

Positionspapier

der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen

1 Ausgangslage

Mit dem Terrorismusbekämpfungsgesetz wurden in § 4 Passgesetz und § 1 Personalausweisgesetz nahezu gleichlautende Regelungen folgenden Inhalts aufgenommen:

- Pässe und Personalausweise dürfen neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von
 - Fingern,
 - Händen oder
 - Gesichtdes Inhabers enthalten.

- Alle biometrischen Merkmale und die Angaben über die Person dürfen auf den Ausweispapieren verschlüsselt gespeichert werden. Durch ein Bundesgesetz ist Folgendes zu regeln:
 - Arten der biometrischen Merkmale,
 - Einzelheiten der Einbringung von Merkmalen und Angaben in verschlüsselter Form,
 - Art der Speicherung und
 - Art ihrer sonstigen Verarbeitung und Nutzung.

- Die biometrischen Merkmale dürfen nur verwendet werden, um die Echtheit des Dokumentes und die Identität des Inhabers zu prüfen.

- Eine bundesweite Datei darf nicht eingerichtet werden.

Um beurteilen zu können, ob diese Maßnahmen geeignet und angemessen sind, müssen die verschiedenen biometrischen Verfahren aus Datenschutzsicht bewertet werden. Im Folgenden werden verschiedene Verfahren beschrieben und die Risiken aufgezeigt, die im Zusammenhang mit einem flächendeckenden Einsatz biometrischer Merkmale in Ausweisdokumenten zu erkennen sind.

2 Technische Möglichkeiten

2.1 Nutzung vorhandener biometrischer Merkmale

Bevor neue Merkmale in Ausweisen gespeichert werden, sollte geklärt werden, ob die vorhandenen nicht bereits ausreichen, um die Identität des Ausweisinhabers zu prüfen. Auf die Erhebung neuer personenbezogener Daten muss dann verzichtet werden. Könnten Verfahren eingesetzt werden, die bereits vorhandene biometrische Merkmale nutzen, wäre eine geringere Eingriffstiefe in das Recht auf informationelle Selbstbestimmung als bei der Verwendung eines völlig neuen Merkmals ausreichend.

Lichtbild

Mit dem Foto des Inhabers enthalten deutsche Ausweisdokumente bereits biometrische Daten. Mit heute vorhandener Technik ist es grundsätzlich möglich, das Foto auf dem Personalausweis automatisch mit dem Gesicht der Person zu vergleichen, die den Ausweis vorlegt.

Möglicherweise können die zurzeit verwendeten Passbilder die Qualitätsanforderungen an eine automatisierte Verarbeitung nicht in vollem Umfang erfüllen. Bisher gibt es allerdings keine verlässlichen Aussagen über die Bildqualität, die für biometrische Verfahren erforderlich ist. Ebenso wenig ist bisher geklärt, wie sich biometrische Merkmale im Laufe der Zeit ändern. Möglicherweise müsste die Gültigkeitsdauer von Personalausweisen

wesentlich verkürzt werden, damit die Verifikation anhand des Passbildes im Ausweis über die gesamte Gültigkeitsdauer sichergestellt werden kann.

Unterschrift

Die Unterschrift des Inhabers ist ein weiteres biometrisches Merkmal, das schon jetzt auf jedem deutschen Ausweisdokument vorhanden ist. Ein automatischer Vergleich der vorhandenen mit einer bei der Kontrolle geleisteten Unterschrift wäre jedoch wenig sinnvoll, weil die zur Erkennung erforderlichen dynamischen Daten der Unterschrift (Druckverlauf, Schreibpausen) im Ausweis nicht gespeichert sind.

2.2 Biometrische Vermessung des Gesichtes

Sollen biometrische Daten des Gesichtes neu erhoben und in den Ausweispapieren maschinenlesbar beispielsweise als Barcode oder elektronischer Datensatz gespeichert werden, sind hohe Qualitätsanforderungen an die Erfassungs- und Kontrollsysteme zu stellen, um eine ausreichende Wiedererkennungsrate sicherzustellen. Für gute Ergebnisse sind gleichmäßig ausgeleuchtete Frontalaufnahmen von Gesichtern erforderlich. In der Praxis werden diese Anforderungen nur mit hohem Aufwand realisierbar sein.

2.3 Papillarmuster der Finger

Werden nur die Merkmale eines bestimmten Fingers genutzt, entstehen Probleme, wenn dieser bei der Erfassung oder bei Vergleichen verletzt oder anderweitig stark beansprucht ist (z. B. bei Bauarbeitern). Die Erfassung von Daten mehrerer Finger und alternative Vergleiche bei Kontrollen sind sehr aufwändig. Außerdem zeigen Tests, dass ein signifikanter (statistisch aber noch nicht abschließend verifizierter) Prozentsatz von Papillarmustern aus physiologischen Gründen nicht nutzbar ist (siehe Punkt 3.2).

2.4 Handgeometrie und Handlinien

Bei der Vermessung der Handgeometrie handelt es sich um ein System, das in den USA bereits im Einsatz ist. Über die Erkennungsqualität gibt es keine verlässlichen Angaben. Über

die Möglichkeiten der Nutzung der Handlinien gibt es ebenfalls keine gesicherten Erkenntnisse. Die Problematik der Verletzungen oder sonstigen Einschränkungen der Nutzung einer Hand und der sich daraus ergebenden Notwendigkeit der Alternativdaten ist vergleichbar mit der bei der Papillarmusterverwendung. Unklar ist zurzeit auch die Wiedererkennungsqualität bei Handveränderungen durch Arbeits- und Alterungsprozesse.

2.5 Iris- und Retinastruktur

Die gesetzliche Formulierung "Gesicht" lässt eine Erfassung detaillierter Merkmale der Augen nicht zu. Ungeachtet dessen ist festzustellen, dass diese Verfahren bisher noch nicht im größeren Stil eingesetzt worden sind. Sie sind sowohl technisch als auch organisatorisch sehr aufwändig. Bisher ist eine genaue Kopfpositionierung erforderlich, so dass fraglich ist, ob sie durch "Ungeübte" in den Erfassungsstellen und an den Kontrollstellen praktiziert werden können. Sofern das Gesicht, die Iris oder die Retina durch ein Infrarot- oder Lasersystem abgetastet wird, ist damit zu rechnen, dass derartige Systeme auf eine signifikante Ablehnung durch die Betroffenen stoßen.

2.6 Weitere biometrische Merkmale

Aus technischer Sicht ist nicht auszuschließen, dass zur Prüfung der Identität Betroffener auch andere biometrische Merkmale verwendet werden könnten (z. B. Stimme, Bewegungsmuster). Diese Merkmale werden hier jedoch nicht weiter betrachtet, weil laut Pass- und Personalausweisgesetz neben dem Lichtbild und der Unterschrift nur biometrische Merkmale von Fingern, Händen oder dem Gesicht des Inhabers verwendet werden dürfen (siehe 1).

3 Allgemeine technische Randbedingungen

3.1 Vorgaben aus der bestehenden Rechtslage

63. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 07. – 08. März 2002

(Positionspapier - AK-Technik)

Aus dem rechtlichen Rahmen ergeben sich für die zu schaffenden Regelungen aus technischer Sicht, unabhängig von der Art der genutzten biometrischen Merkmale, folgende Vorgaben:

- Die Kontrollsysteme bestehen aus vier Komponenten, die untrennbar und unbeeinflussbar miteinander verknüpft sein müssen:
 - Leseinheit für die aktuellen biometrischen Merkmale,
 - Leseinheit für die Ausweispapiere,
 - Entschlüsselungs- und Vergleichseinheit und
 - Einheit zur Freigabe bzw. Sperrung der Passage.
- Um Manipulationen ausschließen zu können, müssen die biometrischen Systeme bei der Kontrolle stand-alone arbeiten.
- Die enthaltenen Softwarekomponenten sollten zertifiziert (z. B. nach Common Criteria oder ITSEC) und signiert sein. Das gilt auch für Hardwarekomponenten, soweit mit ihnen Entschlüsselungen vorgenommen werden.
- Eine Speicherung von personenbezogenen Daten auf den Datenträgern der Kontrollsysteme über den Abschluss des Kontrollvorgangs hinaus ist nicht zulässig.
- Die Zahl der Personen, die Kontrollen trotz falscher Identität passieren können, muss möglichst gering sein (vgl. FAR unter 3.2).
- Eine regelmäßige Falsch-Rückweisung durch Unzulänglichkeiten bei den gespeicherten Daten muss vor der Ausgabe der Ausweise und Pässe schon durch die örtlichen Ausweisbehörden ausgeschlossen werden. Bevor die ausgebende Stelle den Ausweis aushändigt, muss sie ihn daher mit einem entsprechenden Referenz-Kontrollsystem prüfen.
- Die Verschlüsselung kann wahlweise bei der örtlichen Behörde oder in der Bundesdruckerei erfolgen.
- Der Verschlüsselungsalgorithmus muss wissenschaftlich anerkannt sein und dem Stand der Technik entsprechend als sicher gelten (mindestens für den Zeitraum der Gültigkeit der Ausweise).
- Der Schlüssel darf Unbefugten nicht bekannt werden.
- Wird auf eine Verschlüsselung der Daten verzichtet, müssen die gespeicherten Werte auf andere Weise gegen Missbrauch gesichert werden.

3.2 Stand der wissenschaftlichen Erkenntnisse zu biometrischen Verfahren

63. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 07. – 08. März 2002

(Positionspapier - AK-Technik)

- Bisher gibt es keine wissenschaftlich gesicherten Erkenntnisse zu biometrischen Verfahren bei großen Anwendergruppen. Es können lediglich Erfahrungen mit kleineren Systemen (z. B. die automatisierte Kontrolle der Einwanderungsbehörde auf amerikanischen Flughäfen [Handgeometrie] oder auf den Flughäfen Schiphol und Frankfurt [Iriscan]) herangezogen werden.
- Die Leistungsfähigkeit biometrischer Systeme wird durch ihre Zurückweisungsrate berechtigter Personen (FRR False Rejection Rate) und ihre Überwindungssicherheit gegenüber unberechtigten Personen (FAR False Acceptance Rate) beschrieben. Beide Raten stehen in einem engen Zusammenhang. Je größer die Überwindungssicherheit ist, um so mehr berechnete Personen werden abgewiesen. Die Ermittlung der FAR und der FRR und der Beziehung zueinander ist sehr aufwändig. Für große Anwendergruppen gibt es deshalb bisher keine herstellerneutralen Untersuchungen.
- Biometrische Systeme sind bislang hinsichtlich der FRR und der FAR nicht ausreichend überprüft, um flächendeckend eingesetzt zu werden. Das betrifft auch Fragen der Manipulationssicherheit des Gesamtsystems. Von besonderer Bedeutung ist die Verbindung zwischen Rechner und Sensor, da bei unzureichender Sicherung biometrische Merkmale durch Einspielen (Replay) entsprechender Datensätze vorgetäuscht werden können.
- Auch die Lebenderkennung ist bisher wenig ausgereift. Es ist deshalb nicht auszuschließen, dass biometrische Systeme durch die Präsentation nachgebildeter Merkmale (Silikonabdruck eines Fingerabdrucks, Foto eines Gesichtes usw.) überwunden werden können.
- Zur FER (False Enrollment Rate), die den Anteil der Personen nennt, bei denen das jeweilige biometrische Merkmal nicht geeignet ist oder nicht zur Verfügung steht, gibt es bisher keine gesicherten wissenschaftlichen Erkenntnisse. Eine FER von 1% bedeutet beispielsweise bei bundesweiten Ausweisdokumenten, dass mehr als 500.000 Personen bei Kontrollen immer mit Fehlermeldungen rechnen müssen, da sie durch das System nicht erkannt werden. In jedem Fall muss ein Rückfallsystem für die Nutzer vorhanden sein, die eine sehr schlechte Merkmalsausprägung besitzen oder überhaupt nicht erfasst werden können.

4 Einheitliches Personenkennzeichen

Mit neu erfassten biometrischen Merkmalen bzw. mit den daraus generierten Datensätzen lässt sich eine Vielzahl unterschiedlicher Dateien erschließen und verknüpfen. Deshalb muss ausgeschlossen werden, dass die zusätzlichen biometrischen Merkmale der Ausweise sowohl für weitere staatliche Zwecke (z. B. Strafverfolgung) als auch im privatrechtlichen Bereich (z. B. für Vertragsabschlüsse) verwendet werden. Ein derartiges Merkmal käme sehr schnell einem einheitlichen Personenkennzeichen gleich, das gemäß dem Volkszählungsurteil des Bundesverfassungsgerichts unzulässig ist (BVerfGE 65,1, -53-).

In Bereichen, in denen Biometrie für andere als die in § 4 Passgesetz und § 1 Personalausweisgesetz genannten Zwecke zum Einsatz kommt (z. B. Zugangskontrolle), wäre eine Verknüpfung der verschiedenen Daten technisch möglich. Dies könnte zum einen durch Verwendung der im Ausweis gespeicherten Daten als Referenzmaterial für solche Zwecke erfolgen. Zum anderen könnten gespeicherte biometrische Daten mit denen abgeglichen werden, die zum Zwecke der Ausweiserstellung verwendet werden. Dies wäre, auch wenn es keine durchgängig verwendeten Standards für die Codierung biometrischer Daten gibt, verfahrensübergreifend prinzipiell durchführbar.

5 Speicherung biometrischer Daten

Zur Vermeidung der unbefugten Nutzung von Ausweisdokumenten ist nur eine biometrische Verifikation erforderlich, d.h. der Abgleich der biometrischen Merkmale einer konkreten Person mit den auf einem Ausweis gespeicherten Daten. Eine Speicherung außerhalb des Ausweises ist dafür nicht erforderlich. Das Ziel der Erkennung von "Doppelidentitäten" durch Abgleich biometrischer Daten einer unbekanntenen Person mit denjenigen anderer Personen (Identifikation) setzt die Speicherung personenbezogener Daten in zentralen Referenzdateien voraus. Aus Sicht des Datenschutzes ist eine solche Datensammlung insbesondere im Hinblick auf die Bildung eines einheitlichen Personenkennzeichens und die unvermeidlichen Missbrauchsmöglichkeiten jedoch abzulehnen.

Für die Ausweise selbst besteht die Möglichkeit, die Referenzdaten als Rohdaten oder als biometrischen Datensatz zu speichern. Während Rohdaten ggf. auch grafisch gespeichert werden können (z. B. das Bild eines Fingerabdrucks), muss für elektronische Biometriedaten („Template“, „Vektor“) der Ausweis mit einem maschinenlesbaren Datenträger (Barcode, Speicherchip etc.) versehen werden. Um einen Missbrauch dieser Daten zu verhindern, kommt insbesondere eine verschlüsselte Speicherung in Betracht. Während dies gegen einen alltäglichen Zugriff schützen mag, kann bei der Vielzahl von Geräten, in denen der Entschlüsselungsschlüssel vorhanden sein muss (bei Polizei und Grenzkontrollbehörden), jedoch kaum davon ausgegangen werden, dass die verschlüsselt gespeicherten Daten auf Dauer vor interessierten Dritten verborgen bleiben (siehe 3.1).

6 Überschießende Daten

Einige biometrische Merkmale lassen neben der Nutzung zur Identifizierung auch völlig andere Auswertungen zu. So kann möglicherweise auf bestimmte gesundheitliche Zustände oder Dispositionen, auf Faktoren wie Stress, Betrunkenheit oder Müdigkeit geschlossen werden. Bekannt ist dies von Bildern des Gesichts, der Hand und des Augenhintergrunds, von verhaltensbasierten biometrischen Merkmalen (Sprache, Unterschrift) sowie in besonderer Weise von genetischen Daten.

In der Regel sind nur aus den biometrischen Rohdaten solche Zusatzinformationen ableitbar, nicht aber aus den daraus gewonnenen Templates. Aus diesem Grund dürfen insbesondere die Rohdaten selbst nicht zentral gespeichert werden. Außerdem sind im Verarbeitungsprozess einer biometrischen Kontrolle die Rohdaten möglichst früh zu löschen, um die Gefahr einer Zweckentfremdung zu verringern.

7 Eignung für die Überwachung

Die Speicherung biometrischer Merkmale außerhalb des Ausweises birgt neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung. Gelingt es, biometrische Daten im

63. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 07. – 08. März 2002

(Positionspapier - AK-Technik)

Alltag zu erfassen und diese mit einer zentralen Datenbank abzugleichen, können weitgehende Bewegungsprofile der Betroffenen erstellt werden. Im Gegensatz zu einer Erfassung eines biometrischen Merkmals unter Mitwirkung des Betroffenen handelt es sich hierbei um nicht-kooperative Vorgänge, die dem Betroffenen womöglich nicht einmal bewusst sind. Dafür sind Merkmale geeignet, die kontaktlos und über eine gewisse Distanz erfasst werden können. Dies trifft zur Zeit vor allem auf die Gesichtserkennung zu, die bei geeignetem Blickwinkel mittels gewöhnlicher Kameras erfolgen kann. Da es datenschutzrechtlich geboten ist, sensitive Daten nur in Kenntnis der Betroffenen zu erheben, sind nichtkooperative passive Systeme abzulehnen.

Demgegenüber ist die flächendeckende Erfassung des Fingerabdrucks oder der Handgeometrie ohne Wissen und Mitwirkung des Betroffenen nicht oder nur unter sehr großem Aufwand möglich. Zwar können Fingerabdrücke auch heimlich von berührten Gegenständen abgenommen werden. Dies eignet sich jedoch – wegen des hierfür erforderlichen Aufwands – nur zur Behandlung von Einzelfällen und ist daher mit einer Überwachung nicht vergleichbar.

8 Ergebnis

Im Ergebnis zeigt sich, dass keines der weiteren biometrischen Merkmale unproblematisch ist. Vor der Entscheidung, ob ein bestimmtes biometrisches Merkmal in Ausweise aufgenommen werden soll, müssen die verschiedenen Risiken daher sorgfältig gegeneinander abgewogen werden.

Vor der gesetzlichen Einführung neuer biometrischer Merkmale ist eine Evaluation durch einen Großversuch geboten. Dabei wären Ausweise mit zusätzlichen Sicherheitsmerkmalen (z. B. Hologramm) ohne biometrische Merkmale zu erproben und zu bewerten und mit Ausweisen zu vergleichen, die ebenso ausgestaltet sind, jedoch biometrische Merkmale enthalten. Zu prüfen wäre auch, wie hoch das Risiko für Bürgerinnen und Bürger wäre, wegen Gerätedefekten bei hard- oder softwaregestützter Erkennung der Merkmale bzw. wegen statistisch zu erwartenden Falscherkennungen bei der Ausweiskontrolle trotz eines

63. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
vom 07. – 08.März 2002

(Positionspapier - AK-Technik)

echten eigenen Ausweises aufgehoben und intensiver überprüft zu werden, als sonst notwendig.