ARTIKEL-29-DATENSCHUTZGRUPPE

00720/12/DE

WP 193

Stellungnahme 3/2012
zu Entwicklungen im Bereich biometrischer Technologien

Angenommen am 27. April 2012

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Freiheit und Sicherheit, Direktion C (Grundrechte und Unionsbürgerschaft), der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_de.htm

Zusammenfassung

Biometrische Systeme nutzen bestimmte individuelle Merkmale einer Person zur Identifikation und/oder Authentifikation dieser Person und stellen insoweit enge Verknüpfungen mit den betroffenen Personen her. Die Daten einer Person können gelöscht oder geändert werden. Manipulationen oder Änderungen der Datenquelle hingegen sind nicht möglich.

Biometrische Daten werden erfolgreich und wirksam in der Forschung genutzt; sie sind ein wesentliches Element der Forensik und spielen eine wichtige Rolle bei Systemen zur Zugangskontrolle. Sie können helfen, das Sicherheitsniveau zu erhöhen, und sie können dazu beitragen, Identifikations- und Authentifikationsverfahren zu vereinfachen, zu beschleunigen und bequemer zu gestalten. Früher war diese Technologie teuer und hatte entsprechend nur eingeschränkte Auswirkungen auf die Datenschutzrechte natürlicher Personen. Dies hat sich in den letzten Jahren drastisch geändert. DNA-Analysen beanspruchen heute weniger Zeit und sind für nahezu jedermann erschwinglich. Der technische Fortschritt hat dazu geführt, dass Datenspeicher und Rechenkapazitäten billiger wurden. Infolge dieser Entwicklung sind Online-Fotoalben und soziale Netzwerke entstanden, in denen Milliarden von Fotos verwaltet werden. Fingerabdruck-Lesegeräte und Systeme zur Videoüberwachung sind bezahlbare technische Hilfsmittel geworden. Die Entwicklung dieser Technologien hat dazu beigetragen, dass viele Verfahren vereinfacht wurden, zahlreiche Verbrechen aufgeklärt werden konnten und Zugangskontrollsysteme zuverlässiger geworden sind. Diese Entwicklung hat allerdings auch neue Bedrohungen der Grundrechte mit sich gebracht. Die genetische Diskriminierung hat sich zu einem echten Problem entwickelt, und der Diebstahl von Identitäten ist nicht mehr nur eine theoretische Gefahr.

Bei anderen neuen Technologien, die auf große Bevölkerungsgruppen abzielen, und die in jüngster Zeit Anlass zu datenschutzrechtlichen Bedenken gegeben haben, steht die Verknüpfung mit bestimmten Personen nicht unbedingt im Vordergrund bzw. ist diese Verknüpfung mit beträchtlichem Aufwand verbunden. Biometrische Daten hingegen sind direkt mit einer einzigen Person verknüpft. Dies ist nicht immer vorteilhaft, sondern birgt auch erhebliche Nachteile. Die Ausrüstung von Videoüberwachungssystemen und Smartphones mit Funktionen zur Gesichtserkennung, die auf der Nutzung der Datenbanken sozialer Netzwerke beruhen, könnte jegliche Anonymität zunichtemachen und zur Folge haben, dass Einzelpersonen auf Schritt und Tritt überwacht werden. Allerdings könnten Fingerabdruck-Lesegeräte, Geräte zur Erkennung von Venenstrukturen („Venenscanner“) oder auch einfach ein Lächeln in eine Kamera Chipkarten, Codes, Kennwörter und Unterschriften ersetzen.

Diese Zusammenhänge sowie weitere neue Entwicklungen sind Gegenstand dieser Stellungnahme. Ziel dieser Stellungnahme ist es, sowohl die betreffenden Personen als auch die gesetzgebenden Institutionen zu sensibilisieren. Die technischen Innovationen, die allzu häufig nur in ihrer Eigenschaft als Technologien dargestellt werden, die das Erscheinungsbild und die Bedienungsfreundlichkeit von Anwendungen verbessern, könnten auch zu einem schrittweisen Verlust der Privatsphäre führen, wenn keine angemessenen Garantien vorgesehen werden. Daher werden in dieser Stellungnahme technische und organisatorische Maßnahmen erläutert, die die Gefahren im Hinblick auf den Datenschutz und die Verletzung der Privatsphäre verringern und dazu beitragen könnten, Beeinträchtigungen der Privatsphäre und des Grundrechts der Bürger Europas auf den Schutz ihrer personenbezogenen Daten zu verhindern.

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Umfang der Stellungnahme

Im Jahr 2003 hat die Artikel-29-Datenschutzgruppe (Datenschutzgruppe) für Biometrie (WP 80) Fragen des Datenschutzes im Zusammenhang mit der Nutzung aufkommender Technologien zum elektronischen Lesen und Verarbeiten biometrischer Daten untersucht. In den letzten Jahren haben sich diese Technologien sowohl im öffentlichen als auch im privaten Bereich weithin etabliert. Gleichzeitig entwickelte sich eine Reihe neuer Dienstleistungsangebote. Biometrische Technologien, die früher mit einem erheblichen finanziellen Aufwand einhergingen und beträchtliche Rechenkapazität beanspruchten, sind drastisch billiger geworden, und die erforderlichen Rechenprozesse können erheblich schneller durchgeführt werden. Der Einsatz von Fingerabdruck-Lesegeräten ist inzwischen allgemein üblich. Bei manchen Laptops beispielsweise erfolgt eine biometrische Zugangskontrolle mit einem Fingerabdruck-Lesegerät. Dank der erzielten Fortschritte liegen die Ergebnisse von DNA-Analysen nun binnen weniger Minuten vor. Einige der neu entwickelten Technologien (beispielsweise die Erkennung von Venenstrukturen oder die Gesichtserkennung) wurden bereits bis zur Marktreife entwickelt. Diese Technologien gehören in unserem Leben in unterschiedlichen Bereichen bereits zum Alltag. Biometrische Technologien sind eng mit gewissen personenbezogenen Merkmalen verbunden. Teilweise können diese Merkmale genutzt werden, um empfindliche Daten in Erfahrung zu bringen. Außerdem ermöglichen biometrische Daten häufig die automatisierte Verfolgung und Aufspürung von Personen sowie die Erstellung von Profilen. Insoweit können sich diese Entwicklungen erheblich auf die Privatsphäre und auf das individuelle Recht auf Datenschutz auswirken. Mit zunehmender Verbreitung dieser Technologien verschärfen diese Auswirkungen sich noch. Früher oder später wird jede einzelne Person in einem oder mehreren biometrischen Systemen erfasst.

In dieser Stellungnahme soll ein überarbeiteter und aktualisierter Rahmen für einheitliche allgemeine Leitlinien und Empfehlungen zur Berücksichtigung von Grundsätzen des Schutzes der Privatsphäre und des Datenschutzes im Zusammenhang mit biometrischen Anwendungen beschrieben werden. Die Stellungnahme richtet sich an gesetzgebende Institutionen auf europäischer und auf nationaler Ebene sowie an die Biometrieindustrie und an die Nutzer der entsprechenden Technologien.

2. Begriffsbestimmungen

Biometrische Technologien sind nicht neu und wurden bereits in mehreren Stellungnahmen der Datenschutzgruppe behandelt. In diesem Abschnitt wurden wichtige Begriffsbestimmungen zusammengestellt und gegebenenfalls aktualisiert.

Biometrische Daten: Wie von der Datenschutzgruppe bereits in der Stellungnahme 4/2007 (WP 136) erläutert, können „biometrische Daten"

> *„als biologische Eigenschaften, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen definiert werden, wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind, auch wenn die in der Praxis angewandten Modelle für ihre technische Messung in gewissem Umfang auf Wahrscheinlichkeiten beruhen."*

Biometrische Daten wirken sich insoweit unwiderruflich auf die Verbindung zwischen Körper und Identität aus, als sie die Merkmale des menschlichen Körpers „maschinenlesbar" machen und damit vielfältige Nutzungsmöglichkeiten erschließen.

Biometrische Daten können in unterschiedlicher Form gespeichert und verarbeitet werden. Manchmal werden die von einer Person erfassten biometrischen Informationen in einem Rohformat gespeichert und verarbeitet, aus dem sich die Herkunft der Daten auch ohne besondere Kenntnisse ermitteln lässt (z. B. bei Porträtfotos, bei gescannten Fingerabdrücken oder bei Stimmenaufzeichnungen). In anderen Fällen werden die erfassten biometrischen Rohdaten so verarbeitet, dass nur bestimmte Merkmale und/oder Elemente extrahiert und als sogenanntes biometrisches Template gespeichert werden können.

Herkunft biometrischer Daten: Biometrische Daten können aus unterschiedlichen Quellen stammen und physische, physiologische, verhaltensbezogene und psychische Merkmale einer Person umfassen. In der Stellungnahme 4/2007 (WP 136) wurde festgestellt:

> Die Quellen biometrischer Daten (z. B. Proben von menschlichem Gewebe) sind *„selbst [...] keine biometrischen Daten ..."* Sie können jedoch zur Erfassung biometrischer Daten genutzt werden (indem Informationen aus diesen Quellen extrahiert werden).

Wie bereits in WP 80 erläutert, sind biometrische Verfahren zwei Hauptkategorien zuordnen:

- Die erste Gruppe umfasst die Verfahren, die die physischen und **physiologischen** Merkmale einer Person erfassen (Verifikation von Fingerabdrücken, Finger-Bildanalyse, Iris-Erkennung, Netzhautanalyse, Gesichtserkennung, Erkennung der Handgeometrie oder der Ohrenform, Erfassung des Körpergeruchs, Sprecherverifikation, Analyse von DNA-Mustern, Analyse der Schweißporen usw.).
- Die zweite Gruppe beinhaltet die Verfahren, die die **Verhaltensmerkmale** einer Person erfassen. Dazu zählen u. a. die Verifikation von Unterschriften und die Analyse von Tastenanschlägen, Gangarten und Bewegungsmustern sowie die Auswertung von Verhaltensweisen, die Rückschlüsse auf unterbewusstes Denken (etwa beim Lügen) zulassen.

Außerdem sollte der sich entwickelnde Bereich der psychologischen Verfahren nicht außer Acht gelassen werden. Beispielsweise werden aufgrund des Verhaltens in konkreten Situationen oder anhand spezifischer Tests psychologische Profile erstellt.

Biometrische Templates: Aus biometrischen Rohdaten (z. B. Gesichtsmessungen an einem Bild) können Schlüsselmerkmale extrahiert werden, um später nicht die eigentlichen Rohdaten, sondern die daraus extrahierten Merkmale zu verarbeiten. So entsteht ein biometrisches Template der betreffenden Daten. Von entscheidender Bedeutung ist die Definition des Umfangs eines Template (d. h. die Festlegung der Menge der in einem Template enthaltenen Informationen). Einerseits sollte das Template umfangreich genug sein, um die Sicherheitsanforderungen zu erfüllen (wobei Überschneidungen zwischen unterschiedlichen biometrischen Daten ebenso zu vermeiden sind wie die Substitution von Identitäten). Andererseits darf das Template nicht so umfangreich sein, dass sich die biometrischen Daten später vielleicht nicht mehr rekonstruieren lassen. Die Erstellung des Template sollte nur in eine Richtung möglich sein, d. h., es sollte ausgeschlossen sein, dass ausgehend von einem Template die biometrischen Rohdaten wiederhergestellt werden.

Biometrische Systeme: In WP 80 werden biometrische Systeme wie folgt definiert:

> *„Biometrische Systeme sind Anwendungen der Biometrie, die eine automatische Identifikation und/oder Authentifikation/Verifikation von Personen ermöglichen. Authentifikations-/Verifikationsanwendungen werden häufig für verschiedene Aufgaben in völlig unterschiedlichen Bereichen und unter der Verantwortung der unterschiedlichsten Stellen eingesetzt.“*

Mit den neuesten technologischen Entwicklungen können biometrische Systeme nun auch zur Kategorisierung/Aufschlüsselung von Daten verwendet werden.

Die mit biometrischen Systemen verbundenen Risiken liegen in der Natur der zu verarbeitenden biometrischen Daten. Eine allgemeinere Definition wäre daher ein System, das biometrische Daten extrahiert und weiterverarbeitet.

Die Verarbeitung biometrischer Daten in einem biometrischen System beinhaltet gewöhnlich mehrere Prozesse (Erfassung, Speicherung, Abgleich usw.):

> **- Biometrische Erfassung:** Die biometrische Erfassung beinhaltet sämtliche Prozesse in einem biometrischen System, die zur Extrahierung biometrischer Daten aus einer biometrischen Quelle und zur Verknüpfung dieser Daten mit einer bestimmten Person benötigt werden. Umfang und Qualität der zu erfassenden Daten sollten hinreichend sein, um eine zuverlässige Identifikation, Authentifikation, Kategorisierung und Verifikation zu ermöglichen, ohne jedoch Daten in übermäßigem Umfang zu erfassen. Der Umfang der während der Erfassung aus einer biometrischen Quelle extrahierten Daten muss dem Zweck der jeweiligen Verarbeitung und der Leistungsfähigkeit des betreffenden biometrischen Systems angemessen sein.
>
> Bei der Erfassung kommt eine Person gewöhnlich zum ersten Mal mit einem bestimmten biometrischen System in Kontakt. Meist erfordert die Erfassung die Mitwirkung der betreffenden Person (z. B. bei der Abnahme von Fingerabdrücken). Entsprechend bietet dieser Schritt die Gelegenheit zur Aufklärung und zu einer fairen Unterrichtung über die vorgesehene Verarbeitung. Allerdings können Personen auch ohne ihr Wissen und ohne ihre Einwilligung erfasst werden (z. B. mit Überwachungskameras mit integrierter Gesichtserkennung). Die Zuverlässigkeit und die Sicherheit des Erfassungsprozesses sind entscheidend für die Leistungsfähigkeit des gesamten Systems. Einer Person kann die Möglichkeit eingeräumt werden, die in einem biometrischen System erfassten biometrischen Daten zu aktualisieren.

- **Biometrische Speicherung:** Die während der Erfassung erhaltenen Daten können zur späteren Verwendung dort gespeichert werden, wo die Erfassung erfolgt ist (z. B. in einem Lesegerät). Ebenso kommt jedoch die Speicherung in einer zentralen Datenbank in Betracht, auf die eines oder mehrere biometrische Systeme zugreifen können.

- **Biometrischer Abgleich:** Beim biometrischen Abgleich werden die erfassten biometrischen Daten/Templates mit den biometrischen Daten/Templates einer neuen Stichprobe verglichen, um Daten identifizieren, verifizieren/authentifizieren oder kategorisieren zu können.

Biometrische Identifikation: Die Identifikation einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich biometrischer Daten einer Person (die während der Identifikation erfasst wurden) mit einer Reihe biometrischer Templates in einer Datenbank (One-to-many-Verfahren).

Biometrische Verifikation/Authentifikation: Die Verifikation einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich der (während der Verifikation erfassten) biometrischen Daten einer Person mit einer Reihe biometrischer Templates in einer Datenbank (One-to-many-Verfahren).

Biometrische Kategorisierung/Aufschlüsselung: Die Kategorisierung/Aufschlüsselung der Merkmale einer Person durch ein biometrisches System erfolgt gewöhnlich, indem festgestellt wird, ob die biometrischen Daten einer Person einer Gruppe mit vordefinierten Merkmalen zuzuordnen sind, um dann bestimmte Maßnahmen einzuleiten. In diesem Fall kommt es nicht darauf an, die betreffende Person zu identifizieren oder zu verifizieren, sondern die Person automatisch einer bestimmten Kategorie zuzuweisen. Anschließend könnten beispielsweise auf einer Werbetafel je nach Alter oder Geschlecht des Betrachters unterschiedliche Werbungen angezeigt werden.

Multimodale Biometrie: Multimodale Biometrie kann als Kombination verschiedener biometrischer Technologien definiert werden, durch die die Zuverlässigkeit oder die Leistungsfähigkeit eines Systems gesteigert werden soll. Multimodale biometrische Verfahren werden auch als „mehrstufige biometrische Verfahren“ bezeichnet. Die entsprechenden Systeme nutzen beim Abgleich mindestens zwei biometrische Merkmale/Verfahren zur Identifikation einer bestimmten Person. Diese Systeme können auf unterschiedliche Weise funktionieren. Sie können unterschiedliche biometrische Daten mit unterschiedlichen Sensoren erfassen, oder sie können ein bestimmtes biometrisches Merkmal unter Einbeziehung mehrerer Informationseinheiten berücksichtigen. In manchen Studien werden dieser Kategorie auch Systeme zugeordnet, bei denen dieselben biometrischen Informationen mehrfach erfasst werden, oder bei denen Merkmale einer bestimmten biometrischen Probe mit mehreren Algorithmen ermittelt werden. Zu diesen multimodalen biometrischen Systemen zählen beispielsweise auf EU-Ebene der elektronische Reisepass (e-Passport) oder in den Vereinigten Staaten der biometrische Identifikationsdienst US-VISIT.

Zuverlässigkeit: Mit biometrischen Systemen sind zu 100 % fehlerfreie Ergebnisse nur schwer zu erzielen. Dies kann auf unterschiedliche Umgebungen bei der Datenerfassung (Beleuchtung, Temperatur usw.), aber auch auf die jeweils verwendeten Geräte und Einrichtungen (Kameras, Scanner usw.) zurückzuführen sein. Die am weitesten verbreiteten Parameter zur Leistungsbewertung sind die FAR (*False Accept Rate*) und die FRR (*False Reject Rate*). Beide Parameter können dem jeweils eingesetzten System angepasst werden.

- False Accept Rate (FAR): Die FAR gibt Aufschluss über die Wahrscheinlichkeit, dass ein biometrisches System eine Person nicht zuverlässig identifiziert oder einen Betrugsversuch nicht erkennt. Sie gibt den Prozentanteil fälschlicherweise angenommener ungültiger Eingaben an. Die FAR wird auch als Anteil der falsch positiven Ergebnisse bezeichnet.

- False Reject Rate (FRR): Als FRR wird die Wahrscheinlichkeit bezeichnet, dass das System Daten unbegründet ablehnt. Eine unbegründete Ablehnung erfolgt dann, wenn eine Person den jeweils vorhandenen biometrischen Templates nicht zugeordnet wird. Die FFR wird auch als Anteil der falsch negativen Ergebnisse bezeichnet.

Bei geeigneter Anpassung des Systems und angemessener Konfiguration können kritische Fehler bei biometrischen Systemen auf ein in der Praxis annehmbares Niveau reduziert werden. Bei einem perfekten System liegen FAR und FRR bei Null. Meist besteht jedoch eine negative Korrelation derart, dass eine höhere FAR mit einer geringeren FRR einhergeht.

Wichtig ist auch, dass der Zweck der Informationsverarbeitung unter Berücksichtigung sowohl der FAR und der FRR als auch der Populationsgröße als Maßstab für die Entscheidung darüber herangezogen wird, ob die Zuverlässigkeit eines biometrischen Systems als annehmbar zu bewerten ist. Außerdem kann bei der Bewertung der Zuverlässigkeit eines biometrischen Systems berücksichtigt werden, ob das System Merkmale lebender Objekte erfassen kann. Latente Fingerabdrücke beispielsweise können kopiert und zur Erzeugung falscher Fingerabdrücke verwendet werden. Ein Fingerabdruck-Lesegerät darf nicht derart manipulierbar sein, dass eine falsch positive Identifikation erfolgt.

3. Analyse der restlichen Situation

Der relevante Rechtsrahmen besteht in der Datenschutzrichtlinie (95/46/EG). Die Datenschutzgruppe hat bereits in WP 80 darauf hingewiesen, dass biometrische Daten in den meisten Fällen personenbezogene Daten sind. Entsprechend dürfen diese Daten nur dann verarbeitet werden, wenn eine rechtliche Grundlage besteht und wenn die Verarbeitung gemessen am Zweck der jeweiligen Erfassung und/oder Weiterverarbeitung der Daten in angemessener, relevanter und nicht übermäßiger Form erfolgt.

Zweck

Eine Voraussetzung für die Verwendung biometrischer Daten ist eine klare Definition des Zwecks, für den die biometrischen Daten erfasst und verarbeitet werden. Dabei sind die Risiken im Hinblick auf den Schutz grundlegender individueller Rechte und Freiheiten zu berücksichtigen.

Biometrische Daten können beispielsweise erfasst werden, um die Sicherheit von Verarbeitungssystemen zu gewährleisten oder zu erhöhen, indem personenbezogene Daten durch geeignete Maßnahmen vor unbefugtem Zugriff geschützt werden. Grundsätzlich spricht nichts gegen die Einführung geeigneter Sicherheitsmaßnahmen unter Einbeziehung biometrischer Merkmale der für die Verarbeitung verantwortlichen Personen, um ein Sicherheitsniveau gewährleisten zu können, das den mit den betreffenden Verfahren verbundenen Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Dabei sollte allerdings berücksichtigt werden, dass die Nutzung biometrischer Informationen an sich noch keinen Sicherheitsgewinn bedeutet. Zahlreiche biometrische

Daten können nämlich ohne Wissen der betreffenden Person beschafft werden. Je höher das angestrebte Sicherheitsniveau, desto weniger werden biometrische Daten alleine geeignet sein, dieses Ziel zu verwirklichen.

Der Grundsatz der Zweckbindung ist ebenso zu berücksichtigen wie die übrigen Grundsätze des Datenschutzes. Bei der Festlegung der unterschiedlichen Zwecke einer Anwendung sind insbesondere die Grundsätze der Verhältnismäßigkeit, der Notwendigkeit und der Datenminimierung zu beachten. Bei Anwendungen mit unterschiedlichen Funktionen muss die betroffene Person nach Möglichkeit zwischen den jeweiligen Zwecken wählen können. Dies gilt insbesondere, wenn einer oder mehrere Zwecke die Verarbeitung biometrischer Daten erfordern.

Beispiel:
Die Verwendung elektronischer Geräte mit spezifischen Authentifikationsverfahren auf der Grundlage biometrischer Daten wurde in Verbindung mit geeigneten Sicherheitsmaßnahmen in den folgenden Fällen empfohlen:

- Verarbeitung personenbezogener Daten, die von Fernmeldebetreibern durch Abhören mit richterlicher Genehmigung erlangt wurden;
- Zugang zu Verkehrsdaten (und zu Standortdaten), die für gerichtliche Zwecke von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze aufbewahrt werden, und Zugang zu den Räumlichkeiten, in denen diese Daten verarbeitet werden;
- Erfassung und Speicherung genetischer Daten und biologischer Proben.

Fotos im Internet, in sozialen Medien und in Online-Anwendungen zur Verwaltung und Weitergabe von Fotos dürfen nicht zur Erstellung biometrischer Templates oder zum Einlesen von Daten in ein System verwendet werden, das die automatische Erkennung der fotografierten Personen (Gesichtserkennung) ermöglichen würde, ohne dass eine konkrete Rechtsgrundlage (z. B. eine Einwilligung) für diesen neuen Zweck gegeben wäre. Auch wenn eine Rechtsgrundlage für diesen nachgeordneten Verarbeitungszweck besteht, muss die Verarbeitung bezogen auf diesen Zweck angemessen und relevant sein, und die Verarbeitung darf nicht in übermäßigem Umfang erfolgen. Wenn die betroffene Person eingewilligt hat, dass Fotos, auf denen diese Person zu sehen ist, automatisch derart verarbeitet werden, dass die Personen in einem Online-Fotoalbum mit einem Algorithmus zur Gesichtserkennung identifiziert werden können, muss diese Verarbeitung unter Berücksichtigung der geltenden Datenschutzvorschriften erfolgen. Biometrische Daten, die nach der Kennzeichnung der Bilder mit dem Namen, einem Benutzernamen oder einem sonstigen von der betroffenen Person eingegebenen Text nicht mehr benötigt werden, müssen gelöscht werden. Die Erzeugung einer permanenten Datenbank mit biometrischen Daten ist für diesen Zweck nicht unbedingt nicht erforderlich.

Verhältnismäßigkeit

Bei der Nutzung biometrischer Daten stellt sich die Frage der Verhältnismäßigkeit der in den einzelnen Kategorien verarbeiteten Daten vor dem Hintergrund des Zwecks der jeweiligen Verarbeitung. Da biometrische Daten nur dann verwendet werden können, wenn sie angemessen und relevant sind und nicht in übermäßigem Umfang erfasst werden, müssen die Notwendigkeit und die Verhältnismäßigkeit der Verarbeitung streng geprüft werden. Außerdem muss geprüft werden, ob der beabsichtigte Zweck nicht auch unter stärkerer Respektierung der Privatsphäre erreicht werden könnte.

Bei der Analyse der Verhältnismäßigkeit eines vorgeschlagenen biometrischen Systems ist vorab zu prüfen, ob das System erforderlich ist, um den ermittelten Zweck zu erfüllen, d. h., ob dieses System für die Erfüllung dieses Zwecks tatsächlich wesentlich ist oder bloß die bequemste oder kostengünstigste Lösung darstellt. Ein zweiter Faktor ist, ob das System zur Erfüllung des vorgesehenen Zwecks wahrscheinlich effizient ist. In diesem Zusammenhang sind die spezifischen Merkmale der vorgesehenen biometrischen Technologie zu berücksichtigen.[1] Ein dritter Aspekt besteht in der Abwägung, ob die zu erwartende Beeinträchtigung der Privatsphäre im Verhältnis zum erwarteten Nutzen steht. Wenn dieser Nutzen verhältnismäßig gering ist und beispielsweise nur in erhöhter Bequemlichkeit oder in einer geringen Kosteneinsparung besteht, ist die Beeinträchtigung der Privatsphäre nicht als verhältnismäßig zu bewerten. Der vierte Aspekt für die Bewertung der Angemessenheit eines biometrischen Systems besteht in der Prüfung, ob das gewünschte Ergebnis nicht auch mit Mitteln erreicht werden könnte, welche die Privatsphäre weniger beeinträchtigen würden.[2]

Beispiel:
In einem Health- und Fitness-Club wird ein zentrales biometrisches System eingerichtet, das aufgrund der erfassten Fingerabdrücke Zugang zu den Trainingsräumen und zu den entsprechenden Einrichtungen nur den Kunden gewähren soll, die ihre Beiträge ordnungsgemäß gezahlt haben.
Um dieses System einsetzen zu können, müssen die Fingerabdrücke aller Kunden und aller Mitarbeiter erfasst werden. Diese biometrische Anwendung scheint gemessen an der Notwendigkeit der Kontrolle des Zugangs zum Club und der einfacheren Kundenverwaltung als unverhältnismäßig. Andere Maßnahmen wie z. B. die Verwendung einer einfachen Liste oder der Einsatz von RFID-Etiketten oder Magnetstreifenkarten, bei denen die Notwendigkeit der Verarbeitung biometrischer Daten entfiele, wären ebenso gut als praktikabel und wirksam vorstellbar.

Angesichts der potenziell schädlichen Folgen für die betreffenden Personen warnt die Datenschutzgruppe vor den Risiken einer Nutzung biometrischer Daten für Identifikationszwecke in großen zentralen Datenbanken.

Bei derartigen Systemen sollten die erheblichen Auswirkungen auf die Menschenwürde und auf die Grundrechte der betroffenen Personen berücksichtigt werden. Vor dem Hintergrund der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) sowie angesichts der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Zusammenhang mit Artikel 8 der Konvention betont die Datenschutzgruppe, dass jegliche Beeinträchtigung des Rechts auf Datenschutz nur unter der Bedingung zulässig ist, dass die Beeinträchtigung im Einklang mit geltenden Rechtsvorschriften steht und erforderlich ist, um in einer demokratischen Gesellschaft ein übergeordnetes öffentliches Interesse zu schützen.[3]

---

1 Biometrische Verfahren werden entweder für Verifikations- oder für Identifikationszwecke verwendet. Ein biometrischer Identifikator könnte aus technischer Sicht für einen Zweck geeignet und für den anderen Zweck als ungeeignet zu bewerten sein. (Technologien mit einer niedrigen FRR beispielsweise sollten vorzugsweise in Systemen für Identifikationszwecke in der Rechtsdurchsetzung eingesetzt werden.)

2 Beispielsweise mit Smart Cards oder mit sonstigen Methoden, bei denen biometrische Informationen für Authentifikationszwecke nicht erfasst oder zentral verwaltet werden.

3 Siehe Europäischer Gerichtshof, Urteil vom 20. Mai 2003 in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 (Rechnungshof/Österreichischer Rundfunk u. a.), Europäischer Gerichtshof für Menschenrechte, Urteil vom 4. Dezember 2008, Beschwerden Nrn. 30562/04 und 30566/04 (S. und

Um sicherzustellen, dass diese Voraussetzungen erfüllt werden, muss das Ziel spezifiziert werden, das mit dem jeweiligen System verfolgt werden soll. Außerdem muss die Verhältnismäßigkeit der in das System einzubindenden Daten gemessen am betreffenden Ziel bewertet werden.

Dazu muss der für die Verarbeitung Verantwortliche feststellen, ob die Verarbeitung und die eingesetzten Mechanismen sowie die Kategorien der zu erfassenden und zu verarbeitenden Daten und der Transfer der in der Datenbank enthaltenen Informationen notwendig und unumgänglich sind. Die getroffenen Sicherheitsmaßnahmen müssen angemessen und wirksam sein. Der für die Verarbeitung Verantwortliche muss die Rechte der Personen berücksichtigen, auf die sich die jeweiligen personenbezogenen Daten beziehen. Außerdem muss der für die Verarbeitung Verantwortliche sicherstellen, dass ein geeigneter Mechanismus zur Anwendung kommt, um die Wahrnehmung dieser Rechte zu ermöglichen.

Beispiel:
Nutzung biometrischer Daten für Identifikationszwecke: Systeme, die das Gesicht oder die DNA einer Person analysieren, können in erheblichem Umfang zur Bekämpfung von Kriminalität und zur Feststellung der Identität einer unbekannten Person beitragen, die einer schweren Straftat verdächtigt wird. Wenn diese Systeme allerdings in großem Umfang eingesetzt werden, können sie auch mit schwerwiegenden Nachteilen einhergehen. Durch Gesichtserkennung können biometrische Daten ohne Wissen der betroffenen Person leicht für vielfältige Nutzungsmöglichkeiten erfasst werden. Der zunehmende Einsatz dieser Technologie würde der Anonymität in öffentlichen Räumen ein Ende setzen und die konsequente Verfolgung einzelner Personen ermöglichen. Technologien zur Analyse von DNA-Proben bergen die Gefahr, dass empfindliche Daten über die Gesundheit einer Person offen gelegt werden könnten.

Zuverlässigkeit

Biometrische Daten müssen zuverlässig und für den jeweiligen Zweck der Erfassung relevant sein. Die erforderliche Zuverlässigkeit muss sowohl bei der Erfassung als auch bei der Herstellung der Verbindung zwischen einer Person und den betreffenden biometrischen Daten gegeben sein. Die Zuverlässigkeit zum Zeitpunkt der Erfassung ist unter anderem im Hinblick auf die Verhinderung eines Identitätsbetrugs von Bedeutung.

Biometrische Daten sind individuell, und biometrische Daten ergeben meist individuelle Templates oder Bilder. Bei Nutzung in großem Umfang und insbesondere in Verbindung mit einem erheblichen Anteil der Bevölkerung können biometrische Daten als „Kennzeichen allgemeiner Bedeutung“ gemäß der Richtlinie 95/46/EG betrachtet werden. In diesem Fall kommt Artikel 8 Absatz 7 der Richtlinie 95/46/EG zur Anwendung, und die Mitgliedstaaten sind entsprechend verpflichtet, die jeweiligen Verarbeitungsbedingungen zu prüfen.

Marper/Vereinigtes Königreich) und Urteil vom 19. Juli 2011, Beschwerden Nrn. 30089/04, 14449/06, 24968/07, 13870/08, 36363/08, 23499/09, 43852/09 und 64027/09 (Goggins u. a./Vereinigtes Königreich).

Datenminimierung

Eine besondere Schwierigkeit kann sich dadurch ergeben, dass biometrische Daten häufig mehr Informationen erfassen als für den eigentlichen Abgleich erforderlich. Der Grundsatz der Datenminimierung ist vom für die Verarbeitung Verantwortlichen durchzusetzen. Dies bedeutet erstens, dass nicht sämtliche verfügbaren Informationen, sondern nur die tatsächlich benötigten Informationen verarbeitet, übertragen und gespeichert werden sollten. Und zweitens sollte der für die Verarbeitung Verantwortliche sicherstellen, dass bereits die Standardkonfiguration des betreffenden Systems den Datenschutz fördert, ohne dass besondere Maßnahmen zur Durchsetzung des Datenschutzes getroffen werden müssen.

Aufbewahrungsfrist

Der für die Verarbeitung Verantwortliche sollte eine Aufbewahrungsfrist für biometrische Daten festlegen, die nicht länger ist als für die Zwecke der Erfassung oder der Weiterverarbeitung der Daten tatsächlich erforderlich. Er muss sicherstellen, dass die Daten und die von diesen Daten abgeleiteten Profile nach diesem als berechtigt zu betrachtenden Zeitraum unwiderruflich gelöscht werden.

Dabei muss eindeutig zwischen allgemeinen personenbezogenen Daten, die vielleicht über einen längeren Zeitraum benötigt werden, und biometrischen Daten unterschieden werden, die nicht mehr von Bedeutung sind (beispielsweise, weil die betroffene Person zu einem bestimmten Bereich ohnehin keinen Zutritt mehr hat).

Beispiel:
Ein Arbeitgeber setzt ein biometrisches System ein, um den Zugang zu einem bestimmten Bereich einzuschränken. Die Tätigkeit eines Mitarbeiters setzt nicht mehr voraus, dass dieser Mitarbeiter Zugang zu dem betreffenden Bereich hat (etwa weil sich die Zuständigkeit des Mitarbeiters geändert hat oder weil der Mitarbeiter inzwischen bei einem anderen Arbeitgeber beschäftigt ist). In diesem Fall müssen die betreffenden biometrischen Daten gelöscht werden, da der ursprüngliche Erfassungszweck nicht mehr gegeben ist.

3.1. Rechtmäßiger Grund

Die Verarbeitung biometrischer Daten muss aus den in Artikel 7 der Richtlinie 95/46/EG genannten rechtmäßigen Gründen erfolgen.

3.1.1. Einwilligung, Artikel 7 Buchstabe a

Der erste in Artikel 7 Buchstabe a genannte rechtmäßige Grund ist die Einwilligung der betroffenen Person zur Verarbeitung ihrer Daten. Gemäß Artikel 2 Buchstabe h der Datenschutzrichtlinie muss die Einwilligung der betroffenen Person ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgen. Diese Einwilligung wird allerdings dann selbstverständlich nicht ohne Zwang erlangt, wenn allgemeine Geschäftsbedingungen oder Sonderregelungen zwingend vorgeschrieben sind. Außerdem muss die Einwilligung widerruflich sein. In diesem Zusammenhang möchte die Datenschutzgruppe in ihrer Stellungnahme zum Begriff der Einwilligung auf einige wichtige Aspekte hinweisen: die Gültigkeit der Einwilligung, das individuelle Recht zum Widerruf der Einwilligung, die Notwendigkeit der Erteilung der Einwilligung vor Beginn der Verarbeitung und die Anforderungen bezüglich der Qualität und der Zugänglichkeit der Informationen.[4]

[4] WP 187, Stellungnahme 15/2011 zum Begriff der Einwilligung.

In vielen Fällen, in denen biometrische Daten verarbeitet werden, ist eine Einwilligung unter Umständen nicht als freiwillig erteilt zu bewerten. Dies gilt beispielsweise dann, wenn keine gültige Alternative wie z. B. die Eingabe eines Kennwortes oder die Verwendung einer Magnetstreifenkarte verfügbar ist. Ein System, das betroffene Personen von einer Nutzung dieses Systems abhalten würde (beispielsweise weil die Nutzung für die Benutzer zu zeitaufwendig oder zu kompliziert wäre), könnte nicht als gültige Alternative betrachtet werden. Entsprechend wäre auch eine erteilte Einwilligung nicht als gültig zu bewerten.

Beispiele:
Wenn keine sonstigen rechtmäßigen Gründe gegeben sind, könnte ein biometrisches Authentifikationssystem nur dann als Zugangskontrolle für einen Videoclub eingesetzt werden, wenn die Kunden frei entscheiden können, ob sie das betreffende System tatsächlich nutzen möchten. Entsprechend muss der Besitzer des Videoclubs Mechanismen bereitstellen, welche die Privatsphäre der Kunden weniger beeinträchtigen. Die betreffenden Mechanismen würden auch den Kunden Zugang gewähren, die aus persönlichen Gründen nicht bereit oder nicht in der Lage sind, die Zugangskontrolle durch Fingerabdrücke zu nutzen. Wenn als einzige Möglichkeit anstelle der geforderten Einwilligung zur Nutzung der individuellen biometrischen Daten der Verzicht auf das betreffende Angebot bleibt, ist dies ein deutlicher Anhaltspunkt dafür, dass die Einwilligung nicht freiwillig erteilt wurde und somit nicht als rechtmäßiger Grund bewertet werden kann.

In einem Kindergarten wird ein Venenstruktur-Scanner eingerichtet, um die Zugangsberechtigung sämtlicher Erwachsener (Eltern, Erzieher und Verwaltungspersonal) zu prüfen. Um dieses System einsetzen zu können, müssen die Fingerabdrücke aller Eltern und aller Mitarbeiter erfasst werden. Eine Einwilligungsregelung wäre eine fragliche Rechtsgrundlage insbesondere für die Mitarbeiter, da diesen im Grunde keine Wahl bleibt, als die geforderte Einwilligung zu diesem System zu erteilen. Auch für die Eltern wäre diese Regelung zweifelhaft, da keine alternative Möglichkeit gegeben wäre, Zugang zum Kindergarten zu erhalten.

Es kann zwar mit hoher Wahrscheinlichkeit angenommen werden, dass die Einwilligung wegen des typischen Ungleichgewichts zwischen Arbeitgebern und Arbeitnehmern nicht allzu aussagekräftig wäre. Die Datenschutzgruppe kann die Glaubwürdigkeit der Einwilligung jedoch auch nicht vollständig ausschließen, „*sofern hinreichende Garantien dafür bestehen, dass die Einwilligung tatsächlich freiwillig erteilt wurde*“.[5]

Insoweit sind Einwilligungen im Zusammenhang mit Beschäftigungsverhältnissen grundsätzlich zu prüfen, und entsprechende Regelungen müssen angemessen gerechtfertigt sein. Statt eine Einwilligung anzustreben, könnten Arbeitgeber prüfen, ob die Verwendung biometrischer Daten von Mitarbeitern für einen rechtmäßigen Zweck nachweislich erforderlich ist und ob die gegebenenfalls festgestellte Notwendigkeit nicht zu einer Beeinträchtigung der Grundrechte und Freiheiten der Mitarbeiter führt. Wenn die Notwendigkeit angemessen begründet werden kann, könnte das rechtmäßige Interesse des für die Verarbeitung Verantwortlichen gemäß Artikel 7 Buchstabe f der Richtlinie 95/46/EG die Rechtsgrundlage für eine Verarbeitung sein. Der Arbeitgeber muss immer bestrebt sein, das die Privatsphäre am wenigsten beeinträchtigende Verfahren einzusetzen und nach Möglichkeit auf biometrische Prozesse zu verzichten.

[5] WP 187, Stellungnahme 15/2011 zum Begriff der Einwilligung.

Wie in Abschnitt 3.1.3, beschrieben, können jedoch Fälle vorkommen, in denen ein biometrisches System im rechtmäßigen Interesse des für die Verarbeitung Verantwortlichen liegen kann. In diesen Fällen wäre eine Einwilligung nicht erforderlich.

Eine Einwilligung ist nur dann gültig, wenn hinreichende Auskünfte zur Verwendung der biometrischen Daten erteilt werden. Da biometrische Daten als individuelle und universale Identifikatoren dienen können, ist die Bereitstellung klarer und leicht zugänglicher Informationen über die Nutzung der jeweiligen Daten als unabdingbare Voraussetzung für eine faire Verarbeitung zu betrachten. Dies ist entsprechend eine entscheidende Bedingung für das Vorliegen einer gültigen Einwilligung im Zusammenhang mit der Nutzung biometrischer Daten.

Beispiele:
Eine gültige Einwilligung zur Nutzung eines Zugangskontrollsystems unter Verwendung von Fingerabdrücken setzt voraus, dass darüber informiert wurde, ob das betreffende biometrische System ein für dieses System spezifisches Template erzeugt. Wenn ein eingesetzter Algorithmus dasselbe biometrische Template auch in anderen biometrischen Systemen erzeugt, muss die betroffene Person wissen, dass sie in auch in anderen biometrischen Systemen wiedererkannt werden könnte.

Ein Nutzer lädt sein Foto in ein Fotoalbum im Internet hoch. Die Erfassung dieses Fotos in einem biometrischen System erfordert eine ausdrückliche Einwilligung auf der Grundlage umfassender Informationen dahin gehend, was mit den biometrischen Daten geschieht und für welchen Zeitraum und für welche Zwecke die Daten verarbeitet werden.

Eine Einwilligung kann jederzeit widerrufen werden, wenn die für die Verarbeitung Verantwortlichen genötigt sind, technische Einrichtungen in ihre Systeme aufzunehmen, welche die Nutzung biometrischer Daten in ihren Systemen erheblich verändern könnten. Ein biometrisches System, das auf der Grundlage einer Einwilligung genutzt wird, muss daher in der Lage sein, sämtliche von diesem System erzeugten Verknüpfungen mit einer bestimmten Identität wirksam rückgängig zu machen.

3.1.2. Vertrag, Artikel 7 Buchstabe b

Die Verarbeitung biometrischer Daten kann für die Erfüllung eines Vertrags erforderlich sein, an dem die betroffene Person als Partei beteiligt ist. Ebenso kann die Verarbeitung der Daten Voraussetzung für die Durchführung vorvertraglicher Maßnahmen sein, die auf Antrag der betroffenen Person erfolgen. Allerdings ist darauf hinzuweisen, dass dies im Allgemeinen nur für ausschließlich biometrische Dienste von Bedeutung ist. Diese Rechtsgrundlage kann nicht zur Legitimierung einer nachgeordneten Leistung herangezogen werden, die darin bestünde, eine Person in einem biometrischen System zu erfassen. Wenn eine derartige Leistung von der eigentlichen Leistung getrennt werden kann, ist der Vertrag über die eigentliche Leistung nicht als rechtmäßige Grundlage für die Verarbeitung biometrischer Daten zu betrachten. Personenbezogene Daten sind keine Güter, die als Gegenleistung für eine erbrachte Leistung verlangt werden könnten. Daher können entsprechende Verträge sowie Verträge, denen zufolge eine Leistung nur unter der Bedingung erbracht wird, dass jemand zur Verarbeitung seiner biometrischen Daten im Gegenzug für eine anderweitige Leistung zustimmt, keine Rechtsgrundlage für eine derartige Verarbeitung sein.

Beispiele:
a) Zwei Brüder geben in einem Labor Haarproben für eine DNA-Analyse ab, um festzustellen, ob sie tatsächlich leibliche Brüder sind. Der mit diesem Labor geschlossene Vertrag über die Durchführung dieser Analyse stellt eine hinreichende Rechtsgrundlage für die Erfassung und die Verarbeitung der betreffenden biometrischen Daten dar.

b) Jemand lädt in einem sozialen Netz ein Foto in sein Fotoalbum hoch, um seinen Freunden dieses Foto zeigen zu können. Wenn die vertraglichen Bestimmungen (Nutzungsbedingungen) die Inanspruchnahme des betreffenden Dienstes daran knüpfen, dass der jeweilige Nutzer in einem biometrischen System erfasst wird, ist diese Bestimmung nicht als hinreichende Rechtsgrundlage für die Erfassung der Daten zu bewerten.

3.1.3. Rechtliche Verpflichtung, Artikel 7 Buchstabe c

Ein weiterer Rechtsgrund für die Verarbeitung personenbezogener Daten ist gegeben, wenn die Verarbeitung erforderlich ist, um eine rechtliche Verpflichtung des für die Verarbeitung Verantwortlichen zu erfüllen. In manchen Ländern ist dies beispielsweise bei der Erstellung und/oder Vorlage von Reisepässen[6] und Visa[7] erforderlich.

3.1.4. Berechtigtes Interesse des für die Verarbeitung Verantwortlichen, Artikel 7 Buchstabe f

Gemäß Artikel 7 der Richtlinie 95/46/EG kann die Verarbeitung biometrischer personenbezogener Daten auch dann gerechtfertigt sein, wenn diese Daten „*zur Verwirklichung des berechtigten Interesses* [erforderlich sind], *das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiege*n."

Insoweit kann es vorkommen, dass die Verwendung biometrischer Systeme im berechtigten Interesse des für die Verarbeitung Verantwortlichen liegt. Das Interesse ist jedoch nur dann berechtigt, wenn der für die Verarbeitung Verantwortliche nachweisen kann, dass sein Interesse objektiv stärker wiegt als das Recht der betroffenen Personen darauf, der Erfassung in einem biometrischen System zu widersprechen. Wenn beispielsweise die Sicherheit von

---

6 In Reisepässe wurden Fingerabdrücke gemäß der Verordnung (EU) 2252/2004 des Rates vom 13. Dezember 2004 aufgenommen. Rechtsgrundlage für die Aufnahme von Fingerabdrücken in Aufenthaltstitel ist die Verordnung (EU) 1030/2002 des Rates vom 13. Juni 2002.

7 Die Registrierung biometrischer Identifikatoren in das Visa-Informationssystem (VIS) ist in der Verordnung (EG) Nr. 767/2008 l vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) geregelt; siehe auch Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 endg.). WP 134; Stellungnahme 2/2005 – Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (KOM (2004) 835 endgültig) WP 110; Stellungnahme Nr. 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems VIS, WP 96.

Hochrisikobereichen durch einen speziellen Mechanismus gewährleistet werden muss, mit dem genau geprüft werden kann, ob Personen tatsächlich zugangsberechtigt sind, kann die Verwendung eines biometrischen Systems als im berechtigten Interesse des für die Verarbeitung Verantwortlichen liegend bewertet werden. Im folgenden Beispiel eines biometrischen Systems zur Kontrolle des Zugangs zu einem Labor ist ein angemessener Schutz dieses Bereichs durch Maßnahmen, welche die Privatsphäre weniger beeinträchtigen würden, nicht verfügbar. Daher kann der für die Verarbeitung Verantwortliche den Mitarbeitern keinen alternativen Mechanismus anbieten, ohne die Sicherheit des zu schützenden Bereichs zu beeinträchtigen. Insoweit liegt es im berechtigten Interesse des für die Verarbeitung Verantwortlichen, das betreffende System einzurichten und eine begrenzte Anzahl an Mitarbeitern zu erfassen. Die Einwilligung dieser Mitarbeiter ist dazu nicht erforderlich. Auch wenn ein berechtigtes Interesse des für die Verarbeitung Verantwortlichen als gültiger Rechtsgrund für die Verarbeitung zu bewerten ist, sind alle sonstigen Grundsätze des Datenschutzes zu beachten, insbesondere der Grundsatz der Verhältnismäßigkeit und der Datenminimierung.

Beispiel:
In einem Unternehmen, das an gefährlichen Viren forscht, ist das Labor durch Türen geschützt, die erst nach erfolgreicher Prüfung eines Fingerabdrucks und nach einer Iris-Erkennung geöffnet werden. Dieser Kontrollmechanismus wurde eingerichtet, um sicherzustellen, dass nur die mit den jeweiligen Risiken vertrauten, für die betreffenden Verfahren geschulten und von dem jeweiligen Unternehmen für vertrauenswürdig befundenen Personen Versuche mit diesen gefährlichen Materialien durchführen können. Das berechtigte Interesse des Unternehmens, sicherzustellen, dass nur die betreffenden Personen Zugang zu einem geschützten Bereich erhalten, um auf diese Weise die mit einem Zutritt verbundenen Sicherheitsrisiken zu reduzieren, wiegt erheblich stärker als der etwaige Wunsch der jeweiligen Personen, eine Verarbeitung ihrer biometrischen Daten zu verhindern.

Grundsätzlich kann die Verwendung biometrischer Daten im Interesse der allgemeinen Sicherheit von Vermögenswerten und von Personen nicht als berechtigtes Interesse betrachtet werden, das gegenüber den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen überwiegen würde. Im Gegenteil: Die Verarbeitung biometrischer Daten ist nur dann als erforderliches Mittel zur Gewährleistung der Sicherheit von Vermögenswerten und/oder von Personen zu bewerten, wenn anhand objektiver und dokumentierter Umstände nachgewiesen werden kann, dass im konkreten Fall ein erhebliches Risiko besteht. Dazu muss der für die Verarbeitung Verantwortliche nachweisen, dass die betreffenden Gegebenheiten ein konkretes und erhebliches Risiko bedingen, das der für die Verarbeitung Verantwortliche mit besonderer Sorgfalt bewerten muss. Um dem Grundsatz der Verhältnismäßigkeit gerecht zu werden, muss der für die Verarbeitung Verantwortliche bei derart hohen Risiken prüfen, ob alternative Maßnahmen verfügbar sind, mit denen die angestrebten Ziele ebenso verwirklicht werden könnten, die Privatsphäre der betroffenen Personen aber weniger beeinträchtigt würde. Wenn derartige alternative Maßnahmen in Betracht kommen, ist der für die Verarbeitung Verantwortliche verpflichtet, diese alternativen Möglichkeiten zu nutzen.
Außerdem sollte regelmäßig geprüft werden, ob die betreffenden Gegebenheiten immer noch bestehen. Aufgrund dieser Prüfungen müssen jegliche Verarbeitungsprozesse, die sich als nicht mehr gerechtfertigt erweisen, eingestellt oder zumindest ausgesetzt werden.

3.2. Für die Verarbeitung Verantwortliche und Auftragsverarbeiter

Gemäß der Richtlinie 95/46/EG unterliegen die für die Verarbeitung Verantwortlichen bei der Verarbeitung personenbezogener Daten bestimmten Verpflichtungen. Im Zusammenhang mit biometrischen Daten können unterschiedliche Typen von Rechtssubjekten (z. B. Arbeitgeber, Rechtsdurchsetzungsbehörden oder Einwanderungsbehörden) die Funktion des für die Verarbeitung Verantwortlichen übernehmen.

Die Datenschutzgruppe erinnert an die Leitlinien in ihrer Stellungnahme zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".[8] Diese Stellungnahme enthält eindeutige Erläuterungen dahin gehend, wie diese Kernbegriffe der Richtlinie zu verstehen sind.

3.3. Automatisierte Verarbeitung (Artikel 15 der Richtlinie)

Wenn auf der Verarbeitung biometrischer Daten beruhende Systeme eingesetzt werden, sollte sorgfältig auf potenziell diskriminierende Folgen für die vom System zurückgewiesenen Personen geachtet werden. Wenn eine Maßnahme eine natürliche Person beeinträchtigen könnte, weil die Datenverarbeitung ausschließlich automatisch erfolgt, sind zudem geeignete Garantien vorzusehen (z. B. die Möglichkeit manueller Eingriffe sowie Abhilfemaßnahmen oder Mechanismen, die den betroffenen Personen die Darstellung ihrer Standpunkte ermöglichen), damit das individuelle Recht darauf gewahrt werden kann, sich der Unterwerfung unter diese Maßnahme zu entziehen.

In Artikel 15 der Richtlinie 95/46/EG heißt es: *„Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens."*

3.4. Transparenz und Aufklärung der betroffenen Person

Gemäß dem Grundsatz von Treu und Glauben bei der Verarbeitung muss betroffenen Personen bekannt sein, dass ihre biometrischen Daten erfasst und/oder verwendet werden (Artikel 6 der Richtlinie 95/46/EG). Jegliche Systeme, die derartige Daten ohne Wissen der betroffenen Personen erfassen würden, sind zu vermeiden.

Der für die Verarbeitung Verantwortliche muss sicherstellen, dass die betroffenen Personen über die wesentlichen Elemente der Verarbeitung gemäß Artikel 10 der Datenschutzrichtlinie (Identität des für die Verarbeitung Verantwortlichen, Zweckbestimmung der Verarbeitung, Datentyp, Dauer der Verarbeitung Zugriffs-, Änderungs- und Löschungsrechte der betroffenen Personen, das Recht der betroffenen Personen zum Widerruf ihrer Einwilligung und Informationen über die Empfänger bzw. über die Empfängerkategorien, denen die jeweiligen Daten offen gelegt werden) angemessen unterrichtet werden. Da der für die Verarbeitung Verantwortliche bei biometrischen Systemen verpflichtet ist, die betroffene Person entsprechend zu unterrichten, dürfen biometrische Daten nicht ohne Wissen der betroffenen Personen erfasst werden.

---

[8] WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".

3.5. Recht auf Zugang zu biometrischen Daten

Betroffene Personen haben einen Anspruch darauf, dass die für die Verarbeitung Verantwortlichen ihnen Zugang zu ihren Daten (im Allgemeinen einschließlich ihrer biometrischen Daten) gewähren. Außerdem haben betroffene Personen ein Anrecht auf Zugang zu möglichen Profilen, die auf der Grundlage dieser biometrischen Daten erstellt werden. Wenn der für die Verarbeitung Verantwortliche die Identität der betroffenen Personen prüfen muss, um diesen Zugang zu gewähren, ist entscheidend, dass dies geschieht, ohne weitere personenbezogene Daten zu verarbeiten.

3.6. Datensicherheit

Die für die Verarbeitung Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen treffen, um die zufällige oder unbefugte Zerstörung, den zufälligen Verlust, die unbefugte Änderung oder Weitergabe, den ungefugten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und die unbefugte Verarbeitung personenbezogener Daten in jeglicher sonstiger Form zu verhindern.[9]

Alle erfassten und gespeicherten Daten müssen angemessen gesichert werden. Mit der Auslegung eines Systems befasste Personen müssen durch Hinzuziehung geeigneter Sicherheitsexperten sicherstellen, dass Sicherheitsbedrohungen in angemessener Weise gehandhabt werden. Dies gilt insbesondere für die Portierung bestehender Systeme auf das Internet.

3.7. Garantien für Personen mit besonderen Bedürfnissen

Die Verwendung biometrischer Daten kann die Würde, die Privatsphäre und das Recht auf Datenschutz gefährdeter Personen (z. B. kleiner Kinder und älterer Menschen) sowie derjenigen beeinträchtigen, die aus körperlichen Gründen nicht in der Lage sind, sich dem Erfassungsprozess zu unterziehen. In Anbetracht der potenziell nachteiligen Konsequenzen für die betroffenen Personen müssen bei der Folgenabschätzung im Hinblick auf sämtliche Maßnahmen, welche die Würde einer Person beeinträchtigen könnten, strengere Anforderungen erfüllt werden. In diesem Zusammenhang sind die Notwendigkeit und die Verhältnismäßigkeit der Maßnahmen sowie die der jeweils betroffenen Person verbleibenden Möglichkeiten zur Wahrnehmung ihrer Datenschutzrechte zu prüfen, damit die betreffende Maßnahme als zulässig bewertet werden kann. Dem Risiko einer Stigmatisierung und Diskriminierung der betreffenden Personen aufgrund ihres Alters oder infolge der Tatsache, dass es bestimmten Personen nicht möglich ist, die betreffenden Systeme zu nutzen, muss durch geeignete Garantien begegnet werden.

Bezüglich der Einführung einer allgemeinen rechtlichen Verpflichtung zur Erfassung biometrischer Identifikatoren für diese Gruppen (insbesondere für kleine Kinder und für ältere Menschen) im Zusammenhang mit Identifikationen im Rahmen von Grenzkontrollen ist die Datenschutzgruppe der Ansicht, *„dass die Erfassung und die Verarbeitung der Fingerabdrücke – im Interesse der Würde des Betreffenden und der Zuverlässigkeit des Verfahrens – bei Kindern und älteren Menschen eingeschränkt werden sollten und dass die Altersgrenzen den für andere große biometrische Datenbanken der EU (insbesondere Eurodac) geltenden Altersgrenzen entsprechen sollten.“*[10]

---

[9] Artikel 17 Absatz 1 der Richtlinie 95/46/EG.

[10] WP 134 – Stellungnahme Nr. 3/2007 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme

In jedem Fall sollten spezifische Garantien (z. B. geeignete Alternativverfahren) eingerichtet werden, um die Wahrung der Menschenwürde und der Grundrechte von Personen sicherzustellen, bei denen eine Erfassung nicht möglich ist, und um auszuschließen, dass diese Personen Opfer eines unzulänglichen technischen Systems werden.[11]

3.8. Sensible Daten

Gewisse biometrische Daten können als sensible Daten gemäß Artikel 8 der Richtlinie 95/46/EC betrachtet werden. Dies gilt insbesondere für Daten, aus denen die rassische und ethnische Herkunft hervorgehen, sowie für Gesundheitsdaten. Die DNA-Daten einer Person beispielsweise enthalten häufig auch Daten über die Gesundheit der betreffenden Person oder können Aufschluss über die rassische oder die ethnische Herkunft geben. In diesem Fall sind DNA-Daten als sensible Daten zu betrachten, bei denen zusätzlich zu den allgemeinen Grundsätzen des Datenschutzes gemäß der Richtlinie die in Artikel 8 vorgesehenen besonderen Garantien zu berücksichtigen sind. Bei der Bewertung der Sensibilität der mit einem biometrischen System zu verarbeitenden Daten sollten auch die Umstände der Verarbeitung berücksichtigt werden.[12]

3.9. Die Rolle nationaler Datenschutzbehörden

Angesichts der zunehmenden Normierung der Interoperabilität biometrischer Technologien wird allgemein anerkannt, dass die zentrale Speicherung biometrischer Daten sowohl die Gefahr der Nutzung biometrischer Daten zur Verknüpfung von Datenbanken (mit der Möglichkeit der Erzeugung detaillierter Profile einzelner Personen) als auch spezifische Risiken dahin gehend birgt, dass diese Daten – insbesondere bei unbefugten Zugriffen – zu nicht annehmbaren Zwecken genutzt werden.

Die Datenschutzgruppe empfiehlt, dass für Systeme, die biometrische Daten zur Verknüpfung von Datenbanken verwenden, zusätzliche Garantien vorgeschrieben werden, da diese Formen der Verarbeitung spezifische Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können (Artikel 20 der Richtlinie 95/46/EG). Um geeignete Garantien sicherzustellen und insbesondere um die Risiken für die betroffenen Personen zu mindern, sollte der jeweils für die Verarbeitung Verantwortliche die zuständige nationale Datenschutzbehörde konsultieren, bevor die betreffenden Maßnahmen eingeführt werden.

4. Neue Entwicklungen, technische Trends und Szenarien

4.1. Einleitung

Biometrische Technologien werden vorwiegend von Verwaltungsbehörden schon lange genutzt. In letzter Zeit spielen zunehmend auch kommerzielle Organisationen eine entscheidende Rolle bei der Nutzung dieser Technologien und bei der Entwicklung neuer Produkte.

Einer der wichtigsten Gründe für diese Entwicklung liegt darin, dass diese Technologien einen derartigen Reifegrad erlangt haben, dass biometrische Systeme, die ursprünglich nur unter kontrollierten Bedingungen gut funktionierten, inzwischen in großem Umfang auch in

---

biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006)269 endg.).

[11] Siehe WP 134 – Stellungnahme Nr. 3/2007, S. 8.

[12] Siehe WP 29, *Advice paper on special categories of data („sensitive data"), siehe* Ares (2011)444105 – 20.4.2011.

anderen Umgebungen eingesetzt werden können. Insoweit sind biometrische Daten manchmal als Ersatz für konventionelle Identifikationsmethoden oder als Verbesserung dieser Methoden zu betrachten. Dies gilt insbesondere für Methoden, die auf mehreren Identifikationsfaktoren beruhen und die etwa bei starken Authentifikationssystemen benötigt werden. Außerdem werden biometrische Technologien zunehmend in Anwendungen eingesetzt, mit denen Personen zwar mit geringerer Zuverlässigkeit, dafür aber rasch und bequem identifiziert werden können.

Die Nutzung biometrischer Technologien verlagert sich zudem allmählich vom ursprünglichen Anwendungsbereich hin zu neuen Einsatzgebieten: von der Identifikation und der Authentifikation hin zu Verhaltensanalysen, Überwachungen und Verfahren zur Betrugsbekämpfung.

Fortschritte bei Computer- und Netztechnologien tragen ebenfalls zur Entstehung gleichsam der zweiten Generation biometrischer Systeme bei. Diese Systeme beruhen auf der Analyse von Verhaltensweisen und psychologischen Merkmalen. Die Systeme werden entweder isoliert eingesetzt oder mit anderen klassischen Systemen zu multimodalen Systemen kombiniert. Und schließlich kommen biometrische Systeme zunehmend im Zusammenhang mit der intelligenten Erfassung von Umgebungen sowie mit den allgegenwärtigen neuen Entwicklungen im Bereich der Computertechnik zur Anwendung.

4.2. Neue Tendenzen bei biometrischen Systemen

Verschiedene biometrische Technologien können als ausgereifte Technologien betrachtet werden, die bei der Rechtsdurchsetzung sowie in der elektronischen Verwaltung (e-Government) und in kommerziellen Systemen zur Anwendung kommen. Zu den betreffenden Verfahren zählen die Erkennung von Fingerabdrücken und Handgeometrien, Iris-Erkennungen und gewisse Formen der Gesichtserkennung. Außerdem werden gewisse biometrische Technologien zur Analyse körperlicher Merkmale entwickelt. Einige dieser Technologien sind grundsätzlich neu; andere Technologien beziehen Impulse aus neuen Verarbeitungskapazitäten.

Typische Elemente dieser neuen Systeme sind die Einbeziehung körperlicher Merkmale zur Kategorisierung/Identifikation von Personen sowie die Möglichkeit der Erfassung der betreffenden Merkmale aus größeren Entfernungen. Die erfassten Daten werden zur Erstellung von Profilen sowie zur Fernüberwachung oder auch zu nochmals komplexeren Aufgaben (beispielsweise zur intelligenten Umgebungsüberwachung) genutzt.

Diese Möglichkeiten haben sich aus der kontinuierlichen Entwicklung von Sensoren ergeben, welche die Erfassung neuer physiologischer Merkmale ermöglichen und neue Wege zur Verarbeitung traditioneller biometrischer Daten erschließen.

Zu beachten ist auch die Nutzung der sogenannten weichen biometrischen Daten. Die berücksichtigten sehr allgemeinen Merkmale ermöglichen zwar keine eindeutige Identifikation von Personen, können aber dazu beitragen, die Leistungsfähigkeit anderer Identifikationssysteme zu verbessern.

Ein weiteres wesentliches Merkmal der neuen biometrischen Systeme ist das Potenzial zur Erfassung von Informationen aus größerer Entfernung oder zur Erfassung im Laufe von Bewegungen, ohne dass dazu eine Unterstützung oder Mitwirkung der betreffenden Person erforderlich wäre. Wenngleich diese Technologie noch nicht vollständig ausgereift ist, werden doch gewaltige Anstrengungen insbesondere im Bereich der Rechtsdurchsetzung unternommen.

Außerdem ist die rasche Verbreitung multimodaler Systeme festzustellen, die mehrere biometrische Merkmale gleichzeitig berücksichtigen bzw. die biometrische Daten jeweils mehrfach erfassen oder bestimmen, und die so angepasst werden können, dass die Balance zwischen der Sicherheit und der bequemen Handhabbarkeit biometrischer Systeme verbessert werden kann. Durch den Einsatz dieser Systeme können die FAR reduziert, die Leistungen von Erkennungssystemen verbessert und die Erfassung von Daten umfangreicherer Populationen erleichtert werden, indem mit ergänzenden Datenquellen ein Ausgleich für die mangelnde Universalität einer Quelle biometrischer Daten geschaffen wird.

Biometrische Systeme werden sowohl im öffentlichen als auch im privaten Bereich zunehmend eingesetzt. Im öffentlichen Sektor werden biometrische Daten traditionell in der Rechtsdurchsetzung genutzt. Im Finanzbereich, im Banksektor und im Bereich e-Health sowie beispielsweise im Bildungsbereich, im Einzelhandel und in der Telekommunikationsbranche werden biometrische Daten ebenfalls immer häufiger genutzt. Diese Entwicklung wird durch die neuen Möglichkeiten infolge der Konvergenz bzw. der Zusammenführung bestehender Technologien verstärkt. Ein Beispiel ist etwa der Einsatz von Überwachungskameras zur Erfassung und zur Analyse biometrischer Daten und zur Verarbeitung menschlicher Verhaltenssignaturen.

Angesichts dieser Entwicklungen ist auch festzustellen, dass sich der Schwerpunkt bei der Entwicklung biometrischer Systeme von Identifikationsinstrumenten hin zu „weichen“ Erkennungssystemen verlagert (d. h. von der Identifikation hin zur Erkennung von Verhaltensmerkmalen oder von spezifischen Bedürfnissen der betreffenden Personen). Damit werden Nutzungen ermöglicht, die sich von sicherheitstechnischen Anwendungen in großem Maßstab erheblich unterscheiden. Anwendungen im Bereich der persönlichen Sicherheit sowie bei Spielen und im Einzelhandel werden in erheblichem Umfang von einer verbesserten Interaktion zwischen Menschen und Maschinen profitieren, die sich nicht auf die bloße Identifikation oder Kategorisierung von Personen beschränkt.

4.3. Auswirkungen auf die Privatsphäre und auf den Datenschutz

Von Anfang an wurden biometrische Systeme in verschiedenen Bereichen (unter anderem im Hinblick auf den Schutz der Privatsphäre und den Datenschutz) mit erheblichen Vorbehalten betrachtet. Dies hat sich mit Sicherheit auf die soziale Akzeptanz dieser Systeme und auf die Debatte über die Rechtmäßigkeit und die Grenzen einer Nutzung dieser Systeme sowie über die Sicherheitsvorkehrungen und die Garantien zur Abschwächung der bekannten Risiken ausgewirkt.

Ein wesentlicher Vorbehalt gegenüber biometrischen Systemen war schon immer der Schutz der individuellen Rechte. Daran hat sich nichts geändert. Allerdings bieten auch neue Systeme und Weiterentwicklungen bereits verfügbarer Systeme Anlass zu Bedenken. Die Bedenken richten sich unter anderem auf die Möglichkeit der verdeckten Erfassung, Speicherung und Verarbeitung von Daten sowie auf die Erfassung von Material mit äußerst sensiblen Informationen, da diese Nutzungen einen Eingriff in die intimsten persönlichen Bereiche darstellen können.

Von Anfang an wurde die Gefahr einer Zweckentfremdung biometrischer Technologien und Systeme („*Function Creep*“) als problematisch bewertet. Bei traditionellen biometrischen Systemen ist dieses Risiko hinlänglich bekannt, und in diesem Bereich werden auch entsprechende Sicherheitsvorkehrungen getroffen. Es steht jedoch außer Zweifel, dass das umfangreiche technische Potenzial neuer Computersysteme die Gefahr einer schleichenden Ausweitung der Nutzung von Systemen für nicht bestimmungsgemäße Zwecke erhöht.

Verdeckte Techniken ermöglichen die Identifikation von Personen ohne deren Wissen. Dies ist als schwerwiegende Bedrohung der Privatsphäre und als allmählicher Verlust der Kontrolle über personenbezogene Daten zu bewerten. Dies wiederum hat erhebliche Auswirkungen auf die Möglichkeit der betroffenen Personen, von ihrem Recht auf freiwillige Einwilligung Gebrauch zu machen oder auch nur Informationen über die Verarbeitung der Daten zu erhalten. Zudem können manche Systeme Informationen über den Gemütszustand oder über körperliche Merkmale heimlich erfassen und Gesundheitsinformationen offen legen. Dies wäre als unverhältnismäßige Verarbeitung von Daten sowie als Verarbeitung sensibler Daten gemäß Artikel 8 der Richtlinie 95/46/EG zu bewerten.

Angesichts der Tatsache, dass biometrische Technologien keine 100%ige Zuverlässigkeit gewährleisten können, besteht immer auch das Risiko einer fehlerhaften Identifikation. Entscheidungen aufgrund derartiger falsch positiver Befunde können die individuellen Rechte beeinträchtigen. Identitätsdiebstähle unter Verwendung gefälschter oder gestohlener biometrischer Daten können erhebliche Schäden nach sich ziehen. Anders als bei sonstigen Identifikationssystemen können den betreffenden Personen nach einer Fälschung der bereits erfassten Identitätsmerkmale nicht einfach neue Merkmale zugeordnet werden.

Ein wichtiger Aspekt ist auch die Erstellung von Profilen im Zusammenhang mit automatisierten Entscheidungen sowie bei der Vorhersage situationsbezogener Verhaltensweisen oder Vorlieben. Gewisse biometrische Daten können Aufschluss über physische Merkmale einer Person geben. Die betreffenden Informationen können genutzt werden, um die betreffenden Personen ausfindig zu machen oder entsprechende Profile zu erstellen; ebenso können diese Informationen aber auch zur Diskriminierung, Stigmatisierung oder unerwünschten Konfrontation mit nicht erwarteten oder nicht erwünschten Informationen führen.

4.4. Spezifische biometrische Systeme und Technologien

4.4.1. Die Erkennung von Venenstrukturen und kombinierte Verwendungen

Zwei wesentliche Technologien beruhen auf der Erkennung von Venenstrukturen: Sowohl Handflächen als auch Finger werden insbesondere in Japan inzwischen häufig anhand der Venenstrukturen identifiziert.

Technisch gesehen beruht die Erkennung von Venenstrukturen auf einem Template der mit einer Infrarotkamera erfassten Venen. Die Erfassung erfolgt, wenn eine Person einen Finger oder eine Hand vor eine Infrarot-Lichtquelle bringt. Das aufgenommene Bild wird so verarbeitet, dass das jeweilige Gefäßnetz sichtbar wird. Der wesentliche Vorteil dieser Technologie liegt darin, dass die betroffene Person bei der Erfassung der biometrischen Merkmale keine physische Probe hinterlassen muss.[13] (Die Identifikation erfolgt berührungslos.) In diesem Zusammenhang ist auch zu beachten, dass biometrische Daten gegenwärtig nur schwer ohne die Einwilligung der betroffenen Personen erfasst werden können. Da der Blutfluss analysiert werden kann, ist mit diesem Verfahren schließlich auch festzustellen, ob die von einem System untersuchte Person lebt.

[13] Einige Autoren sind der Ansicht, dass Technologien im Zusammenhang mit der Erkennung von Venenstrukturen Rückschlüsse auf Erkrankungen wie z. B. Bluthochdruck oder Gefäßanomalien zulassen könnten.

Die Erkennung von Venenstrukturen kann auch genutzt werden, um den virtuellen Zugang zu Anwendungen oder den physischen Zugang zu Räumlichkeiten zu regeln. Häufig sehen die Hersteller die Möglichkeit vor, die betreffenden Sensoren auch in andere Produkte einzubauen (insbesondere im Zusammenhang mit Bankgeschäften).

Im Zusammenhang mit der Nutzung von Systemen zur Erkennung von Venenstrukturen können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Die Leistungsfähigkeit von Venenstruktur-Analysen ist hoch. Daher gilt diese Technologie als realistische Alternative zur Analyse von Fingerabdrücken. Außerdem zeichnet sich die Erkennung von Venenstrukturen durch eine niedrige FER (*Failure to Enrol Rate* = Erfassungsfehlerquote) aus, da sich die Venen im Gegensatz zu Fingern oder Händen nicht verändern. Trotzdem wurden diese Technologien bislang noch nicht an einem größeren Bevölkerungsregister erprobt. (In Japan wird die ermittelte Struktur mit dem jeweils auf einem Magnetstreifen gespeicherten Template verglichen.) Manchmal kann diese Technologie auch durch klimatische Bedingungen beeinträchtigt werden, die sich auf das Gefäßsystem auswirken (Wärme, Druck usw.).

- Auswirkung: Systeme zur Untersuchung der Venenstrukturen haben hinsichtlich des Datenschutzes nur begrenzte Relevanz, da die betreffenden biometrischen Daten nicht einfach abgegriffen werden können, und da sich die Analyse von Venenstrukturen gegenwärtig auf Anwendungen im privaten Bereich beschränkt.

- Einwilligung und Transparenz: Da Daten zu Venenstrukturen ausschließlich unter Einsatz von Lichtquellen und Kameras in der Nähe des Infrarotspektrums erfasst werden können, ist davon auszugehen, dass der jeweils betroffenen Person die Verarbeitung der Daten bewusst ist und dass die betroffene Person ihre Einwilligung zum Ausdruck gebracht hat, indem sie ihren Finger oder ihre Hand auf das Lesegerät gelegt hat. Wie bei allen biometrischen Systemen ist jedoch auch bei diesen Systemen diese Annahme unter gewissen Umständen mit Vorbehalten zu bewerten (beispielsweise wenn die betroffene Person bei dem für die Verarbeitung Verantwortlichen beschäftigt ist).

- Sonstige Zwecke bzw. Verarbeitungszwecke: Gegenwärtig sind mit Strukturdaten nur geringe Risiken hinsichtlich einer Nutzung für anderweitige Zwecke verbunden. Dieses Risiko kann sich jedoch erhöhen, wenn diese Form der Verarbeitung weitere Verbreitung findet und Betrugsversuche durch Spoofing (Täuschung) erleichtert werden.

- Verknüpfbarkeit: Venenstrukturdaten enthalten keine Informationen, die mit anderen Daten verknüpft werden könnten (außer mit Venenstrukturdaten aus anderen Verarbeitungsprozessen).

- Nachverfolgung/Erstellung von Profilen: Das Risiko einer Nachverfolgung/Profilerstellung aufgrund von Venenstrukturdaten ist begrenzt, solange dieser Typ biometrischer Daten nicht allgemein verbreitet ist und beispielsweise in einer zentralen Zahlungskarten-Datenbank gespeichert wird.

- Verarbeitung sensibler Daten: Die einzigen sensiblen Daten, die aus Venenstrukturdaten abzuleiten wären, betreffen die Gesundheit der jeweiligen Personen. Eine entsprechende formale Bewertung ist bislang jedoch noch nicht erfolgt.

- Widerruflichkeit: Venenstrukturen dürften auch über längere Zeiträume sehr stabil sein. Diese Annahme ist jedoch noch empirisch zu belegen. (Systeme zur Analyse von Venenstrukturen werden noch nicht so lange eingesetzt, dass bestätigte Ergebnisse verfügbar wären.) Daher sind Venenstrukturen wohl als unwiderruflich zu behandeln.

- Schutz gegen Spoofing: Umfangreiche Untersuchungen zu Spoofing-Angriffen im Zusammenhang mit Venenstrukturdaten wurden bislang noch nicht durchgeführt. In letzter Zeit wurde jedoch in einer Studie festgestellt, dass mit Geräten zur Erkennung von Handflächen-Venenstrukturen Spoofing-Angriffe möglich sind.[14] Die wesentliche Schwierigkeit beim Spoofing in Verbindung mit Venenstrukturdaten besteht darin, die benötigten biometrischen Daten überhaupt zu erfassen.

4.4.2. Fingerabdrücke und kombinierte Nutzungen

Systeme zur Erkennung von Fingerabdrücken zählen zu den ältesten und am häufigsten untersuchten und eingesetzten biometrischen Systemen. Die Nutzung von Fingerabdrücken ist in der Rechtsdurchsetzung seit über 100 Jahren sowohl für Überprüfungen als auch für Identifikationszwecke üblich. Die Identifikation aufgrund von Fingerabdrücken beruht auf der Tatsache, dass jeder Mensch Fingerabdrücke mit individuellen messbaren Merkmalen hinterlässt, die mit bereits erfassten Abdrücken verglichen werden können.

Die Erfassung setzt voraus, dass die betreffende Person physisch anwesend ist und dass – je nach beabsichtigtem Verwendungszweck – gut geschulte Mitarbeiter verfügbar sind, um eine hinreichend gute Qualität der Daten gewährleisten zu können. Die Bedeutung der Abnahme der Fingerabdrücke ist nicht zu unterschätzen. Die Zuverlässigkeit eines Abgleichs hängt von der Bildqualität und vom jeweiligen Abbildungsverfahren ab. Je nach Verfahren werden Abdrücke nur von einem oder zwei Fingern oder aber auch von allen zehn Fingern genommen. Die Abdrücke können flach aufgesetzt oder abgerollt werden. Je nach System können Fingerabdrücke zur bloßen Überprüfung (1:1) oder zur Identifikation und zum Abgleich mit gesicherten Spuren (1:n) verwendet werden. Einigen Studien zufolge können von einem Teil der Bevölkerung jedoch aus unterschiedlichen Gründen keine Abdrücke genommen werden. Dies ist insoweit problematisch, als insbesondere bei umfangreichen Systemen geeignete Alternativverfahren verfügbar sein müssen, damit niemandem seine individuellen Rechte vorenthalten werden.

Auch wenn die Erfassung von Fingerabdrücken nicht als Verfahren zu betrachten ist, das die Privatsphäre erheblich beeinträchtigen würde, kann dies doch so empfunden werden. Infolge der verbreiteten Nutzung bei der Rechtsdurchsetzung wird die Abnahme von Fingerabdrücken häufig mit dem negativen Image einer Behandlung als Tatverdächtiger assoziiert.

Fingerabdrücke sind durch individuelle Merkmale gekennzeichnet, die zur Verifikation/Identifikation genutzt werden können. Im Allgemeinen sind jedoch weiterhin

[14] Siehe http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf.

gründliche detaillierte Analysen erforderlich. Die Entwicklung neuer Verfahren (d. h. der Einsatz hoch auflösender Scanner) wird die Nutzung anderer Merkmale ermöglichen. Auch die Techniken zur Identifikation anhand umfangreicher Datenbanken wurden weiterentwickelt.

Die modernsten Systeme sind sogenannte AFIS (*Automated Fingerprint Identification Systems* = automatisierte daktyloskopische Identifizierungssysteme). Diese Systeme werden bei der Rechtsdurchsetzung eingesetzt. Sie ermöglichen den Austausch von Daten und die Durchsuchung unterschiedlicher länderübergreifender Bestände. Der Austausch von Daten ist allerdings je nach Standort, Formaten und Qualität mit unterschiedlichen Problemen verbunden.

AFIS auf EU-Ebene beispielsweise sind Eurodac und das Visa-Informationssystem. Mit einem Bestand von ca. 70 Mio. Fingerabdrücken dürften diese Systeme zu den weltweit größten Datenbanken zählen. Im Zusammenhang mit der Nutzung umfangreicher Datenbanken hat die Datenschutzgruppe bereits in früheren Stellungnahmen auf Probleme hinsichtlich der Gewährleistung der erforderlichen Verhältnismäßigkeit hingewiesen. Zu klären sind insbesondere die Zuverlässigkeit der Ergebnisse (falsch positive und falsch negative Ergebnisse) sowie die wirksame Kontrolle des Zugangs zu diesen Datenbanken und die Verwendung der Fingerabdrücke von Kindern und alten Menschen.

In biometrischen Systemen, die auf erfassten Fingerabdrücken beruhen, werden häufig Templates eingesetzt. Die Anbieter betrachten diese Systeme gewöhnlich als Instrumente zum Schutz der betreffenden Personen. Je nach System bzw. je nach dem zur Erzeugung der Templates eingesetzten Algorithmus kann die Gefahr einer Verknüpfung der Templates mit anderen Fingerabdruck-Datenbanken bestehen, die die Identifikation einzelner Personen ermöglichen würde.

Problematisch ist auch, dass mit Systemen zur Erzeugung von Fingerabdrücken unter Verwendung künstlicher Finger oder künstlicher Fingerabdrücke Identitätsdiebstähle begangen werden könnten. Mit verschiedenen Ansätzen wird versucht, der entsprechenden Gefährdung dieser Systeme zu begegnen (etwa durch Erkennung in Echtzeit oder durch den Einsatz von Systemen, bei denen jeweils mehrere Finger berücksichtigt werden, durch die Beaufsichtigung der Erfassung und der Identifikation und durch die Verifikation durch geeignete Personen).

Die datenschutzrechtlichen Bedenken hinsichtlich der Verwendung von Fingerabdrücken lassen sich wie folgt zusammenfassen:

- Zuverlässigkeit: Ungeachtet ihrer letztlich hohen Zuverlässigkeit sind Fingerabdruck-Analysen wegen der verwendeten Informationen (schlechte Qualität des Datenmaterials oder inkonsistente Erfassungsverfahren) sowie wegen der Darstellung der Fingerabdrücke (ausgewählte Merkmale oder Qualität der Analysealgorithmen) angreifbar. Infolge der genannten Faktoren kann es zu falsch positiven oder falsch negativen Ergebnissen kommen.

- Auswirkung: Die Unumkehrbarkeit des Prozesses kann die Möglichkeit beeinträchtigen, dass die betroffenen Personen ihre Rechte wahrnehmen oder dass Entscheidungen rückgängig gemacht werden, die aufgrund falscher Identifikationen getroffen wurden. Das Vertrauen auf die Zuverlässigkeit von Fingerabdruck-Analysen kann die Korrektur von Fehlern erschweren und weitreichende Folgen für die betroffenen Personen nach sich ziehen. Dies muss bei der Bewertung der

Verhältnismäßigkeit einer Verarbeitung gemessen an der jeweils aufgrund der bewerteten Fingerabdrücke zu treffenden konkreten Entscheidung berücksichtigt werden. Außerdem ist darauf hinzuweisen, dass mangelnde Sicherheitsvorkehrungen Identitätsdiebstähle begünstigen können, die mit nachdrücklichen Auswirkungen auf die betroffenen Personen verbunden sein können.

- Verknüpfbarkeit: Fingerabdrücke können insoweit missbraucht werden, als die entsprechenden Informationen mit anderen Datenbanken verknüpft werden können. Diese Möglichkeit der Verknüpfung mit anderen Datenbanken kann Verwendungen zur Folge haben, die mit dem ursprünglichen Zweck nicht in Einklang stehen. Mit gewissen Techniken (z. B. mit Systemen zur Konvertierung biometrischer Daten oder durch biometrische Verschlüsselung) kann dieses Risiko verringert werden.

- Verarbeitung sensibler Daten: Einigen Studien zufolge können abgenommene Fingerabdrücke Aufschluss über die ethnische Herkunft der betroffenen Personen geben.[15]

- Weitere Zwecke bzw. Verarbeitungszwecke: Die zentrale Speicherung von Daten – insbesondere in großen Datenbanken – verringert Risiken im Hinblick auf die Sicherheit und die Verknüpfbarkeit der Daten sowie hinsichtlich der Gefahr eines Function Creep. Das Fehlen geeigneter Garantien kann dazu führen, dass Fingerabdrücke zu anderen Zwecken genutzt werden als ursprünglich vorgesehen.

- Einwilligung und Transparenz: Die Einwilligung ist ein zentraler Aspekt bei der Verwendung von Fingerabdrücken außerhalb des Bereichs der Rechtsdurchsetzung. Fingerabdrücke können von latenten Abdrücken und sogar von Fotografien leicht auch ohne Wissen der betroffenen Personen kopiert werden. Ebenfalls problematisch im Zusammenhang mit dem Aspekt der Einwilligung sind die Einwilligung eines Kindes und die Rolle der Eltern (z. B. bei der Abnahme von Fingerabdrücken in Schulen) sowie die Gültigkeit einer Einwilligung zur Abgabe von Fingerabdrücken im Zusammenhang mit Beschäftigungsverhältnissen.

- Widerruflichkeit: Fingerabdrücke ändern sich nicht und sind insoweit als äußerst stabile Daten zu bewerten. Entsprechend sollten diese Daten als unwiderruflich betrachtet werden. Unter gewissen Bedingungen ist allerdings vorstellbar, dass auch Fingerabdruck-Templates widerrufen werden.

- Schutz gegen Spoofing: Fingerabdrücke können leicht erfasst werden, weil Menschen zahllose Abdrücke hinterlassen. Außerdem können bei vielen Systemen und Sensoren falsche Fingerabdrücke verwendet werden, insbesondere wenn diese Systeme keine spezifischen Mechanismen zum Schutz gegen Spoofing enthalten. Der Erfolg eines Angriffs hängt weitgehend vom jeweiligen Sensortyp (optisch, kapazitiv usw.) und vom Material ab, das der Angreifer verwendet.

[15] http://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm und http://www.crime-scene-investigator.net/fingerprintpatterns.html.

Beispiel:
Ein Krankenhaus verwendet Fingerabdrücke in einer zentralen Datenbank zur Authentifikation von Patienten, um bei Strahlenbehandlungen sicherzustellen, dass der betreffende Patient die richtige Behandlung erhält. Fingerabdrücke werden gegenüber Venenstrukturen bevorzugt, weil Strahlenbehandlungen das Gefäßsystem beeinträchtigen. Außerdem wird eine zentrale Datenbank verwendet, weil angesichts des Gesundheitszustands der Patienten (Alter und Pathologie) mit hoher Wahrscheinlichkeit damit zu rechnen wäre, dass Namensschilder verloren gingen und der Zugang zur betreffenden Behandlung verhindert würde. Vor diesem Hintergrund könnte die Verwendung von Fingerabdrücken eine angemessene Lösung sein.

4.4.3. Gesichtserkennung und kombinierte Verwendungen

Ähnlich wie Fingerabdrücke werden auch biometrische Daten aufgrund von Gesichtserkennungen seit Jahren in erheblichem Umfang genutzt. Neuerdings werden Gesichter jedoch nicht nur zur Identifikation, sondern auch zur Feststellung physiologischer und psychologischer Merkmale (ethnische Herkunft, Gefühle, Wohlbefinden usw.) analysiert. Aus der Tatsache, dass die betreffenden Daten auch aus einem Bild ermittelt werden können und dass Fotos auch aus größerer Entfernung ohne Wissen der betroffenen Personen aufgenommen werden können, wird deutlich, welche datenschutzrechtlichen Probleme mit diesen Technologien verbunden sein können.

Die Bedeutung der Gesichtserkennung als Mittel zur Identifikation von Personen und zur Verifikation von Sachverhalten wurde auch im Bereich der Rechtsdurchsetzung sowie von anderen öffentlichen Stellen und von privaten Einrichtungen erkannt. Seit vielen Jahren werden Fotos in Reisepässen, Führerscheinen, Ausweisen und Fahndungsfotos verwendet. Vielfach werden Fotos auf Ansteckschilder oder auf sonstige unternehmensinterne Ausweise gedruckt. Die betreffenden Bilder werden gewöhnlich unter kontrollierten Lichtverhältnissen aufgenommen und beschränken sich auf eine Profilansicht der jeweiligen Person. Ein Satz derart kontrollierter Bilder bietet sich als Grundlage für die automatisierte Verarbeitung und die Erkennung von Personen an. Die entsprechenden Möglichkeiten wurden inzwischen weiterentwickelt, und die verfügbare Technologie ist inzwischen derart ausgereift, dass eine Identifikation anhand von Bildern möglich ist, die mit den unterschiedlichsten Kameras, aus ganz verschiedenen Blickwinkeln und unter unterschiedlichen Beleuchtungsbedingungen aufgenommen wurden. Zahlreiche Bilder sind im Internet öffentlich zugänglich (z. B. Fotos, die in soziale Netze oder in sonstige öffentliche Alben hochgeladen wurden). Die betreffenden Risiken beschränken sich nicht auf traditionelle Bilder, da Funktionen zur Gesichtserkennung inzwischen erfolgreich auch in Echtzeit-Video-Feeds genutzt werden können. Wenn für die Verarbeitung Verantwortliche in vorhandene Systeme neue Verarbeitungsfunktionen aufnehmen (z. B. durch die Einbindung einer Funktion zur Gesichtserkennung in ein System zur Videoüberwachung), muss ihnen bewusst sein, dass sie damit eine Änderung der vorgesehenen Zwecke des ursprünglichen Systems bewirken. Entsprechend müssen sie die Auswirkungen dieser Änderung auf den Schutz der Privatsphäre neu bewerten.

Systeme zur Gesichtserkennung gehen mit folgenden Risiken in Bezug auf den Datenschutz einher:

- Zuverlässigkeit: Wenn die Qualität der Bilder nicht garantiert werden kann, besteht die Gefahr einer Beeinträchtigung der Zuverlässigkeit. Wird ein Gesicht nicht vollständig erfasst (weil es durch Haare oder einen Hut verdeckt ist), können ein Abgleich und

eine Kategorisierung natürlich nur mit einer hohen Fehlerquote erfolgen. Unterschiedliche Haltungen und Lichtverhältnisse sind weitere große Herausforderungen für eine zuverlässige Gesichtserkennung.

- Auswirkung: Die spezifischen Auswirkungen auf den Datenschutz eines Systems zur Gesichtserkennung hängen vom jeweiligen Zweck und von den betreffenden Umständen ab. Ein System, das die Besucher einer Sehenswürdigkeit nach demografischen Gesichtspunkten kategorisiert, aber nicht über eine Speicherfunktion verfügt, wirkt sich hinsichtlich des Datenschutzes anders aus als ein System, das im Bereich der Rechtsdurchsetzung zur verstärkten Überwachung potenzieller Unruhestifter einsetzt wird.

- Einwilligung und Transparenz: Ein Risiko für den Datenschutz, das bei vielen anderen Systemen zur Verarbeitung biometrischer Daten nicht gegeben ist, besteht darin, dass Fotos aus zahlreichen Blickwinkeln und unter den unterschiedlichsten Bedingungen ohne Wissen der betroffenen Personen aufgenommen und verarbeitet werden können. In Stellungnahme 15/2011 zum Begriff der Einwilligung betont die Datenschutzgruppe, dass nur eine „informierte“ Einwilligung Rechtsgrundlage für die Verarbeitung von Daten sein kann. Wenn die betroffene Person keine Kenntnis von der Verarbeitung von Fotos zum Zweck der Gesichtserkennung hat, ist diese Rechtsgrundlage nicht gegeben. Und selbst wenn die betroffene Person weiß, dass eine Kamera eingesetzt wird, ist vielleicht nicht erkennbar, ob die Gesichtserkennung mit einer laufenden Überwachungskamera oder anhand statischer Fotos erfolgt.

- Sonstige Zwecke bzw. Verarbeitungszwecke: Einmal erfasst, können digitale Bilder leicht weitergegeben oder kopiert und dann in anderen Systemen umfassender bearbeitet werden als ursprünglich vorgesehen. Dabei ist unerheblich, ob die Bilder rechtmäßig oder widerrechtlich aufgenommen wurden. Dies wird z. B. im Bereich der sozialen Medien deutlich, wo Nutzer ihre persönlichen Fotos hochladen, um die Fotos ihrer Familie, ihren Freunden und ihren Kollegen zu zeigen. Sobald in einem sozialen Medium Bilder verfügbar sind, können sie durch die betreffende Plattform zu vielfältigen Zwecken verwendet werden. Manche dieser Verwendungszwecke werden unter Umständen erst nachträglich eingeführt (d. h. nach dem Aufnehmen und/oder dem Hochladen der betreffenden Bilder).

- Verknüpfbarkeit: Viele Online-Dienste bieten Nutzern die Möglichkeit, Bilder hochzuladen, die sie mit dem jeweiligen Nutzerprofil verknüpfen können. Systeme zur Gesichtserkennung können eingesetzt werden, um die Profile unterschiedlicher Online-Dienste (über das jeweilige Profilbild) miteinander zu verknüpfen. Ebenso können jedoch auch Verknüpfungen zwischen Online-Medien und Offline-Datenbeständen hergestellt werden. Es ist durchaus möglich, eine Person in Echtzeit anhand eines Fotos zu identifizieren, indem diese öffentlichen Profilbilder durchsucht werden. Auch Fremddienste können Profilbilder und sonstige öffentlich zugängliche Bilder durchsuchen, um riesige Bilddatenbanken zu erstellen. Die Bilder in diesen Datenbanken können dann Identitäten in der realen Welt zugeordnet werden.

- Nachverfolgung/Erstellung von Profilen: Außerdem könnte ein Identifikationssystem genutzt werden, um die Identität einer abgebildeten Person in der realen Welt zu ermitteln. Ein System zur Gesichtserkennung in einem Einkaufszentrum oder einem ähnlichen öffentlichen Bereich könnte eingesetzt werden, um Wege und

Gewohnheiten einzelner Kunden zu verfolgen. Aufgrund der ermittelten Informationen könnten Warteschlangen gesteuert oder Produkte präsentiert werden, um das Einkaufserlebnis attraktiver zu gestalten. Mit der Möglichkeit der Verfolgung oder Lokalisierung einzelner Personen geht die Möglichkeit einher, Profile zu erstellen und gezielte Werbung anzubringen oder sonstige spezifische Dienste anzubieten.

- Verarbeitung sensibler Daten: Wie bereits erläutert, könnten durch die Verarbeitung biometrischer Daten sensible Daten ermittelt werden. Insbesondere könnten Bilder erfasst werden, die Aufschluss über die rassische oder ethnische Herkunft oder vielleicht auch den Gesundheitszustand geben könnten.

- Widerruflichkeit: Eine Person kann ihr Gesicht leicht verändern (beispielsweise durch einen Bart, eine Brille oder einen Hut). Diese Veränderungen können hinreichend sein, um Systeme zur Gesichtserkennung zu täuschen, insbesondere wenn diese Systeme in einer nicht kontrollierten Umgebung eingesetzt werden. Die wesentlichen Merkmale eines Gesichts sind jedoch unveränderlich, und die Systeme können die Erkennungsgenauigkeit verbessern, indem sie mehrere unterschiedliche „Gesichter“ einer Person erfassen und miteinander verknüpfen.

- Schutz gegen Spoofing: Viele Systeme zur Gesichtserkennung können leicht Gegenstand von Spoofing-Angriffen werden. Die Hersteller bemühen sich um entsprechende Schutzmechanismen beispielsweise unter Nutzung von 3D-Bildern oder von Videoaufnahmen. Die meisten in öffentlichen Anwendungen eingesetzten Systeme sind jedoch nicht mit derartigen Schutzmechanismen ausgerüstet.

Beispiel:
Als extremes Beispiel wäre etwa ein Einkaufszentrum der Zukunft vorstellbar, in dem eine Videoüberwachung Personen erkennt, Bewegungen automatisch verfolgt und anhand der erfassten Gesichter emotionelle Reaktionen wie z. B. ein Lächeln oder Anzeichen von Verärgerung feststellen kann. Das System könnte regelmäßige Kunden erkennen, die ins Parkhaus einfahren und diese Kunden zu bevorzugten Parkplätzen lotsen. Wenn die Kunden das Einkaufszentrum betreten, könnte das System aufgrund der erkannten Kleidung je nach Angebot, früherem Einkaufsverhalten und zuvor definierten Indikatoren unterschiedliche Ladengeschäfte vorschlagen. Ebenso könnte in den Schaufenstern kundenspezifische Werbung platziert oder der Zugang zu bestimmten Läden, Restaurants und sonstigen Orten verweigert werden. Potenzielle Autodiebe könnten identifiziert und verfolgt werden, noch bevor sie sich an einem Auto zu schaffen machen. Wenn nötig, könnten telematisch geführte Luftfahrzeuge (Drohnen) mit Kameras und Sensoren Verdächtige verfolgen, bis der betreffende Verdacht entweder bestätigt oder als unbegründet bewertet wurde. In Kleidungsstücken verborgene Objekte (Messer oder Diebesgut) könnten erkannt werden. Diese Technologie würde nicht nur auf neuen biometrischen Systemen beruhen, sondern würde Informationen kombinieren und verarbeiten, die bereits in den Datenbeständen weiterer Systeme erfasst sind.

Eine ähnliche Anwendung wurde mit dem Projekt INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*) entwickelt, in dem Technologien kombiniert werden, mit denen potenzielle terroristische und kriminelle Handlungen bereits im Vorfeld bekämpft werden sollen. Die Datenschutzgruppe weist nachdrücklich darauf hin, dass eine derartige Nutzung biometrischer Daten eine angemessene Rechtsgrundlage und strenge Prüfungen der Notwendigkeit und der Verhältnismäßigkeit der entsprechenden Maßnahmen voraussetzen würde.

4.4.4. Sprecherverifikation und kombinierte Verwendungen

Systeme zur Stimmerkennung („Sprecherverifikation“) werden nicht nur zur biometrischen Identifikation genutzt. Verhältnismäßig häufig werden auch spezifische Merkmale von Stimmstrukturen identifiziert, um die Sprecher entsprechend zu kategorisieren. Eine entsprechende Anwendung wäre beispielsweise die Analyse der Reaktionen einer Person während eines Telefonats, um Stressmuster und Unregelmäßigkeiten im Sprechverhalten zu erkennen und aus den erkannten Informationen auf betrügerisches Verhalten schließen zu können.

Hersteller berichten, dass durch die Einrichtung einer derartigen Technologie bei Finanzdienstleistern Betrugsfälle zuverlässiger erkannt und berechtigte Forderungen rascher erfüllt werden konnten.

In Verbindung mit einem Kategorisierungssystem stellen sich die Risiken im Hinblick auf den Datenschutz etwas anders dar als bei biometrischen Identifikationssystemen. Bei diesen Systemen dürfte eine Erfassung und langfristige Speicherung biometrischer Templates nicht erforderlich sein. Wenn jedoch ein Telefonat aufgezeichnet wird (was etwa bei Finanzinstituten häufig der Fall ist), müssen geeignete Kontrollen eingerichtet sein, um die Sicherheit dieser Daten zu gewährleisten.

- Zuverlässigkeit: Datenschutzrechtlich problematisch sind bei derartigen Systemen die Erkennungsquoten, insbesondere im Hinblick auf falsch positive und falsch negative Ergebnisse, d. h. hinsichtlich des Anteils der Personen, die fälschlicherweise als Betrüger identifiziert bzw. die nicht als Betrüger erkannt werden. Bei einem Kategorisierungssystem sind höhere Fehlerquoten vielleicht eher annehmbar als bei Verifikations- oder Identifikationssystemen. Es müssen jedoch geeignete Prozesse zur zeitnahen Handhabung der Fälle eingerichtet sein, in denen möglicherweise eine unzutreffende Kategorisierung vorgenommen wurde.

- Einwilligung und Transparenz: Bei derartigen Technologien kommen jedoch auch für den Datenschutz vorteilhafte Ansätze in Betracht, etwa indem darauf geachtet wird, dass Anrufe auf ihre Eignung für eine entsprechende Analyse geprüft werden oder indem die betroffenen Personen über den durchgeführten Prozess unterrichtet werden. In einer Fallstudie wurden einzelne Personen, die Englisch nicht als Hauptsprache verwendeten oder deren Hörvermögen oder kognitive Fähigkeiten beeinträchtigt waren oder die keinen Zugang zu einem Telefon hatten, als für das betreffende System zur Sprecherverifikation ungeeignet bewertet. Den betreffenden Personen war freigestellt, eine telefonische Mitteilung abzulehnen und ihr Anliegen in herkömmlicher Weise vorzubringen. Den Personen, die nicht bereit oder nicht in der Lage waren, sich der Erkennung durch ein entsprechendes System zu unterziehen, sollten jedoch keine Nachteile entstehen.

- Weitere Zwecke bzw. Verarbeitungszwecke: Bei dieser Technologie werden in den meisten Fällen spezielle Infrastrukturänderungen benötigt, da der öffentliche und der private Sektor ihre jeweiligen IT-Infrastrukturen so konsolidieren müssen, dass Technologien wie z. B. Voice over IP (VoIP) genutzt werden können. Gleichzeitig werden Spracherkennungstechnologien leichter einzubinden sein, ohne dass datenschutzrechtliche Verpflichtungen des für die Verarbeitung Verantwortlichen angemessen berücksichtigt würden.

- Widerruflichkeit: Auch wenn jemand seine Stimme bewusst verstellen kann, sind die zugrunde liegenden Sprechmuster doch verhältnismäßig stabil und können entsprechend hilfreich sein, um eine Person zuverlässig zu identifizieren. Dies gilt insbesondere, wenn die betreffende Person nicht über die Erkennung unterrichtet wurde (und sich daher auch nicht veranlasst sieht, ihre Stimme zu verstellen).

- Schutz gegen Spoofing: Sprachaufzeichnungen können genutzt werden, um Stimmerkennungssysteme durch Spoofing anzugreifen. Verfahren zum Schutz gegen Spoofing beinhalten Fragen und Antworten zum jeweiligen Hintergrund. (Beispielsweise wird etwa nach dem aktuellen Datum gefragt oder aufgefordert, seltene Wörter nachzusprechen.)

4.4.5. DNA-Analysen

Die Weiterentwicklung von Geräten zur Sequenzierung und zum Abgleich von DNA-Proben sowie die Verfügbarkeit kostengünstiger Geräte zur Durchführung von DNA-Analysen machen die Überprüfung gewisser Annahmen des bereits vorliegenden Arbeitspapiers über Biometrie (WP 80) erforderlich.

Eine der wesentlichen Änderungen bei Technologien zur Erstellung von DNA-Profilen ist die Beschleunigung der Prozesse zur Sequenzierung und zum Abgleich von DNA-Proben. Die in den letzten Jahren aufgrund von Forschungen im akademischen Bereich sowie infolge der Entwicklungstätigkeit von Biotechnologieunternehmen erzielten Fortschritte haben dazu geführt, dass sich der Zeitaufwand für die Erzeugung eines DNA-Profils von ursprünglich einigen Tagen auf wenige Stunden und schließlich auf weniger als eine Stunde reduziert hat.

Die Entstehung eines Marktes für DNA-bezogene Online-Dienste gefährdet das Recht auf den Schutz personenbezogener Daten. Dies gilt insbesondere dann, wenn die betreffenden Dienste die Übertragung biometrischer Proben und Daten zwischen mehreren Ländern (einschließlich Ländern außerhalb der EU) erfordern, sowie wenn mehrere Auftragsverarbeiter beteiligt sind und bei der Verarbeitung genetischer Daten oder gesundheitsbezogener Daten geeignete Garantien fehlen.

Sehr wahrscheinlich wird es in der näheren Zukunft möglich sein, Profile aufgrund von DNA-Proben in Echtzeit (oder nahezu in Echtzeit) auch mit tragbaren Geräten zu erstellen. Damit wird die Entwicklung biometrischer Identifikations- und Authentifikationssysteme auf der Grundlage von DNA-Proben beginnen, die sich gegenüber Systemen zur Authentifikation aufgrund von Fingerabdrücken, Stimmen und Gesichtern durch eine größere Zuverlässigkeit auszeichnen.

Weiterentwicklungen bei der Erstellung von DNA-Profilen sind auf das zunehmende Interesse von Verwaltungseinrichtungen, Richtern und Rechtsdurchsetzungsbehörden am Einsatz biotechnologischer Verfahren in der Kriminalistik zurückzuführen. Wegen der Zuverlässigkeit des Abgleichs von DNA-Proben sowie aufgrund der Tatsache, dass DNA-Proben ohne Wissen der betroffenen Person kontrolliert werden können, haben mehrere

Mitgliedstaaten im Laufe der Zeit verschiedene Initiativen ins Leben gerufen, um aufgrund von an Tatorten gesicherten Spuren zentrale Datenbanken mit DNA-Proben und mit DNA-Profilen verurteilter Personen aufzubauen.

Im Mai 2005 haben sieben EU-Mitgliedstaaten den Prümer Vertrag unterzeichnet, um die Zusammenarbeit bei grenzübergreifenden strafrechtlichen Untersuchungen und Gerichtsverfahren durch den Austausch geeigneter Informationen zu verbessern. Der Vertrag schafft insoweit eine neue Grundlage für die Zusammenarbeit, als er den Unterzeichnern bestimmte Rechte für den Zugang zu nationalen DNA-Datenbanken einräumt. Das betreffende Datenmaterial beschränkt sich allerdings auf die Verwendung für repressive Maßnahmen (Verfolgung von Straftaten) sowie auf die Nutzung von Fingerabdrücken, personenbezogenen und nicht personenbezogenen Daten und auf Fahrzeugregistrierungsdaten. Seit damals haben viele Mitgliedstaaten den Vertrag unterzeichnet, und die wesentlichen Inhalte des Vertrags wurden in den Beschluss 2008/615/JI des Rates übernommen.

Nach Maßgabe dieses Rechtsrahmens werden mehrere EU-Mitgliedstaaten in näherer Zukunft über eine funktionsfähige nationale Datenbank mit DNA-Profilen verurteilter Personen sowie mit DNA-Daten aufgrund von Spurensicherungen an Tatorten verfügen. Dies gibt Anlass zu gewissen Bedenken hinsichtlich dieser besonderen Form der Datenverarbeitung.

Einer der wesentlichen Aspekte im Zusammenhang mit der Einrichtung von DNA-Datenbanken ist die Tatsache, dass die aus DNA-Proben (Loci) abgeleiteten genetischen Daten Aufschluss über den Gesundheitszustand der betroffenen Personen sowie über Dispositionen für Krankheiten oder die ethnische Herkunft geben könnten (zwar nicht bereits während der Erfassung, jedenfalls aber zu einem späteren Zeitpunkt). Insoweit ist die Erstellung von DNA-Datenbanken als erhebliches Risiko für die Achtung der Menschenwürde und für die Wahrung der Grundrechte zu bewerten. Dieses Risiko wurde in der Entschließung 2009/C 296/01 des Rates berücksichtigt. Mit konkreten Vorschriften sollen DNA-Analysen auf Chromosomenbereiche ohne genetische Aussagekraft beschränkt werden. Dazu wird eine spezielle Gruppe von DNA-Markern verwendet, die nach aktuellem Kenntnisstand keine Informationen über spezifische Erbmerkmale enthalten. (Diese Gruppe von Markern wird auch als „ESS“ (*European Standard Set* = Europäischer Standardsatz) bezeichnet.

Da bestimmte Marker in einer nationalen DNA-Datenbank jedoch zu einem späteren Zeitpunkt Aufschluss über gewisse Erbmerkmale oder über sonstige sensible Informationen geben könnten, müssen Entwicklungen in der Biologie mit kontinuierlicher Aufmerksamkeit verfolgt werden. Gegebenenfalls müssten gewisse in der betreffenden Datenbank enthaltene Informationen sogar umgehend gelöscht werden. Und da diese DNA-Datenbanken Profile verurteilter Personen erfassen, sollten statistische Analysen der vorhandenen Daten streng eingeschränkt werden, um die Erstellung von Profilen aufgrund des Geschlechts oder der rassischen Herkunft zu verhindern.

In Bezug auf DNA-Datenbanken für polizeiliche oder strafrechtliche Zwecke hat der Europäische Gerichtshof für Menschenrechte festgestellt, dass zwischen der Verarbeitung personenbezogener Daten und der Verarbeitung genetischer Profile von Tatverdächtigen und von verurteilten Personen klar zu unterscheiden ist.[16]

[16] EGMR, Urteil vom 4.12.2008, S. und Marper/Vereinigtes Königreich (Anträge Nrn. 30562/04 und 30566/04), insbesondere Randnummer 125.

Außerdem besteht die Gefahr, dass DNA-Analysen zur Identifikation von Familienmitgliedern oder Verwandten im Zusammenhang mit nicht aufgeklärten Straftaten oder mit verurteilten Personen herangezogen werden könnten, weil die in der Datenbank gespeicherten DNA-Profile aufgrund von Teilgruppen der erfassten Marker oder mithilfe von Platzhaltern durchsucht werden könnten. Angesichts dieser Möglichkeit sind die Auswirkungen der Ableitung von Informationen aus familienbezogenen Suchabfragen zu prüfen.

Außerdem ist darauf hinzuweisen, dass mit der Nutzung von Genom-Datensätzen auch im Bereich der Forschung bestimmte Risiken verbunden sind. Die Datenschutzgruppe ist der Ansicht, dass der Zugang zu Proben und Datensätzen streng auf den Bereich der Forschung beschränkt und nur für Forschungszwecke gestattet sein sollte. Darüber hinaus muss geklärt werden, unter welchen Bedingungen Forschungsergebnisse (unter Berücksichtigung des jeweils persönlichen Anspruchs auf entsprechende Unterrichtung) gegenüber Einzelpersonen offen gelegt oder in medizinische Unterlagen eingebunden werden können.

Im Zusammenhang mit der Nutzung von Systemen zur Analyse von DNA-Proben können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Auch wenn die Zuverlässigkeit von DNA-Analysen sehr hoch ist, sollte berücksichtigt werden, dass die Qualität der Ergebnisse von der Anzahl der analysierten Marker (Loci) abhängt. Die eingesetzten Testsysteme sollten die größtmögliche Zuverlässigkeit gewährleisten.

- Auswirkung: Die Durchführung von DNA-Analysen kann als äußerst schwerer Eingriff in die Privatsphäre betrachtet werden. Genetische Daten können sensible Informationen enthalten. Anhand statistischer Analysen der vorhandenen Daten können Profile erstellt werden, die Diskriminierungen der betroffenen Personen zur Folge haben können.

- Sonstige Zwecke bzw. Verarbeitungszwecke: Mit neuen Technologien können inzwischen zunehmend größere Datenbestände ausgetauscht werden. Daher muss klar sein, wer Zugang zu den Informationen in einer DNA-Datenbank erhält. Familienbezogene Suchabfragen und Abfragen nach rassischer Herkunft können als neue Technologien betrachtet werden, die dem ursprünglichen Zweck der Verarbeitung der gegenwärtig verfügbaren DNA-Datenbanken zuwiderlaufen.

- Einwilligung und Transparenz: Inzwischen werden Dienste zur Durchführung von DNA-Analysen anhand biologischer Proben angeboten, die auf dem Postweg eingesandt werden (beispielsweise Speichelproben), und bei denen die Ergebnisse im Internet bereitgestellt werden. Unzureichende Identitätsprüfungen könnten dazu führen, dass Einzelpersonen oder sonstige Rechtssubjekte Proben anderer Personen übermitteln und dadurch sensible personenbezogene Daten Dritter in Erfahrung bringen.

- Verknüpfbarkeit: Angesichts des Umfangs und der Vielfalt der Informationen, die aus der Sequenzierung von DNA-Proben abgeleitet werden können, besteht bei DNA-Analysen ein hohes Missbrauchsrisiko, da die gewonnenen Daten leicht mit anderen Datenbanken verknüpft werden können, um dann personenbezogene Profile zu erstellen. Familienbezogene Suchabfragen ermöglichen die Herstellung von Verknüpfungen mit Verwandten.

- Verarbeitung sensibler Daten: DNA-Proben können Informationen über den Gesundheitszustand sowie über die Disposition für bestimmte Krankheiten oder die ethnische Herkunft einer Person enthalten. Bei der Auswahl der relevanten Loci ist daher von äußerster Bedeutung, dass der Grundsatz der Datenminimierung berücksichtigt wird. DNA-Informationen können aus vielen Proben auch über einen längeren Zeitraum gewonnen werden. Daher sollte sichergestellt werden, dass der Zugang zu den Proben streng auf befugte Benutzer und auf zugelassene Verwendungen beschränkt wird.

- Widerruflichkeit: DNA-Informationen sind nicht widerruflich.

- Schutz gegen Spoofing: DNA-Daten sind für Spoofing-Angriffe naturgemäß äußerst schwierig einzusetzen. Häufig ist es jedoch nicht schwer, sich DNA-Proben (z. B. Haare) ohne Wissen der betroffenen Person zu beschaffen.

4.4.6. Biometrische Identifikation von Unterschriften

Die Erfassung biometrischer Daten zu Unterschriften ist ein Beispiel für neue Nutzungen herkömmlicher biometrischer Technologien. Biometrische Daten zu Unterschriften werden durch biometrische Verfahren ermittelt, bei denen das Verhalten einer Person aufgrund der Dynamik der jeweiligen Handschrift bewertet wird. Herkömmliche Systeme zur Erkennung von Unterschriften beruhen auf der Analyse statischer oder geometrischer Merkmale des jeweiligen Unterschriftsbildes. (Die Analysen erfolgen also aufgrund der Darstellung einer Unterschrift.) Biometrische Verfahren zur Erkennung von Unterschriften hingegen analysieren die dynamischen Merkmale einer Unterschrift (d. h., wie die Unterschrift vorgenommen wurde). Entsprechend heißt es häufig, diese Verfahren analysieren „dynamische Unterschriften“.

Typische dynamische Merkmale, die von biometrischen Systemen zur Erkennung von Unterschriften (z. B. von einem Digitalisierungstablett) ermittelt werden, sind der Schreibdruck, der Schreibwinkel, die Geschwindigkeit und die Beschleunigung der Stiftführung, die Bildung der Buchstaben und die Strichrichtung sowie eine Reihe weiterer individueller dynamischer Merkmale. Welche dieser Merkmale berücksichtigt werden, ist von Anbieter zu Anbieter unterschiedlich. Gewöhnlich werden diese Merkmale mithilfe druckempfindlicher Geräte festgestellt. Einige Systeme zur Erkennung von Unterschriften können Verifikationen durchführen, indem sie Analysen statischer Merkmale (d. h. des Schriftbildes) mit Analysen dynamischer Merkmale (Schreibdruck, Schreibwinkel, Schreibgeschwindigkeit usw.) verknüpfen.

Im Zusammenhang mit der Nutzung von Systemen zur biometrischen Erkennung von Unterschriften können sich die folgenden Risiken für den Datenschutz ergeben:

- Zuverlässigkeit: Unterschriften werden nicht immer in der gleichen Weise geleistet. Entsprechend können die Erfassung und die Verifikation von Identitäten problematisch sein.

- Auswirkung: Auf Verhaltensmerkmalen beruhende biometrische Daten wie beispielsweise eine Unterschrift können sich im Laufe der Zeit ändern, oder die betreffenden Personen können ihr Verhalten bewusst ändern. Auch physiologische Ursachen können Änderungen einer Unterschrift zur Folge haben und einer erfolgreichen Verifikation entgegenstehen. Entsprechend müssen alternative Verfahren verfügbar sein, um die Identität von Personen zu verifizieren.

- Schutz gegen Spoofing: Das Schriftbild einer herkömmlichen Unterschrift kann leicht nachgebildet und (von einer entsprechend erfahrenen Person) nachgeahmt, fotokopiert oder mit einer Grafik-Software erfasst werden. Sicherer ist die Verifikation anhand einer dynamischen Unterschrift, weil im Verifikationsprozess auch die komplexeren und für die Handschrift einer Person ganz typischen dynamischen Merkmale geprüft werden.

5. Allgemeine Leitlinien, sektorbezogene Empfehlungen und technische und organisatorische Maßnahmen

Der Einsatz eines biometrischen Systems hängt vom Zusammenwirken mehrerer Akteure ab:

- Hersteller: Entwicklung und Prüfung biometrischer Sensoren und Feststellung der Leistungsfähigkeit biometrischer Technologien;
- integrierte Dienstleister: Entwicklung des Endproduktes, das schließlich an die Kunden verkauft wird; Auswahl der biometrischen Technologie und teilweise Festlegung der Zwecke, für die das jeweilige System eingesetzt wird; (dabei werden die jeweiligen Kunden berücksichtigt;)
- Wiederverkäufer: Vermarktung des Endproduktes bei den Kunden: Aufklärung der Kunden über die Leistungsfähigkeit und die Risiken der Systeme sowie möglicherweise über den maßgeblichen Rechtsrahmen;
- mit der Einrichtung der Systeme befasste Fachkräfte: Einrichtung des Produktes in den Räumlichkeiten der Kunden;
- Kunden: Entscheidung für den Erwerb eines biometrischen Systems; Festlegung des Zwecks und der Mittel zur Verarbeitung der Daten; insoweit sind die Kunden als für die Verarbeitung Verantwortliche zu betrachten;
- betroffene Personen: Bereitstellung biometrischer Daten zur Verwendung im System.

Einige Akteure übernehmen eine oder mehrere der oben beschriebenen Rollen. Mit jeder Rolle ist eine eigene Zuständigkeit verbunden, um eine mit der Wahrung der Privatsphäre zu vereinbarende Verwendung biometrischer Systeme zu gewährleisten. Eine mit der Einrichtung eines Systems beauftragte Person beispielsweise kann keine vom jeweiligen integrierten Dienstleister entwickelte Sicherheitsfunktion aktivieren.

5.1. Allgemeine Grundsätze

Die Sicherheit biometrischer Daten sollte ein wesentlicher Aspekt sein, weil biometrische Daten nicht widerruflich sind. Entsprechend gefährdet die Verletzung des Schutzes biometrischer Daten auch die weitere sichere Verwendung des Datenmaterials für Identifikationsprozesse und beeinträchtigt das Recht der betroffenen Personen auf den Schutz ihrer Daten. Dabei ist zu beachten, dass die Auswirkungen einer Beeinträchtigung der Sicherheit nicht mehr rückgängig gemacht werden können.

Die entsprechenden Risiken erhöhen sich mit der Anzahl der eingesetzten Anwendungen zur Verarbeitung dieser Daten. (Dies gilt insbesondere für das Risiko einer Verletzung des Schutzes personenbezogener Daten und eines Function Creep.) Je mehr biometrische Daten verwendet werden, desto wahrscheinlicher wird auch ein Diebstahl biometrischer Daten.

Die Datenschutzgruppe stellt gegenwärtig einen Trend dahin gehend fest, Fernzugriffe auf biometrische Systeme zuzulassen (beispielsweise über Internet-Schnittstellen). Mit diesem Trend ist eine Reihe neuer Sicherheitsprobleme verbunden, die in der IT-Branche durchaus bekannt sind. Bereits in einer frühen Phase der Systementwicklung sollten daher IT-Fachkräfte, die über angemessene Erfahrungen mit der technischen Sicherheit der

einzusetzenden Systeme verfügen, mit der Einrichtung eines geeigneten Systems beauftragt werden.

Die Datenschutzgruppe empfiehlt einen weitreichenden technischen Schutz bei der Verarbeitung biometrischer Daten. Dabei sollten die modernsten technischen Mittel zum Einsatz kommen. In diesem Zusammenhang sollten bestehende Industrienormen für den Schutz von Systemen berücksichtigt werden, in denen biometrische Informationen verarbeitet werden.

5.2. Eingebauter Datenschutz (*Privacy by Design*)

Die Einrichtung von Funktionen zur Gewährleistung des Datenschutzes bereits bei der Systemauslegung (*Privacy by Design* = „eingebauter Datenschutz“) bedeutet, dass die Wahrung der Privatsphäre proaktiv bereits bei der Entwicklung der eigentlichen Technologie berücksichtigt wird.

Das Konzept des „eingebauten Datenschutzes“ betrifft bei biometrischen Systemen die gesamte Wertschöpfungskette:

- Bei der Entwicklung neuer Technologien und Sensoren sollten Hersteller die Grundsätze des eingebauten Datenschutzes berücksichtigen. Nach diesen Grundsätzen sind unter anderem Rohdaten automatisch zu löschen, nachdem ein Template berechnet wurde. Außerdem sind biometrische Daten grundsätzlich verschlüsselt zu speichern. (Dies gilt sowohl für die Speicherung in einer zentralen Datenbank als auch für die Speicherung auf einer Smart Card.) Zudem sollten sich die Hersteller auf die Entwicklung biometrischer Technologien konzentrieren, die schon durch ihre Auslegung einen besseren Datenschutz gewährleisten;
- auch integrierte Dienstleister und Wiederverkäufer sollten die Grundsätze des eingebauten Datenschutzes bei der Beschreibung des zu vermarktenden Endproduktes berücksichtigen, indem sie datenschutzgerechtere Technologien auswählen und geeignete Garantien für das Endprodukt vorsehen (beispielsweise durch eine dezentrale Gestaltung der Datenbank);
- die Kunden (als potenziell für die Verarbeitung Verantwortliche) sollten die Grundsätze des eingebauten Datenschutzes berücksichtigen, wenn sie ein bestimmtes biometrisches System bestellen oder die technischen Merkmale eines Systems spezifizieren. In diesem Zusammenhang sollten Hersteller und integrierte Dienstleister in ihren Produkten eine gewisse Flexibilität vorsehen, um den Grundsätzen der Verhältnismäßigkeit, der Zweckbindung, der Datenminimierung und der Sicherheit Rechnung zu tragen.

Diese Grundsätze wurden bei einigen biometrischen Geräten bereits erfolgreich in der Praxis berücksichtigt. Um unbefugten Zugriffen auf biometrische Daten entgegenzuwirken, haben manche Hersteller in einem bestimmten biometrischen Lesegerät Verschlüsselungsfunktionen sowie Schaltungen vorgesehen, die das Auslesen und Manipulieren von Daten verhindern.

Die Datenschutzgruppe empfiehlt, bei der Auslegung biometrischer Systeme formale „Entwicklungslebenszyklen“ mit folgenden Schritten zu berücksichtigen:

1. Spezifikation von Anforderungen gemäß einer Risikoanalyse und/oder gemäß einer speziellen PIA (*Privacy Impact Assessment* = Datenschutz-Folgenabschätzung);
2. Beschreibungen und Begründungen dahin gehend, wie durch die jeweilige Auslegung die bestehenden Anforderungen erfüllt werden;
3. Validierung mithilfe von Funktions- und Sicherheitstests;

4. Verifikation der Konformität der endgültigen Gestaltung mit dem geltenden Rechtsrahmen.

Die Datenschutzgruppe befürwortet die Definition von Zertifizierungsplänen, welche die Umsetzung des Grundsatzes des eingebauten Datenschutzes gewährleisten und die Aufklärung der für die Verarbeitung Verantwortlichen über die datenschutzrechtlichen Risiken biometrischer Systeme verbessern könnten.

5.3. Rahmen der Datenschutz-Folgenabschätzung

5.3.1. Allgemeine Grundsätze

Die PIA (*Privacy Impact Assessment* = Datenschutz-Folgenabschätzung) ist ein Prozess, bei dem ein Rechtssubjekt die mit der Verarbeitung personenbezogener Daten verbundenen Risiken bewertet und zusätzliche Maßnahmen zur Verringerung dieser Risiken definiert. Bezüglich der RFID-Technologie beispielsweise hat die Datenschutzgruppe festgestellt, dass das Rechtssubjekt, das die betreffende Anwendung beschreibt, auch für die Durchführung der PIA zuständig ist. Dieses Rechtssubjekt kann sowohl der für die Verarbeitung Verantwortliche als auch der Anbieter sein, der die jeweilige RFID-Anwendung konzipiert.

Wegen der mit der Nutzung biometrischer Daten verbundenen spezifischen Risiken empfiehlt die Arbeitsgruppe, dass derjenige, der den Zweck eines Geräts und die jeweils eingesetzten Mittel beschreibt (d. h. der Hersteller, der integrierte Dienstleister oder der Endkunde), im Zusammenhang mit der Auslegung eines Systems zur Verarbeitung des betreffenden Datentyps auch Datenschutz-Folgenabschätzungen durchführt und dass diese Folgenabschätzungen als wesentlicher Bestandteil der Systemauslegung behandelt werden.

Bei der PIA sollten die folgenden Aspekte berücksichtigt werden:

- Art der erfassten Informationen,
- Zweck der Informationserfassung,
- Zuverlässigkeit des Systems (in der Annahme, dass ein positives bzw. negatives Ergebnis einer biometrischen Prüfung wesentliche Entscheidungen für die betroffene Person zur Folge haben kann),
- Rechtsgrundlage und rechtliche Konformität; ist eine Einwilligung vorgeschrieben?
- Zugang zum jeweiligen Gerät und interne und externe Weitergabe von Informationen durch den für die Verarbeitung Verantwortlichen, wobei personenbezogene Daten durch geeignete Sicherheitstechniken und -verfahren gegen unbefugte Zugriffe zu schützen sind,
- bereits getroffene und die Privatsphäre weniger beeinträchtigende Maßnahmen; ist im Hinblick auf das jeweilige biometrische Gerät bereits ein alternatives Verfahren denkbar (beispielsweise die Vorlage eines Ausweises)?
- Entscheidungen bezüglich der Aufbewahrungszeit und der Löschung von Daten; welche Zeiträume wurden vorgesehen? Gelten für sämtliche Daten die gleichen Aufbewahrungszeiten? Besteht ein automatisierter Mechanismus oder ein geeigneter Alternativprozess?
- Rechte der betroffenen Personen.

Die Datenschutz-Folgenabschätzung sollte sich nicht nur auf die Identifikation der bestehenden Risiken konzentrieren. Vielmehr sollten auch geeignete datenschutzrechtliche Maßnahmen vorgesehen werden; außerdem sollte erläutert werden, wie der für die

Verarbeitung Verantwortliche zu geeigneten Lösungen gelangt ist, mit denen die im vorherigen Schritt ermittelten datenschutzrechtlichen Risiken verringert werden können.

Wenn der Hersteller oder der integrierte Dienstleister die PIA durchgeführt hat, kann die Einführung des jeweiligen biometrischen Systems eine weitere Bewertung erfordern, bei der die besonderen Bedingungen des für die Verarbeitung Verantwortlichen zu berücksichtigen sind. Wenn ein biometrisches System beispielsweise in das Informationssystem eines Kunden integriert wird, sollte der Kunde eine weitere PIA durchführen, bei der die sicherheitstechnischen Maßnahmen und Verfahren im eigenen IT-System geprüft werden.

5.3.2. Die Spezifität biometrischer Daten

Biometrische Daten erfordern insoweit besondere Aufmerksamkeit, als anhand dieser Daten einzelne Personen aufgrund ihrer individuellen verhaltensbezogenen oder physiologischen Merkmale zweifelsfrei identifiziert werden können.

Daher sollte mit PIAs möglichst bewertet werden, wie die drei folgenden Risiken durch das zu analysierende System vermieden oder zumindest in erheblichem Umfang eingeschränkt werden können:

Das erste Risiko ist die Gefahr des Identitätsbetrugs, insbesondere in Verbindung mit Identifikations- und Authentifikationverfahren. Das betreffende biometrische System darf nicht durch Spoofing-Angriffe zu täuschen sein und muss gewährleisten, dass die Person, die einen Abgleich vornehmen möchte, tatsächlich mit der im System registrierten Person identisch ist. Diese Bedrohung erscheint bei biometrischen Daten, die ohne Wissen der betroffenen Person nicht erfasst werden können (d. h. beispielsweise in Bezug auf Venenstrukturen), weniger einsichtig.[17] Bei Geräten zur Verarbeitung von Fingerabdrücken oder zur Gesichtserkennung ist dies jedoch ein wesentlicher Aspekt. Fingerabdrücke werden nämlich überall hinterlassen, einfach indem jemand einen Gegenstand berührt. Und Gesichter können auf einem Foto erfasst werden, ohne dass der betreffenden Person dies bewusst ist.

Das zweite Risiko besteht in einer Modifikation des ursprünglichen Zwecks entweder durch den für die Verarbeitung Verantwortlichen selbst oder durch einen Dritten (einschließlich der Rechtsdurchsetzungsbehörden. Diese allgemeine Bedrohung im Hinblick auf personenbezogene Daten wird bei biometrischen Daten zur zentralen Bedrohung. Die Hersteller sollten alle verfügbaren Sicherheitsmaßnahmen treffen, um jegliche unangemessene Nutzung der Daten zu verhindern und um sicherzustellen, dass für eine Verarbeitung nicht mehr benötigte Daten umgehend gelöscht werden.

Ebenso wie andere Daten können auch rechtmäßig verarbeitete oder gespeicherte biometrische Daten bzw. die Quellen biometrischer Daten von dem für die Verarbeitung Verantwortlichen nicht für neue oder anderweitige Zwecke verarbeitet oder erfasst werden, wenn keine neue rechtmäßige Begründung für den neuen Verarbeitungszwecke gegeben ist.

Das dritte Risiko ist die Verletzung des Schutzes personenbezogener Daten; dieses Risiko erfordert je nach Art der gefährdeten biometrischen Daten besondere Maßnahmen. Wenn bei einem System, das biometrische Daten mithilfe eines Algorithmus erzeugt, der ein biometrisches Template in einen bestimmten Code konvertiert, entweder die eigentlichen biometrischen Daten oder die betreffenden Algorithmen gestohlen oder gefährdet werden,

[17] Angesichts der zunehmenden Verbreitung dieser Technologie gilt dies auch dann, wenn schwer abzusehen ist, wie sich Angriffe auf Systeme zur Verarbeitung von Venenstrukturen in den folgenden Jahren gestalten könnten.

müssen die betreffenden Daten oder Algorithmen ersetzt werden. Wenn eine Verletzung des Schutzes personenbezogener Daten mit dem Verlust direkt identifizierter biometrischer Daten einhergeht, die in engem Zusammenhang mit der Quelle dieser biometrischen Daten stehen (z. B. Fingerabdrücke oder Porträtbilder), muss die betreffende Person umfassend unterrichtet werden, damit sie sich verteidigen kann, wenn diese gefährdeten biometrischen Daten als Beweismittel gegen diese Person verwendet werden.

5.4. Technische und organisatorische Maßnahmen

Wegen der Art des Datenmaterials erfordert die Verarbeitung biometrischer Daten spezielle technische und organisatorische Maßnahmen und Vorkehrungen, um Beeinträchtigungen der betroffenen Personen infolge einer Verletzung des Schutzes personenbezogener Daten zu vermeiden. Dies gilt insbesondere angesichts der Gefahr eines rechtswidrigen Verhaltens nach der unbefugten „Rekonstruktion" eines biometrischen Merkmals anhand eines Referenz-Template oder aufgrund der Verknüpfung mit anderen Datenbanken sowie für die Gefahr einer nicht bestimmungsgemäßen Nutzung ohne Wissen der betroffenen Personen und/oder die Gefahr, dass gewisse biometrische Daten genutzt werden könnten, um Informationen über die rassische Herkunft oder über den Gesundheitszustand bestimmter Personen zu erhalten.

5.4.1. Technische Maßnahmen

- *Verwendung biometrischer Templates*

Biometrische Daten sollten nach Möglichkeit grundsätzlich als biometrische Templates gespeichert werden.

Die Templates sollten in einer für das jeweilige biometrische System spezifischen Form extrahiert werden, und eine Verwendung in ähnlichen Systemen durch die jeweils für die Verarbeitung Verantwortlichen muss ausgeschlossen werden, um sicherzustellen, dass die betreffenden Personen nur in den biometrischen Systemen identifiziert werden können, bei denen eine entsprechende Rechtsgrundlage gegeben ist.

- *Speicherung auf einem persönlichen Gerät im Vergleich zu einer zentralen Speicherung*

Wenn die Verarbeitung biometrischer Daten zulässig ist, sollten personenbezogene biometrische Informationen vorzugsweise nicht zentral gespeichert werden.

Insbesondere im Zusammenhang mit Verifikationen hält die Datenschutzgruppe für empfehlenswert, dass biometrische Systeme biometrische Daten aus verschlüsselten Templates auf Medien lesen, die sich ausschließlich im Besitz der betroffenen Personen befinden (z. B. Smart Cards oder ähnliche Speichermedien). Die biometrischen Merkmale der betroffenen Personen können mit den auf der Karte und/oder den sonstigen Medien gespeicherten Templates verglichen werden. Dazu sollten Standard-Vergleichsverfahren zum Einsatz kommen, die ebenfalls unmittelbar auf der betreffenden Karte und/oder dem betreffenden Medium definiert sind. Auf diese Weise sollte die Erstellung einer Datenbank mit biometrischen Informationen im Allgemeinen nach Möglichkeit vermieden werden. Wenn die Karte und/oder das Speichermedium verloren gehen oder verlegt werden, besteht die Gefahr eines Missbrauchs der biometrischen Informationen nach gegenwärtigem Kenntnisstand nur in eingeschränktem Umfang. Um das Risiko eines Identitätsdiebstahls zu verringern, sollten auf den entsprechenden Systemen identifikationsrelevante Daten zur betreffenden Person ebenfalls nur in eingeschränktem Umfang gespeichert werden.

Für spezifische Zwecke sowie wenn objektive Erfordernisse gegeben sind, kommt jedoch auch eine zentrale Datenbank mit biometrischen Informationen und/oder Templates in Betracht. Das eingesetzte biometrische System und die ausgewählten Sicherheitsmaßnahmen

sollten die genannten Risiken begrenzen und gewährleisten, dass die Weiterverwendung der betreffenden biometrischen Daten für sonstige Zwecke ausgeschlossen ist oder zumindest zurückverfolgt werden kann. Um das unbefugte Lesen, Kopieren, Modifizieren oder Löschen biometrischer Daten zu verhindern, sollten Mechanismen auf der Grundlage von Verschlüsselungstechnologien eingesetzt werden.

Wenn die biometrischen Daten auf einem System gespeichert werden, das der physischen Kontrolle der betroffenen Person unterliegt, sollte ein spezifischer Verschlüsselungscode als wirksame Maßnahme vorgesehen werden, um diese Daten vor unbefugten Zugriffen zu schützen. Außerdem bieten diese dezentralen Systeme schon aufgrund ihrer Auslegung einen besseren Schutz der biometrischen Daten, da die betroffene Person die physische Kontrolle über ihre biometrischen Daten behält und da kein gemeinsames Ziel existiert, auf das sich Angriffe richten könnten.

Die Datenschutzgruppe betont ferner, dass der Begriff einer zentralen Datenbank eine Vielzahl technischer Anwendungen von der Speicherung in einem Lesegerät bis hin zu Datenbanken auf einem Netz-Host beinhaltet.

- *Möglichkeit der Erneuerung und des Widerrufs*

Da die Quelle biometrischer Daten nicht geändert werden kann, müssen biometrische Systeme zur Verknüpfung von Identitäten so ausgelegt sein, dass der Prozess der Erfassung sowie die Verarbeitung biometrischer Daten die Möglichkeit bieten, aus der gleichen Quelle mehrere voneinander unabhängige biometrische Templates zu extrahieren, damit die Daten beispielsweise bei einer Verletzung des Schutzes personenbezogener Daten oder infolge einer technischen Weiterentwicklung ersetzt werden können.

Biometrische Systeme sollten so ausgelegt werden, dass die Verknüpfung mit einer Identität aufgehoben werden kann, um die Verknüpfung zu erneuern oder endgültig zu löschen (z. B. wenn die erteilte Einwilligung widerrufen wurde).[18]

- *Verschlüsselung*

Aus Sicherheitsgründen sollten angemessene Maßnahmen zum Schutz der durch das jeweilige biometrische System gespeicherten und verarbeiteten Daten getroffen werden. Daher sind biometrische Informationen grundsätzlich verschlüsselt zu speichern. Um sicherzustellen, dass die Codes nur für die entsprechend befugten Personen zugänglich sind, muss ein geeigneter Rahmen für die Verwaltung der Codes definiert werden.

Angesichts der verbreiteten Nutzung öffentlicher und privater Datenbanken mit biometrischen Informationen sowie im Bestreben, die Interoperabilität biometrischer Systeme zu verbessern, sollte die Nutzung spezifischer Technologien oder Datenformate angestrebt werden, bei denen

[18] Ein Beispiel ist etwa die TURBINE-Technologie zum Schutz biometrischer Templates durch fotografische Umwandlung von Fingerabdruckdaten in einen nicht mehr konvertierbaren Code, der Bit für Bit verglichen werden kann. Es wird davon ausgegangen, dass sich die biometrischen Proben und die Original-Templates aus den umgewandelten biometrischen Daten nicht mehr wiederherstellen lassen. Um das Vertrauen der Nutzer auf die Technologie zusätzlich zu erhöhen, wird auch dieser Code widerruflich definiert. Entsprechend kann gegebenenfalls ein neuer unabhängiger Code erzeugt werden, um biometrische Identitäten neu zu definieren (siehe auch http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-02-01_FP7_EN.pdf).

eine Verknüpfung biometrischer Datenbanken und die ungeprüfte Offenlegung von Daten nicht möglich sind.

- *Schutz gegen Spoofing:*

Um die Zuverlässigkeit eines biometrischen Systems zu erhalten und Fälle von Identitätsbetrug auszuschließen, müssen die Hersteller Systeme einrichten, mit denen festgestellt werden kann, ob die biometrischen Daten echt sind und ob die Verknüpfung mit einer natürlichen Person noch besteht. Bei Systemen zur Gesichtserkennung kann entscheidend sein, dass die Systeme echte Gesichter zuverlässig beispielsweise von Bildern unterscheiden, die ein Betrüger vor sein eigenes Gesicht hält.

- *Biometrischer Ver- und Entschlüsselung*

Die biometrische Verschlüsselung ist ein Verfahren, bei dem biometrische Merkmale in die Prozesse zur Verschlüsselung und zur Entschlüsselung von Daten einbezogen werden. Dazu wird im Allgemeinen ein Auszug der verfügbaren biometrischen Daten als Code zur Verschlüsselung eines Identifikators verwendet, der zur Nutzung des betreffenden Dienstes benötigt wird.

Dieser Ansatz hat viele Vorteile.[19] Bei diesen Systemen werden der Identifikator und die biometrischen Daten nicht in ihrer ursprünglichen Form gespeichert. Nur das Ergebnis der Identifikatorprüfung wird biometrisch verschlüsselt im System abgelegt. Zudem können die personenbezogenen Daten insoweit widerrufen werden, als die Möglichkeit besteht, einen weiteren Identifikator zu erzeugen und biometrisch zu verschlüsseln. Und schließlich sind diese Systeme sicherer und benutzerfreundlicher, da sich die Benutzer bei diesen Systemen keine langen und komplexen Kennwörter merken müssen.

Die Verschlüsselung ist jedoch insoweit problematisch, als Verschlüsselungen und Entschlüsselungen unveränderliche Codes voraussetzen und biometrische Daten unterschiedliche Strukturen ergeben, durch die sich die jeweils generierten Codes ändern können. Daher muss das System in der Lage sein, auch bei leicht abweichenden biometrischen Daten dieselben Codes zu erzeugen, ohne die Quote falsch positiver Ergebnisse zu erhöhen.

Die Datenschutzgruppe ist sich einig dahin gehend, dass die biometrische Verschlüsselung ein vielversprechendes Forschungsgebiet darstellt und so weit ausgereift ist, dass die politische Diskussion auch in der breiten Öffentlichkeit erfolgen kann und dass Prototypen entwickelt und praktische Anwendungen in Erwägung gezogen werden können.

- *Automatisierte Mechanismen zur Löschung von Daten*

Um zu verhindern, dass biometrische Informationen länger als für die ursprünglich vorgesehenen Zwecke bzw. für die anschließende Verarbeitung erforderlich gespeichert werden, sind geeignete automatisierte Mechanismen zur Löschung der Daten auch dann einzurichten, wenn die Aufbewahrungszeit rechtmäßig verlängert werden kann. Dadurch ist die umgehende Löschung personenbezogener Daten sicherzustellen, die für den Einsatz des jeweiligen biometrischen Systems nicht mehr benötigt werden.

Wenn das Lesegerät über einen integrierten Speicher verfügt, können die Hersteller biometrische Templates auch auf einem flüchtigen Speicher erfassen, bei dem garantiert ist, dass die Daten gelöscht werden, sobald die Verbindung zum Lesegerät getrennt wird. Damit

[19] http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

ist gewährleistet, dass bei einem Verkauf oder bei einer Deinstallation des Lesegeräts keine biometrische Datenbank mehr gespeichert ist. Die automatische Löschung der Daten kann auch durch Schaltungen bewirkt werden, die ein Auslesen der gespeicherten Daten verhindern (Anti-Pulling-Switches), indem das betreffende Datenmaterial bei einem Diebstahlversuch sofort gelöscht wird.

- *Umfangreiche biometrische Datenbanken und Datenbanken mit „schwachen Verknüpfungen“*

In manchen Ländern werden umfangreiche biometrische Datenbanken hauptsächlich für zwei Zwecke eingesetzt: zur Unterstützung strafrechtlicher Untersuchungen und um sicherzustellen, dass Ausweispapiere (Reisepässe, Ausweise, Führerscheine) ordnungsgemäß erfasst werden. In Datenbanken für strafrechtliche Untersuchungen werden im Allgemeinen Informationen über Straftäter und über verdächtige Personen verwaltet. Diese Datenbanken müssen so gestaltet sein, dass Personen anhand der jeweiligen biometrischen Daten identifiziert werden können. Datenbanken zur Bekämpfung von Identitätsbetrug enthalten dagegen biometrische Daten der gesamten Bevölkerung und sollten ausschließlich genutzt werden, um einzelne Personen zu authentifizieren (beispielsweise, wenn jemand seine Ausweispapiere verloren hat oder wenn der Sicherheits-Chip des Reisepasses mit den entsprechenden biometrischen Daten zerstört wurde).

Wenn eine zentrale Datenbank genutzt wird, um gegen Fälle von Identitätsbetrug vorzugehen, ist die Datenschutzgruppe der Ansicht, dass geeignete technische Maßnahmen vorgesehen werden müssen, um jegliche nicht mit dem ursprünglichen Zweck zu vereinbarende Nutzung der Datenbank zu verhindern. Erstens erfordert der Grundsatz der Datenminimierung, dass ausschließlich die zur Authentifikation einer Person erforderlichen Daten erfasst werden. Beispielsweise wird davon ausgegangen, dass der Vergleich der Abdrücke von zwei Fingern hinreichende Informationen für die Authentifikation einer Person ergibt.

Außerdem können für die Verarbeitung Verantwortliche Datenbanken mit „schwachen Verknüpfungen“ nutzen, bei denen die Identität einer Person nicht mit einem einzelnen Satz biometrischer Daten verknüpft ist, sondern vielmehr einer ganzen Gruppe biometrischer Daten zugeordnet wird. Die Gestaltung dieser Datenbank sollte die Authentifikation einer Person mit sehr hoher Wahrscheinlichkeit gewährleisten (d. h. z. B. mit einer Wahrscheinlichkeit von 99,9 %, die hinreichend sein müsste, um Betrüger abzuschrecken). Außerdem müsste durch die Gestaltung der Datenbank sichergestellt sein, dass die Datenbank nicht für Identifikationen genutzt werden kann (weil nämlich jeder einzelne Satz biometrischer Daten zahlreichen Personen zugeordnet werden kann).

Die Datenschutzgruppe befürwortet den Einsatz dieser Systeme, wenn umfangreiche biometrische Datenbanken genutzt werden, um gegen Fälle von Identitätsbetrug vorzugehen.

Beispiel: Technische Maßnahmen für Authentifikationssysteme
Biometrische Daten haben jeweils eine individuelle Quelle, die lebenslang mit der betroffenen Person verbunden sein kann. Wenn diese Quelle von einem Authentifikationssystem als Grundlage genutzt wird, ist zu beachten, dass diese Quelle nicht geändert werden kann. Bei sonstigen Authentifikationstechnologien, bei denen die Nutzer in der Regel ein bestimmtes Merkmal „wissen“ oder „besitzen“ müssen (beispielsweise eine Benutzerkennung oder ein Kennwort), kann das definierte Ausweiskriterium immer geändert werden. Daher müssen beim Einsatz biometrischer Authentifikationssysteme spezielle Garantien vorgesehen werden, um die Verknüpfung der biometrischen Daten mit sonstigen personenbezogenen Daten zu verhindern:

- Template-Daten sollten nicht zentral gespeichert werden, da die Sicherheit der Speicherung biometrischer Daten von wesentlicher Bedeutung für die Gesamtsicherheit des jeweiligen biometrischen Systems ist. Vorzugsweise sollte eine verteilte Speicherung (z. B. auf Smart Cards) erfolgen. In diesem Fall befinden sich sowohl die Quelle der Daten als auch das Template im Besitz der betroffenen Person.
- Die Speicherung und Übertragung biometrischer Daten müssen derart geschützt erfolgen, dass die Daten nicht durch geeignete Verschlüsselungstechnologien abgefangen, unbefugt offen gelegt oder geändert werden können.
- Bestimmte Typen biometrischer Daten sind nicht geheim (z. B. Gesichter). Diese Daten können nach einer Verletzung des Schutzes personenbezogener Daten sowie nach einer Offenlegung oder einem Missbrauch nicht gesperrt, blockiert oder geändert werden. Daher sollte die Authentifikation mit weiteren Merkmalen kombiniert werden, bei denen Sperrungen oder Änderungen vorgenommen werden können.

5.4.2. Organisatorische Maßnahmen

Um den erforderlichen Datenschutz zu gewährleisten, müssen organisatorische Maßnahmen geplant und durchgeführt werden. Der für die Verarbeitung Verantwortliche muss beispielsweise ein klares Verfahren entwickeln, mit dem festgestellt werden kann, wer auf die im System gespeicherten Informationen zugreifen kann. Außerdem muss in diesem Verfahren geregelt sein, ob die Zugriffe unbeschränkt oder nur auf gewisse Informationen erfolgen können sowie gegebenenfalls, aus welchen Gründen Einschränkungen vorgenommen wurden. Sämtliche Eingriffe müssen rückverfolgbar sein.

Die Datenschutzgruppe stellt fest, dass die Auslagerung an externe Dienstleister sogar in Verbindung mit der Bearbeitung von Visaanträgen möglich ist (siehe Abschnitte 13 und 43 der Verordnung (EG) Nr. 810/2009 vom 13. Juli 2009 über einen Visakodex der Gemeinschaft) und dass diese Auslagerung infolge des Aufkommens von Cloud-Speichern zunehmend häufiger erfolgt.

In diesem Fall muss der für die Verarbeitung Verantwortliche eine detaillierte Regelung dahin gehend treffen, wie die jeweiligen Unterauftragnehmer kontrolliert werden können (beispielsweise durch unangekündigte Nachprüfungen). Außerdem muss er Garantien in Bezug auf die betreffenden Mitarbeiter, Verfahren zum Schutz der individuellen Rechte usw. vorsehen.

Brüssel, den 27. April 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM