Schutz des **Rechts auf informationelle Selbstbestimmung** gebietet es daher, eine solche Speicherung gänzlich zu unterlassen.

5) Fazit

So nachvollziehbar die Bedenken der FDP-Fraktion des schleswig-holsteinischen Landtages daher auch sind, so müssen diese nicht zwangsläufig zu einem vollständigen Verzicht auf biometrische Merkmale in Ausweisen führen. Zusammenfassend lässt sich feststellen, dass den großen Risiken, die biometrische Massenverfahren bergen können, durch eine sinnvolle, abwägende Auswahl der biometrischen Merkmale und durch sorgfältige Gestaltung des technischen, organisatorischen und rechtlichen Umfeldes begegnet werden kann.

Erste Voraussetzung ist aber, dass § 4 Abs. 4 PassG bzw. § 1 Abs. 5 PAuswG von allen Beteiligten so verstanden wird, dass eine Speicherung biometrischer Daten außerhalb der Verfügungsgewalt des Betroffenen überhaupt nicht in Betracht kommt. Wenn dies nicht gewährleistet ist – und bestimmte Äußerungen aus Polizeikreisen lassen daran zweifeln –, müsste § 4 Abs. 4 PassG bzw. § 1 Abs. 5 PAuswG nachgebessert werden, bevor biometrische Daten in Ausweise aufgenommen werden.

Die Diskussion über die Nutzung biometrischer Daten muss auf verfassungsrechtlicher Ebene geführt werden. Dabei muss aber vornehmlich – wie dargelegt – die Frage der **Verfügungsgewalt** über biometrische Daten im Mittelpunkt stehen. Das informationelle Selbstbestimmungsrecht gebietet es, die biometrischen Merkmale des Pass- oder Personalausweisinhabers lediglich auf seinem Dokument und damit im Verfügungsbereich des Betroffenen selbst zu speichern

und bei einer Kontrolle über ein Lesegerät mit den Merkmalen des Inhabers zu vergleichen. Für eine dauerhafte Speicherung biometrischer Daten außerhalb des Verfügungsbereichs des Betroffenen besteht keine Erforderlichkeit; auf sie ist deshalb gänzlich zu verzichten. Unter dieser - nach Auffassung des ULD nur unter dieser - Voraussetzung ist eine Nutzung biometrischer Merkmale in Ausweisparpieren auch unter datenschutzrechtlichen Gesichtspunkten denkbar.