Seit dem 01. November 2005 werden in Deutschland neue Reisepässe ausgegeben. Im Passdeckel befindet sich ein über Funk auslesbarer RFID-Chip, auf dem neben den herkömmlichen Daten des Passinhabers auch biometrische Merkmale gespeichert sind. Hierbei handelt es sich zunächst um ein Gesichtsbild; ab 2007 sollen zusätzlich die Bilder zweier Fingerabdrücke auf dem Chip gespeichert werden. Für ab 2008 neu ausgegebene Personalausweise ist Ähnliches geplant. Ziel der Aufnahme elektronisch auslesbarer biometrischer Merkmale in Pässe und Ausweise ist, die Dokumente fälschungssicherer zu machen und ihren Missbrauch besser zu verhindern.

Was sind biometrische Verfahren?

Schon seit vielen Jahrzehnten werden Fotos, Fingerabdrücke oder die Unterschrift verwendet, um einzelne Personen eindeutig zu bestimmen. Der technische Fortschritt ermöglicht es, hierzu verstärkt automatisierte biometrische Verfahren zu nutzen.

> ➢ Die Biometrie befasst sich mit der Messung und Auswertung bestimmter Merkmale von Lebewesen – insbesondere mit der automatisierten Erkennung von Personen anhand ihrer Merkmale durch Nutzung moderner Rechentechnik.

Zu den Eigenschaften, die mit biometrischen Verfahren ausgewertet werden, gehören

- physiologische Merkmale wie Gesichtsbild, Finger- oder Handabdruck, Irismuster, DNA
- Verhaltensmerkmale wie Schreib- oder Sprechverhalten, Mimik, Gang.

Um eine Person anhand ihres Gesichts, des Fingerabdrucks, des Sprechverhaltens usw. zu bestimmen, muss zunächst das jeweilige Merkmal erfasst und digital gespeichert werden. Die Speicherung kann in Form von Rohdaten (z.B. als Bild- oder Tondatei) oder in Form so genannter „Templates“ erfolgen. Bei letzteren werden aus den Rohdaten nur die wesentlichen, charakteristischen Elemente (z.B. bei einem Gesicht einzelne Punkte, ihre Lage und ihr Abstand) extrahiert und abgespeichert.

Die Speicherung biometrischer Daten kann zentral (z.B. in einer gemeinsamen Datenbank für alle Betroffenen) oder dezentral (z.B. auf dem Chip im Reisepass des Einzelnen) erfolgen.

Zur (Wieder-)Erkennung einer Person wird das biometrische Merkmal erneut erfasst (z.B. ein Foto des Gesichts oder eine Sprechprobe aufgenommen) und digitalisiert. Dann gibt es zwei Ansätze:

- Bei der Verifikation gibt die Person vor, eine bestimmte Identität zu besitzen („Ich bin Max Mustermann“). Das System vergleicht dann die aktuell bestimmten Daten mit den für die jeweilige Person gespeicherten (1:1-Vergleich).
- Bei der Identifikation werden die aktuellen Daten mit denen aller gespeicherten Personen verglichen (1:n-Vergleich). Der Betroffene wird in der Menge identifiziert („Das ist Max Mustermann“).

Eine Person gilt dann als erkannt, wenn die aktuell gemessenen biometrischen Daten hinreichend ähnlich zu den gespeicherten sind (bzgl. eines einstellbaren Schwellwerts).

Wo werden biometrische Verfahren angewendet?

Biometrische Merkmale haben die Eigenschaft, dass sie bei (fast) jedem Menschen vorhanden sind, zeitlich weitgehend unveränderlich bleiben und den Einzelnen meist eindeutig bestimmen. Aus diesen Gründen eignen sich biometrische Verfahren für Anwendungen, bei denen die Identität einer Person festzustellen oder nachzuweisen ist.

So lässt sich z.B. mit Gesichtserkennungssystemen der Zutritt zu Gebäuden oder Räumen kontrollieren. Neue Laptops enthalten oft Sensoren für Fingerabdrücke. Dies erlaubt den Nutzern eine komfortable Anmeldung, da sie biometrische Merkmale im Gegensatz zu Passwörtern nicht vergessen können.

Beim neuen Reisepass kann der Passmissbrauch dadurch effektiver verhindert werden, dass die digital gespeicherten biometrischen Merkmale mit denen der kontrollierten Person verglichen werden.

Und letztlich profitiert auch die Kriminalistik von biometrischen Verfahren, da die Bestimmung der Identität von Opfern oder potentiellen Tätern schneller und genauer möglich ist (z.B. durch DNA-Analysen).

Wie leistungsfähig sind biometrische Verfahren?

Biometrische Verfahren arbeiten nicht fehlerfrei. Sie liefern nur Wahrscheinlichkeitsaussagen über den Grad an Übereinstimmung von aktuell gemessenen und gespeicherten biometrischen Daten.

Betrachtet man z.B. biometrische Systeme zur Verifikation (wie sie bei der Zutritts- oder Passkontrolle eingesetzt werden), sind für die Beurteilung der Leistungsfähigkeit eines konkreten Systems die folgenden Fehlerraten wichtig:

- Die Falschakzeptanzrate (FAR) misst den Anteil der Personen, die vom System akzeptiert wurden, obwohl sie nicht berechtigt sind.
- Die Falschrückweisungsrate (FRR) misst den Anteil der Personen, die vom System zurückgewiesen wurden, obwohl sie berechtigt sind.

Beide Fehlerraten können nicht losgelöst voneinander betrachtet werden. Bei der Konfiguration eines Systems ist stets ein Kompromiss zwischen Sicherheit und Benutzbarkeit bzw. Akzeptanz zu finden.

> ➢ Wird ein biometrisches System „schärfer“ eingestellt, sinkt zwar der Anteil falsch akzeptierter Personen, dafür steigt der Anteil falsch zurückgewiesener Personen – und umgekehrt.

Umfangreiche experimentelle Untersuchungen ergeben für aktuelle biometrische Systeme bei der Gesichtserkennung eine Falschrückweisungsrate zwischen 2 und 10 %, beim Fingerabdruck zwischen 1 und 7 % und beim Irismuster zwischen 2 und 23 % (FAR jeweils bei 0,1 %).

Der oft noch recht hohe Anteil fälschlicherweise zurückgewiesener Personen wird mit der fortschreitenden Entwicklung biometrischer Systeme und ihrer

routinemäßigen Nutzung sinken. Daneben lässt sich durch gleichzeitige Auswertung mehrerer Merkmale die Leistungsfähigkeit der Systeme verbessern.

Was ist aus Sicht des Datenschutzes zu beachten?

Auch wenn die Nutzung biometrischer Verfahren einige Vorteile bei der Feststellung oder beim Nachweis der Identität von Personen bietet, sind die Prinzipien der Datensparsamkeit und der Zweckbindung einzuhalten. Dies gilt umso mehr, da einige biometrische Merkmale zusätzliche Informationen über den Betroffenen enthalten können (z.B. über Krankheitsbilder, Berufsgruppen, ethnische Gruppen).

- Biometrische Daten dürfen nur zu dem Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Datensparsame Templates sind gegenüber Rohdaten vorzuziehen.

Beim neuen Reisepass ist festgelegt, dass die digital gespeicherten biometrischen Daten nur für hoheitliche Zwecke bei der Passkontrolle genutzt werden dürfen. Eine Verwendung von Templates scheiterte an weltweit uneinheitlichen Erkennungsverfahren.

Da biometrische Daten Personen (mit großer Wahrscheinlichkeit) eindeutig bestimmen, können sie als Referenzmerkmal für die Verknüpfung mit Daten aus anderen Systemen dienen. Eine solche Profilbildung ist jedoch unzulässig. Auch die Speicherung biometrischer Daten in zentralen oder vernetzten Datenbanken ist in Deutschland zurzeit rechtlich ausgeschlossen. Für andere Staaten gilt dies nicht.

- Biometrische Verfahren, die der Verifikation dienen, lassen sich grundsätzlich mit einer dezentralen Datenspeicherung betreiben.

Werden biometrische Verfahren zur Zutrittskontrolle oder zur Anmeldung an Computersystemen verwendet, besteht die Gefahr, dass bei einem Diebstahl der biometrischen Daten Unberechtigte eine falsche Identität vortäuschen können. Biometrische Merkmale lassen sich nicht so einfach und beliebig oft wechseln wie z.B. Passwörter.

- Biometrische Daten müssen durch geeignete Sicherheitsmaßnahmen vor unberechtigtem Zugriff und vor Diebstahl geschützt werden.

Für das Auslesen der biometrischen Daten aus dem neuen Reisepass wurden deshalb auf technischer Ebene eine Reihe von Maßnahmen ergriffen, die den Identitätsdiebstahl erschweren sollen (z.B. die Verschlüsselung der Funkkommunikation).

Und auch bei der Nutzung biometrischer Verfahren müssen Betreiber stets das Gebot der Transparenz beachten: Betroffene sind darüber zu informieren, welche Daten, warum und wie verarbeitet werden. Lassen sich Personen nicht eindeutig mit biometrischen Verfahren bestimmen, dürfen sie deswegen nicht benachteiligt werden.

Weiterführende Informationen

- Grundlagen zur Biometrie und viele Verweise bei Wikipedia - http://de.wikipedia.org/wiki/Biometrie
- Informationen und Hinweise zum neuen Reisepass http://www.neuer-reisepass.de

Haben Sie Fragen oder Hinweise?
Schreiben Sie uns oder rufen Sie an!

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77, 14532 Kleinmachnow
Telefon: 033203 / 356 - 0 Fax: 033203 / 356 49
Internet: http://www.lda.brandenburg.de

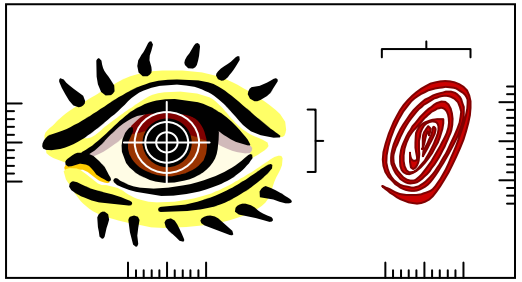
Berliner Beauftragter für Datenschutz und
Informationsfreiheit
An der Urania 4-10, 10787 Berlin
Telefon: 030 / 13 88 9 - 0 Fax: 030 / 21 55 05 0
Internet: http://www.datenschutz-berlin.de

(letzte Änderung: September 2006)

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Berliner Beauftragter für Datenschutz und Informationsfreiheit

Vom Fingerabdruck bis zur DNA-Analyse



Datenschutz beim Einsatz biometrischer Verfahren