ARTIKEL 29-DATENSCHUTZGRUPPE

12168/02/DE
WP 80

Arbeitspapier über Biometrie

angenommen am 1. August 2003

Die Arbeitsgruppe wurde durch Artikel 29 Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der EU in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 Richtlinie 95/46/EG festgelegt, ferner in Artikel 14 Richtlinie 97/66/EG. Das Sekretariat wird von folgender Dienststelle gestellt:

Europäische Kommission, GD Binnenmarkt, Direktion E (Dienstleistungen, geistiges und gewerbliches Eigentum, Medien und Datenschutz), Anschrift: Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgien - Büro: C100-6/136.

Website: www.europa.eu.int/comm/privacy

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

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

gestützt auf ihre Geschäftsordnung, insbesondere auf Artikel 12 und 14 -

hat folgendes Arbeitspapier angenommen:

1. EINFÜHRUNG

Die rasanten Fortschritte auf dem Gebiet der biometrischen Verfahren und ihre in jüngster Zeit zunehmende Anwendung in unterschiedlichsten Bereichen machen eine sorgfältige Prüfung aus Datenschutzsicht erforderlich[2]. Ein weit verbreiteter und unkontrollierter Einsatz der Biometrie bietet Anlass zu Sorge um den Schutz der Grundrechte und -freiheiten des Einzelnen. Biometrische Daten sind Daten besonderer Art, da sie sich auf die verhaltenstypischen und physiologischen Merkmale einer Person beziehen und unter Umständen ihre eindeutige Identifizierung ermöglichen[3].

Die Verarbeitung biometrischer Daten wird heutzutage häufig in automatischen Verfahren zur Authentifikation/Verifikation und Identifikation eingesetzt, vor allem zur Kontrolle des Zugangs zu physischen und virtuellen Bereichen (d. h. zu bestimmten elektronischen Systemen oder Diensten).

Früher war der Einsatz der Biometrie in erster Linie auf DNA-Tests und die Überprüfung von Fingerabdrücken beschränkt. Die Erfassung von Fingerabdrücken wurde vor allem im Rahmen der Strafverfolgung (z. B. kriminalpolizeilichen Ermittlungen) verwendet. Wenn jedoch der Aufbau von Datenbanken mit Fingerabdrücken oder anderen biometrischen Daten für weitere Routineanwendungen Unterstützung in der Gesellschaft findet, steigt das Risiko, dass diese Daten von Dritten, u. a. den Strafverfolgungsbehörden, für Vergleiche und Recherchen zu ihren eigenen Zwecken verwendet werden, ohne dass dies ursprünglich beabsichtigt gewesen wäre.

Besonders Besorgnis erregend ist in diesem Zusammenhang, dass sich die Öffentlichkeit aufgrund der zunehmenden Verwendung biometrischer Daten immer weniger Gedanken

---

1 ABl. L 281 vom 23.11.95, S. 31, verfügbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

2 Seit dem 11. September wird die Biometrie häufig als geeignetes Mittel zur Verbesserung der öffentlichen Sicherheit dargestellt. In der Europäischen Union wird die Aufnahme biometrischer Daten in Personalausweise, Pässe und andere Reisedokumente sowie Visa diskutiert. Die USA werden in Kürze bei der Ein- und Ausreise von Ausländern eine obligatorische Überprüfung biometrischer Identifikatoren einführen. 2003 wurde durch eine Änderung des IAO-Übereinkommens 108 die Aufnahme biometrischer Daten in Ausweispapiere für Seeleute eingeführt. Ähnliche Diskussionen finden auch in anderen internationalen Foren wie z. B. G8 und OECD statt.

3 Allerdings hängt die eindeutige Identifizierung von verschiedenen Faktoren wie dem Umfang der Datenbank und der Art der verwendeten biometrischen Daten ab.

über die Auswirkungen der Verarbeitung dieser Daten auf das tägliche Leben macht. So kann die Verwendung biometrischer Daten in Schulbüchereien dazu führen, dass die Kinder für die datenschutzrelevanten Risiken, die sich u. U. erst in späteren Jahren auswirken, weniger sensibilisiert sind.

Das vorliegende Dokument soll zu einer wirksamen und einheitlichen Anwendung der gemäß Richtlinie 95/46/EG erlassenen nationalen Vorschriften auf biometrische Systeme beitragen. Es befasst sich in erster Linie mit Biometrieanwendungen für Authentifikations- und Verifikationszwecke. Die Arbeitsgruppe beabsichtigt, europaweit einheitliche Leitlinien zu entwickeln, die sich vor allem an die Hersteller biometrischer Systeme und ihre Nutzer wenden.

2. BESCHREIBUNG BIOMETRISCHER SYSTEME

Biometrische Systeme sind Anwendungen der Biometrie, die eine automatische Identifikation und/oder Authentifikation/Verifikation von Personen ermöglichen[4]. Authentifikations-/Verifikationsanwendungen werden häufig für verschiedene Aufgaben in völlig unterschiedlichen Bereichen und unter der Verantwortung der unterschiedlichsten Stellen eingesetzt.

Biometrische Daten, ob sie nun Authentifikations-/Verifikations- oder Identifikationszwecken dienen, zeichnen sich, wenn auch in unterschiedlichem Maße, durch folgende Eigenschaften aus. Sie sind:

- **universell**: das biometrische Merkmal ist bei jedem Menschen vorhanden;[5]
- **einzigartig**: das biometrische Merkmal muss einen Menschen eindeutig kennzeichnen;
- **dauerhaft**: das biometrische Merkmal bleibt bei jedem Menschen im Laufe der Zeit weitgehend unverändert.

Die biometrischen Verfahren lassen sich zwei Hauptkategorien zuordnen, je nachdem, ob sie dauerhafte physiologische Merkmale oder dynamische Verhaltensmerkmale[6] verwenden.

Die erste Gruppe sind die Verfahren, die die **physiologischen** Merkmale einer Person erfassen. Dazu zählen Verifikation von Fingerabdrücken und Finger-Bildanalyse, Iriserkennung, Netzhautanalyse, Gesichtserkennung, Handgeometrie, Erkennung der

---

[4] Die Unterscheidung zwischen Authentifikation (Verifikation) und Identifikation ist wichtig. Die Authentifikation beantwortet die Frage: Bin ich die Person, als die ich mich ausgebe? Das System verifiziert die Identität der Person durch die Verarbeitung biometrischer Daten des Fragestellers und trifft eine Ja/Nein-Entscheidung (1:1-Vergleich). Die Identifikation beantwortet die Frage: Wer bin ich? Das System erkennt den Fragesteller, indem es ihn von anderen Personen, deren biometrische Daten ebenfalls gespeichert sind, unterscheidet. In diesem Fall trifft das System eine 1:n-Entscheidung und bestätigt, dass der Fragesteller die Person X ist.

[5] In dieser Hinsicht sind nicht alle biometrischen Daten gleichwertig, und sie sind als Mittel zur Unterscheidung zwischen Einzelpersonen von sehr unterschiedlichem Nutzen, je nach Art der verwendeten biometrischen Kennzeichen. Die geeignetsten Unterscheidungsmerkmale scheinen DNA, Netzhaut und Fingerabdruck zu sein.

[6] Einige Verfahren stützen sich sowohl auf physiologische als auch auf verhaltenstypische Merkmale.

Ohrenform, Erfassung des Körpergeruchs, Sprecherverifikation, Analyse von DNA-Mustern[7], Analyse der Schweißporen usw.

Die zweite Gruppe sind die Verfahren, die die **Verhaltensmerkmale** einer Person erfassen. Dazu zählen Verifikation der Unterschrift, Analyse des Tastenanschlags, Analyse der Gangart usw.

Angesichts der rasanten technischen Entwicklung und der gestiegenen Sicherheitsanforderungen verbinden viele biometrische Systeme unterschiedliche biometrische Merkmale des Benutzers mit anderen Identifikations- oder Authentifikationstechniken. Manche Systeme kombinieren z. B. Gesichtserkennung und Stimmaufzeichnung. Um eine Person zu authentifizieren, können drei verschiedene Methoden miteinander kombiniert werden, die auf Wissen (PIN, Passwort), Besitz (Marke, CAD-Schlüssel, Smartcard) und persönlichem Merkmal (biometrisches Kennzeichen) beruhen. Beispielsweise könnte man an einem Computer eine Smartcard einführen, ein Passwort eingeben und seinen Fingerabdruck lesen lassen.

Die Erfassung biometrischer Daten (z. B. Bild des Fingerabdrucks, der Iris oder der Netzhaut, Stimmaufzeichnung) erfolgt in einer so genannten „Einlernphase“ mit Hilfe eines für das betreffende biometrische Merkmal spezifischen Sensors. Das biometrische System extrahiert aus den biometrischen Daten nutzerspezifische Merkmale, um ein biometrisches „Template” zu erstellen. Beim Template handelt es sich um eine strukturierte Reduzierung eines biometrischen Abbilds: die gespeicherten biometrischen Messungen eines Individuums. Gespeichert wird nicht das biometrische Merkmal selbst, sondern die digitalisierte Darstellung des Template. Je nach Funktionsweise des verwendeten biometrischen Systems können biometrische Daten auch als Rohdaten (Bild) verarbeitet werden[8].

Der Einlernphase kommt eine Schlüsselrolle zu, denn nur in dieser Phase sind gleichzeitig sowohl die Rohdaten, die Extraktions- und Schutzalgorithmen (Kryptographie, Hash-Funktionen usw.) als auch die Templates vorhanden. In diesem Zusammenhang ist Folgendes hervorzuheben: Wenn die Rohdaten Informationen enthalten, die als sensibel im Sinne von Artikel 8 Richtlinie 95/46/EG eingestuft werden könnten, sollte das „Einlernen“ der Daten gemäß dieser Bestimmung erfolgen (s. u. Punkt 3.7).

Ein weiterer, aus Datenschutzsicht überaus wichtiger Aspekt ist die Frage, wie die Benutzer-Templates gespeichert werden. Dies hängt von der Art der Anwendung ab, für die das Biometriegerät eingesetzt wird, sowie von der Größe der Templates. Folgende Formen der Speicherung von Templates stehen zur Wahl:

a) im internen Speicher eines Biometriegeräts;
b) in einer zentralen Datenbank;
c) auf Plastikkarten, optischen Karten oder Smartcards. Bei dieser Speichermethode tragen die Benutzer ihr Template als Ausweis bei sich.

---

[7] Die Verwendung der DNA zur biometrischen Identifikation wirft spezifische Fragen auf, die im vorliegenden Papier nicht erörtert werden sollen. An dieser Stelle sei nur erwähnt, dass die Erstellung eines DNA-Profils in Echtzeit als Mittel zur Authentifikation derzeit nicht möglich erscheint.

[8] Das vorliegende Papier befasst sich im Wesentlichen mit biometrischen Systemen, die mit „Templates“ arbeiten, ließe sich aber auch auf Systeme übertragen, die Rohdaten verarbeiten. Allerdings könnten aufgrund der Besonderheiten von Rohdaten Anpassungen der Datenschutzanforderungen erforderlich werden.

Grundsätzlich ist es für Authentifikations-/Verifikationszwecke nicht erforderlich, die Referenzdaten in einer Datenbank zu speichern; eine dezentrale Speicherung der personenbezogenen Daten reicht aus. Die Identifikation dagegen erfordert eine zentrale Speicherung der Referenzdaten, da das System zur Identitätsfeststellung die Templates oder Rohdaten (Bild) der betroffenen Person mit den Templates oder Rohdaten sämtlicher Personen vergleichen muss, deren Daten bereits in der zentralen Datenbank gespeichert sind.

Aus Datenschutzsicht überaus wichtig ist des Weiteren, dass sich manche biometrische Systeme auf Informationen wie Fingerabdrücke oder DNA-Muster stützen, die ohne Wissen der betroffenen Person erfasst werden können, da es sich um unwissentlich von ihr hinterlassene Spuren handelt. Durch Anwendung eines biometrischen Algorithmus auf den Fingerabdruck an einem Glas lässt sich unter Umständen herausfinden[9], ob die betreffende Person in einer Datenbank mit biometrischen Daten gespeichert ist, und falls ja, ist durch den anschließenden Vergleich der beiden Templates feststellbar, wer die Person ist. Entsprechendes gilt aufgrund der Besonderheiten der eingesetzten Technologie auch für andere biometrische Systeme, die z. B. auf der Analyse des Tastenanschlags oder Gesichtserkennung aus der Ferne beruhen[10]. Problematisch ist hierbei zum einen, dass die Erfassung und Verarbeitung dieser Daten unter Umständen ohne Wissen der betroffenen Person erfolgt, und zum anderen, dass ungeachtet ihrer derzeitigen Verlässlichkeit die Tendenz zu weit verbreitetem Einsatz dieser biometrischen Verfahren besteht, da sie „relativ wenig intrusiv“ sind. Aus diesem Grund erscheint es erforderlich, bei derartigen Verfahren besondere Garantien vorzusehen.

3. ANWENDUNG DER GRUNDSÄTZE DER RICHTLINIE 95/46/EG

3.1. Anwendung der Richtlinie 95/46/EG

Gemäß Artikel 2 Absatz a) Richtlinie 95/46/EG sind „personenbezogene Daten” „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (...); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, (...) Identität sind”. Erwägungsgrund 26 enthält hierzu folgende Erläuterung: „Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung *oder von einem Dritten* eingesetzt werden könnten, um die betreffende Person zu bestimmen”.

Nach dieser Definition sind Messungen biometrischer Kennzeichen oder ihre digitalisierte Darstellung in Form eines Template in den meisten Fällen personenbezogene Daten[11]. Biometrische Daten dürften stets als „Informationen über eine natürliche Person“

---

[9] Dies setzt allerdings zumindest Folgendes voraus: die Fähigkeit und die erforderlichen Mittel zur Abnahme des unversehrten Fingerabdrucks vom Glas, die technische Ausrüstung für die Verarbeitung der Daten des Fingerabdrucks und schließlich den Zugang zum Algorithmus des Datenbankentwicklers und/oder zur Fingerabdruck-Datenbank.

[10] Siehe Abschnitt 3 über die Anwendung der Richtlinie 95/46/EG, insbesondere Punkt 3.3 über die Pflicht zur Information der betroffenen Person.

[11] Biometrische Daten sollten dann nicht als personenbezogene Daten eingestuft werden, wenn sie wie ein Template so gespeichert werden, dass eine Identifizierung der betroffenen Person durch den Verantwortlichen für die Verarbeitung oder Dritte mit angemessenen Mitteln ausgeschlossen ist.

einzustufen sein, da sie naturgemäß Aufschluss über eine bestimmte Person geben. Bei der biometrischen Identifikation ist die betroffene Person generell bestimmbar, da die biometrischen Daten zur Identifikation oder Authentifikation/Verifikation zumindest in dem Sinne verwendet werden, dass die Person von jeder anderen unterschieden wird[12].

Gemäß Artikel 3 Absatz 1 Richtlinie 95/46/EG gelten die Datenschutzprinzipien für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Die Richtlinie findet keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. Hierzu sind zahlreiche Biometrieanwendungen des häuslichen Gebrauchs zu zählen.

Von diesen spezifischen Ausnahmen abgesehen kann die Verarbeitung biometrischer Daten nur dann als rechtmäßig betrachtet werden, wenn sämtliche damit verbundenen Verfahren ab der Einlernphase gemäß den Bestimmungen der Richtlinie 95/46/EG durchgeführt werden.

Das vorliegende Papier untersucht nicht sämtliche Fragen, die im Zusammenhang mit der Anwendung der Richtlinie 95/46/EG auf biometrische Daten aufgeworfen werden, sondern nur diejenigen, die am ehesten von Belang sind. Es ist daher nicht als erschöpfende Darstellung der Konsequenzen zu betrachten, die sich aus der Anwendung der Richtlinie ergeben.

3.2. Grundsatz der Zweckbestimmung und der Verhältnismäßigkeit

Laut Artikel 6 Richtlinie 95/46/EG müssen personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben werden und dürfen nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Darüber hinaus müssen personenbezogene Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und dürfen nicht darüber hinausgehen (Grundsatz der Zweckbestimmung).

Dieser Grundsatz setzt zunächst eine klare Bestimmung des Zwecks voraus, für den die biometrischen Daten erfasst und verarbeitet werden. Des Weiteren ist die Wahrung der Verhältnismäßigkeit und der Rechtmäßigkeit zu bewerten; dabei sind die Risiken für den Schutz der Grundrechte und -freiheiten des Einzelnen zu berücksichtigen, vor allem die Frage, ob der beabsichtigte Zweck nicht auch auf eine weniger in die Rechte der Betroffenen eingreifende Weise zu erreichen ist. Fast alle bisherigen Beschlüsse der Datenschutzbehörden zur Verarbeitung biometrischer Daten stellen vornehmlich auf das Kriterium der Verhältnismäßigkeit ab.[13]

Nach Ansicht der Datenschutzgruppe sind biometrische Systeme, die zur Zugangskontrolle (Authentifikation/Verifikation) eingesetzt werden, mit geringeren

---

[12] Die Bestimmbarkeit der Person hängt auch von der Verfügbarkeit anderer Daten ab, die für sich allein oder in Verbindung mit den biometrischen Daten eine Identifizierung der fraglichen Person erlauben. Die Möglichkeit einer „direkten Identifizierung“ durch Zuordnung zu „einem oder mehreren spezifischen Elementen“ wird in der Bestimmung des Begriffs „personenbezogene Daten“ in Artikel 2 Absatz a) Richtlinie 95/46/EG ausdrücklich erwähnt.

[13] Beispielsweise Beschlüsse der niederländischen, französischen, deutschen, italienischen und griechischen Behörden.

Gefahren für den Schutz der Grundrechte und -freiheiten des Einzelnen verbunden, wenn sie entweder auf Körpermerkmalen basieren, die keine Spuren hinterlassen (z. B. Form der Hand, aber keine Fingerabdrücke), oder wenn sie zwar Körpermerkmale verwenden, die Spuren hinterlassen, die Daten jedoch nicht auf einem Medium speichern, das sich nicht im Besitz der betroffenen Person befindet (mit anderen Worten, wenn die Daten nicht im Gerät, das den Zugang kontrolliert, oder in einer zentralen Datenbank gespeichert werden)[14]. Diese Ansicht wird von verschiedenen Datenschutzbehörden geteilt, denen zufolge die Anwendung des Grundsatzes der Verhältnismäßigkeit bedeutet, dass biometrische Merkmale möglichst nicht in einer Datenbank gespeichert werden sollten, sondern nur auf einem Medium, das ausschließlich dem Benutzer zugänglich ist (Chipkarte, Handy, Bankkarte usw.)[15]. Mit anderen Worten: Authentifikations-/Verifikationsanwendungen, die ohne zentrale Speicherung biometrischer Daten funktionsfähig sind, sollten auf unverhältnismäßige Identifikationsverfahren verzichten.

Daher sollte nach Meinung der Datenschutzgruppe der Einführung von Anwendungen, die auf der Speicherung von Templates digitaler Fingerabdrücke in einem Zugangsendgerät oder einer zentralen Datenbank basieren, eine sorgfältige Prüfung und Bewertung vorausgehen. Werden derartige Systeme dennoch z. B. in Hochsicherheitsanlagen[16] eingesetzt, sollte dies als Datenverarbeitung eingestuft werden, die Risiken im Sinne des Artikels 20 Richtlinie 95/46/EG birgt und daher einer Vorabkontrolle durch die Datenschutzbehörden gemäß den einzelstaatlichen Rechtsvorschriften unterliegt (s. u. Punkt 3.5).

Richtlinie 95/46/EG verbietet eine Weiterverarbeitung von Daten, die mit dem Zweck, zu dem sie erhoben wurden, unvereinbar ist. Wenn beispielsweise biometrische Daten, die zu Zugangskontrollzwecken verarbeitet werden, zur Überwachung am Arbeitsplatz genutzt werden oder um den Gemütszustand der betroffenen Person einzuschätzen, wäre dies nicht mit dem ursprünglichen Zweck zu vereinbaren. Die Wiederverwendung biometrischer Daten für Zwecke, die mit denen, für die sie erfasst und weiterverarbeitet wurden, unvereinbar sind, ist mit allen Mitteln zu vermeiden[17]. Richtlinie 95/46/EG sieht zwar Ausnahmen von dem Verbot einer mit der ursprünglichen Zweckbestimmung nicht zu vereinbarenden Weiterverarbeitung von Daten vor, allerdings nur unter spezifischen Bedingungen.

Es wird allgemein anerkannt, dass das Risiko einer Wiederverwendung biometrischer Daten, die unwissentlich hinterlassenen physischen Spuren entnommen wurden (z. B. Fingerabdrücke), für mit ihrer ursprünglichen Zweckbestimmung nicht zu vereinbarende Zwecke dann relativ gering ist, wenn die Daten nicht in zentralen Datenbanken

---

[14] Es wäre zu unterscheiden zwischen Systemen, bei denen biometrische Daten in einem zentralen System verarbeitet werden, und solchen, bei denen Referenzdaten auf einem mobilen Medium gespeichert werden und der Datenabgleich auf der Karte und nicht im Sensor erfolgt oder bei denen auch der Sensor Teil des mobilen Mediums ist.

[15] Die vorhandenen Mechanismen zur Lösung der Probleme, die sich aus dem Verlust, Diebstahl oder der Beschädigung von Karten ergeben, müssen überprüft und diejenigen, bei denen keine biometrischen Daten gespeichert werden, gefördert werden. Wo immer möglich, sollte eine neuerliche Erfassung der Daten direkt bei der betroffenen Person erfolgen.

[16] Nach dem gegenwärtigen Stand der Biometrie gibt es noch keine verlässlichen reinen Identifikationslösungen, die in Echtzeit die Daten eines Personenkreises realistischer Größe verarbeiten könnten, und in absehbarer Zukunft ist auch nicht damit zu rechnen.

[17] Wie bereits dargelegt, muss der Verwendungszweck klar bestimmt werden.

gespeichert werden, sondern bei der betroffenen Person verbleiben und für Dritte unzugänglich sind. Eine zentrale Speicherung biometrischer Daten erhöht das Risiko, dass die Daten als Schlüssel zur Verknüpfung verschiedener Datenbanken verwendet werden und auf diese Weise im öffentlichen wie im privaten Bereich detaillierte Gewohnheitsprofile der betroffenen Person erstellt werden können. Darüber hinaus berührt die Vereinbarkeit der Zwecke Fragen der Interoperabilität unterschiedlicher Biometriesysteme. Die Standardisierung, die zur Erreichung von Interoperabilität erforderlich ist, könnte zu einer verstärkten Datenbankvernetzung führen.

Der Einsatz der Biometrie wirft darüber hinaus die Frage auf, ob die einzelnen Kategorien verarbeiteter Daten in Bezug auf den Verarbeitungszweck verhältnismäßig sind. Biometrische Daten dürfen nur dann verwendet werden, wenn sie den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen. Dies setzt voraus, dass an die Notwendigkeit und die Verhältnismäßigkeit der verarbeiteten Daten strenge Maßstäbe angelegt werden[18]. Die französische Datenschutzbehörde CNIL hat beispielsweise die Verwendung des Fingerabdrucks für den Zugang von Kindern zu einer Schulkantine[19] abgelehnt, der Verwendung der Handgeometrie für diesen Zweck dagegen zugestimmt. Die portugiesische Datenschutzbehörde hat kürzlich über die Verwendung eines biometrischen Systems (Fingerabdruck), mit dem an einer Universität Arbeitsleistung und Pünktlichkeit der nicht zum Lehrpersonal gehörigen Beschäftigten kontrolliert werden sollten, negativ beschieden[20]. Die deutsche Datenschutzbehörde hat die Aufnahme biometrischer Merkmale in Ausweise, um diese fälschungssicher zu machen, positiv beurteilt, sofern die Daten für den Vergleich mit den Fingerabdrücken des Ausweisbesitzers auf dem Mikrochip der Ausweiskarte gespeichert werden und nicht in einer Datenbank.

Ein besonderes Problem kann sich daraus ergeben, dass biometrische Daten häufig mehr Informationen enthalten als für die Identifikations- oder Authentifikationsfunktionen benötigt werden. Dies ist bei Rohdaten (dem ursprünglichen Bild) mit größerer Wahrscheinlichkeit der Fall, da das Template technisch so gestaltet werden kann und sollte, dass die Verarbeitung überschüssiger Daten ausgeschlossen ist. Nicht benötigte Daten sollten zum frühest möglichen Zeitpunkt vernichtet werden[21]. Zu beachten ist ferner, dass manche biometrische Daten Aufschluss über die ethnische Herkunft geben oder die Gesundheit betreffen können (s. u. Punkt 3.7).

Abschließend sollte die Möglichkeit nicht unerwähnt bleiben, biometrische Systeme so zu gestalten, dass sie als datenschutzfördernde Technologie eingestuft werden können,

---

[18] Darüber hinaus muss Anonymität oder die Verwendung von Pseudonymen unter bestimmten Umständen weiterhin möglich sein. Die vorhandenen Mechanismen zur Lösung der Probleme, die sich aus dem Verlust, Diebstahl oder der Beschädigung von Karten ergeben, müssen überprüft und diejenigen, bei denen keine biometrischen Daten gespeichert werden, gefördert werden. Wo immer möglich, sollte eine neuerliche Erfassung der Daten direkt bei der betroffenen Person erfolgen.

[19] Allerdings scheint die britische Datenschutzbehörde der Verwendung von Fingerabdrücken für ähnliche Zwecke zugestimmt zu haben, sofern angemessene Sicherheitsvorkehrungen getroffen werden.

[20] Die portugiesische Datenschutzbehörde vertrat die Ansicht, die Anwendung eines solchen Systems sei angesichts des Verarbeitungszwecks unverhältnismäßig und gehe darüber hinaus. Das System hätte die Daten in einem Biometriegerät gespeichert, der zu kontrollierende Personenkreis umfasste etwa 140 Beschäftigte.

[21] Diese Forderung kann sich auf Artikel 6 Absatz 1 Buchstabe e) Richtlinie 95/46/EG stützen, dem zufolge personenbezogene Daten *nicht länger* aufbewahrt werden dürfen, als für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist.

u. U. weil sie dazu führen, dass andere personenbezogene Daten wie Name, Anschrift, Wohnort usw. in geringerem Umfang verarbeitet werden.

3.3. Datenerhebung nach Treu und Glauben und Information der betroffenen Person

Die Verarbeitung und insbesondere die Erhebung biometrischer Daten sollte nach Treu und Glauben erfolgen[22]. Der für die Verarbeitung Verantwortliche sollte die betroffene Person im Einklang mit Artikel 10 und 11 Richtlinie 95/46/EG informieren[23]. Dies schließt vor allem die Angabe der genauen Zweckbestimmung und der Identität des für die Verarbeitung Verantwortlichen ein (häufig der Betreiber des biometrischen Systems oder der Anwender des biometrischen Verfahrens).

Systeme, die biometrische Daten ohne Wissen der betroffenen Personen erheben, sind zu vermeiden. Ein besonderes Risiko stellen hier biometrische Systeme dar, die etwa mit Gesichtserkennung aus der Ferne, Erfassung von Fingerabdrücken oder heimlicher Stimmaufzeichnung arbeiten.

3.4. Kriterien für eine rechtmäßige Datenverarbeitung

Die Verarbeitung biometrischer Daten ist nur dann als rechtmäßig anzusehen, wenn eine der in Artikel 7 Richtlinie 95/46/EG genannten Voraussetzungen erfüllt ist. In den Fällen, in denen sich der für die Verarbeitung Verantwortliche auf die Einwilligung der betroffenen Person stützt, muss die Einwilligung nach Auffassung der Datenschutzgruppe der in Artikel 2 der Richtlinie enthaltenen Definition entsprechen (der zufolge als Einwilligung jede Willensbekundung gilt, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden).

3.5. Vorabkontrolle – Meldung

Wie bereits dargelegt, unterstützt die Datenschutzgruppe die Verwendung biometrischer Systeme, die biometrische Spuren weder in einem Zugangsendgerät noch in einer zentralen Datenbank speichern (siehe Punkt 3.2). In Fällen, in denen gleichwohl der Einsatz von Systemen beabsichtigt ist, die mit der Speicherung von Daten in einem Zugangsendgerät oder einer zentralen Datenbank verbunden sind, empfiehlt die Arbeitsgruppe angesichts des Risikos einer zweckentfremdeten (Wieder-)Verwendung und der besonderen Gefahren bei unbefugtem Zugriff, dass die Mitgliedstaaten die Möglichkeit prüfen, sie einer Vorabkontrolle durch die Datenschutzbehörden gemäß Artikel 20 Richtlinie 95/46/EG zu unterwerfen, da diese Verarbeitung spezifische Risiken für die Rechte und Freiheiten der Betroffenen birgt. Beabsichtigen die Mitgliedstaaten die Einführung einer Vorabkontrolle im Zusammenhang mit der Verarbeitung biometrischer Daten, sollten die nationalen Datenschutzbehörden ordnungsgemäß konsultiert werden, ehe derartige Maßnahmen ergriffen werden.

---

22 Siehe Artikel 6 Absatz 1 Buchstabe a) Richtlinie 95/46/EG.

23 Ausnahmen von der Pflicht zur Information der betroffenen Person gemäß Artikel 10 und 11 Richtlinie 95/46/EG sollten auf Rechtsvorschriften gestützt sein und die Beschränkung der Informationspflicht sollte eine Maßnahme darstellen, die zum Schutz der in Artikel 13 der Richtlinie aufgeführten Interessen (Sicherheit des Staates; Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten usw.) notwendig ist.

3.6. Sicherheitsmaßnahmen

Der für die Verarbeitung Verantwortliche muss gemäß Artikel 17 Richtlinie 95/46/EG die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen durchführen, die für den Schutz personenbezogener Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang erforderlich sind, insbesondere wenn im Rahmen der Verarbeitung biometrische Daten in einem Netz übertragen werden. Sicherheitsmaßnahmen sind bei der Verarbeitung biometrischer Daten (Speicherung, Übertragung, Extraktion von Merkmalen, Vergleich usw.) insbesondere dann durchzuführen, wenn der für die Verarbeitung Verantwortliche die Daten über das Internet überträgt. Denkbare Sicherheitsmaßnahmen sind u. a. die Verschlüsselung der Templates und der Schutz der Kryptografieschlüssel zusätzlich zu Zugangskontrolle und Schutzvorkehrungen, die eine Wiederherstellung der ursprünglichen Daten aus den Templates unmöglich machen.

In diesem Zusammenhang sollten einige neue Technologien berücksichtigt werden. Eine interessante Entwicklung ist die Möglichkeit, biometrische Daten als Kryptografieschlüssel zu verwenden. Dies wäre von vornherein mit geringeren Risiken für die betroffene Person verbunden, da ein solcher Schlüssel nur auf Grundlage neuerlicher Erfassung der biometrischen Daten bei der betroffenen Person selbst entschlüsselt werden könnte. Damit würde das Anlegen von Datenbanken mit den Templates biometrischer Daten, die möglicherweise zu anderen Zwecken wieder verwendet werden, vermieden.

Die erforderlichen Sicherheitsmaßnahmen sollten bereits ab Beginn der Verarbeitung ergriffen werden, insbesondere in der „Einlernphase“, in der die biometrischen Daten in Templates oder Bilder umgewandelt werden. Jede Verletzung der Integrität, Vertraulichkeit und Verfügbarkeit der Datenbanken würde zweifellos nicht nur sämtliche künftigen Anwendungen beeinträchtigen, die auf den in den Datenbanken enthaltenen Informationen beruhen, sondern auch den betroffenen Personen nicht wiedergutzumachenden Schaden zufügen. Werden beispielsweise die Fingerabdrücke einer berechtigten Person mit der Identität einer unbefugten Person verknüpft, könnte Letztere die Dienstleistungen, zu denen die berechtigte Person Zugang hat, in Anspruch nehmen, ohne dazu berechtigt zu sein. Dies eröffnet die Möglichkeit des Identitätsraubes, mit der Folge, dass die Fingerabdrücke der betroffenen Person unabhängig davon, ob der Diebstahl entdeckt wird oder nicht, als verlässliches Merkmal für künftige Anwendungen nicht mehr in Frage kommen und somit die Freiheitsrechte dieser Person beschränkt werden.

In biometrischen Systemen auftretende Fehler können schwerwiegende Konsequenzen für den Einzelnen haben. Insbesondere die fälschliche Zurückweisung berechtigter Personen und die fälschliche Akzeptierung nicht berechtigter Personen können auf den verschiedensten Ebenen ernsthafte Probleme verursachen. Die Verwendung biometrischer Daten sollte das Risiko derartiger Fehler von vornherein mindern. Allerdings könnte dabei auch die Illusion einer stets fehlerfreien Identifikation bzw. Authentifikation/Verifikation entstehen. Für die betroffene Person könnte es sich als schwierig oder gar unmöglich erweisen, das Vorliegen eines Fehlers nachzuweisen. So könnte ein System beispielsweise eine Person fälschlich als jemanden identifizieren, dem die Benutzung eines Flugzeugs oder die Einreise in ein bestimmtes Land zu verweigern ist. Angesichts „unstrittiger“, gegen sie sprechender Beweise wäre die betroffene Person

kaum zur Aufklärung des Irrtums in der Lage. Auch an dieser Stelle ist noch einmal zu betonen, dass gemäß Artikel 15 Richtlinie 95/46/EG jede Entscheidung, die rechtliche Folgen für den Einzelnen nach sich zieht, erst nach Bestätigung des Ergebnisses der automatisierten Verarbeitung getroffen werden sollte.

Abschließend sollte nicht unerwähnt bleiben, dass der Einsatz der Biometrie die Verfahren z. B. zur Kontrolle des Zugangs zu Daten Dritter und zum Schutz vor Diebstahl und Missbrauch (Autorisierungsverfahren) verbessern könnte.

3.7. Sensible Daten

Einige biometrische Daten könnten als sensibel im Sinne des Artikels 8 Richtlinie 95/46/EG eingestuft werden, vor allem Gesundheitsdaten oder Daten, aus denen die rassische oder ethnische Herkunft hervorgeht. So werden beispielsweise in biometrischen Systemen, die auf der Gesichtserkennung basieren, unter Umständen Daten verarbeitet, die Rückschlüsse auf die rassische oder ethnische Herkunft ermöglichen. In solchen Fällen gelten zusätzlich zu den allgemeinen Schutzprinzipien der Richtlinie die in Artikel 8 vorgesehenen besonderen Garantien.

Dies bedeutet nicht, dass es sich bei biometrischen Daten grundsätzlich um sensible Daten handelt. Für die Einschätzung, ob eine Verarbeitung sensible Daten berührt, ist zum einen zu berücksichtigen, welches spezifische biometrische Merkmal verwendet wird, zum anderen ist die Anwendung selbst zu betrachten. Eine Verarbeitung sensibler Daten dürfte mit größerer Wahrscheinlichkeit dann vorliegen, wenn die biometrischen Daten in Bildform verarbeitet werden, da das Template im Prinzip keine Rückschlüsse auf die Rohdaten zulässt.

3.8. Eindeutiges Kennzeichen

Biometrische Daten sind einzigartig, und mit den meisten lässt sich ein eindeutiges Template (oder Bild) erzeugen. Im Falle einer weit verbreiteten Verwendung, insbesondere wenn diese einen erheblichen Teil der Bevölkerung betrifft, könnten biometrische Daten als Kennzeichen allgemeiner Bedeutung im Sinne der Richtlinie 95/46/EG angesehen werden. In diesem Fall wäre Artikel 8 Absatz 7 der Richtlinie anzuwenden, und die Mitgliedstaaten müssten die Bedingungen für die Verarbeitung dieser Daten bestimmen.

Sollen biometrische Daten als Schlüssel zur Verknüpfung von Datenbanken mit personenbezogenen Daten dienen[24], kann dies besonders schwierige Probleme aufwerfen, wenn die betroffene Person keine Möglichkeit hat, der Verarbeitung biometrischer Daten zu widersprechen. Dieser Fall dürfte besonders häufig im Rahmen der Beziehungen zwischen Bürgern und staatlichen Behörden eintreten.

Im Hinblick darauf wäre es wünschenswert, die Templates und ihre digitalen Darstellungen mit mathematischen Operationen (Verschlüsselung, Algorithmen oder Hash-Funktionen) zu verarbeiten und dabei für jedes biometrische Produkt unterschiedliche Parameter zu verwenden, um zu vermeiden, dass personenbezogene

[24] Siehe oben Punkt 3.2 zur mit den ursprünglichen Zwecken zu vereinbarenden Wiederverwendung.

Daten aus verschiedenen Datenbanken durch einen Vergleich der Templates oder ihrer digitalen Darstellungen miteinander verknüpft werden können.

3.9. Verhaltensregeln und Verwendung datenschutzfördernder Technologie

Die Datenschutzgruppe fordert die Industrie zur Herstellung biometrischer Systeme auf, die die Umsetzung der in diesem Arbeitspapier enthaltenen Empfehlungen erleichtern. Wenn europäische oder internationale Standards in diesem Bereich entwickelt werden, sollte dies in Abstimmung mit den Datenschutzbehörden geschehen, um biometrische Systeme zu fördern, die datenschutzfreundlich gestaltet sind, die gesellschaftlichen Risiken minimieren und dem Missbrauch biometrischer Daten vorbeugen. Die Datenschutzgruppe unterstreicht in diesem Zusammenhang die Bedeutung datenschutzfördernder Technologie (Privacy Enhancing Technology, PET) für eine möglichst sparsame Datenerhebung und zur Verhütung unrechtmäßiger Verarbeitung.

Des Weiteren hebt die Datenschutzgruppe die Bedeutung von Verhaltensregeln hervor, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Umsetzung der Datenschutzprinzipien beitragen sollen (siehe Artikel 27 Richtlinie 95/46/EG). Gemeinschaftliche Verhaltensregeln können der Datenschutzgruppe unterbreitet werden, die insbesondere dazu Stellung nimmt, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung der Richtlinie 95/46/EG erlassenen einzelstaatlichen Vorschriften im Einklang stehen.

SCHLUSSFOLGERUNGEN

Nach Auffassung der Datenschutzgruppe sind die meisten biometrischen Systeme mit der Verarbeitung personenbezogener Daten verbunden. Bei der Entwicklung derartiger Systeme sind daher die in Richtlinie 95/46/EG niedergelegten Grundsätze des Datenschutzes in vollem Umfang zu beachten. Gleichzeitig ist dem besonderen Charakter der Biometrie Rechnung zu tragen, der sich unter anderem aus der Möglichkeit ergibt, biometrische Daten ohne Wissen der betroffenen Person zu erfassen, sowie aus der Tatsache, dass sich nahezu mit Gewissheit eine Verbindung zu dem betreffenden Individuum herstellen lässt.

Beachtung des Grundsatzes der Verhältnismäßigkeit – Kern des durch Richtlinie 95/46/EG gewährleisteten Schutzes – bedeutet, vor allem im Zusammenhang mit Authentifikations-/Verifikationsverfahren, denjenigen biometrischen Anwendungen eindeutig den Vorzug zu geben, die keinerlei Daten verarbeiten, die unwissentlich hinterlassenen physischen Spuren entnommen wurden, bzw. Anwendungen, bei denen die Daten nicht in einem zentralen System gespeichert werden. Auf diese Weise erhält die betroffene Person stärkere Kontrolle darüber, welche ihrer personenbezogenen Daten verarbeitet werden.

Die Datenschutzgruppe beabsichtigt, dieses Arbeitspapier im Lichte der von den Datenschutzbehörden gemachten Erfahrungen und der technischen Entwicklungen auf dem Gebiet der biometrischen Anwendungen zu überarbeiten. Biometrische Daten finden bereits in einer Vielzahl verschiedener Bereiche und zu den unterschiedlichsten Zwecken Verwendung. Daher müssen unverzüglich Maßnahmen ergriffen werden, insbesondere in den Bereichen Beschäftigung, Visa, Einwanderung und Reisesicherheit.

Auch wenn die Entwicklung mit dem Datenschutz zu vereinbarender biometrischer Systeme Sache der Industrie bleibt, wäre ein Dialog mit allen interessierten Kreisen einschließlich der Datenschutzbehörden in jeder Hinsicht von großem Nutzen, insbesondere dann, wenn er sich auf den Entwurf eines Verhaltenskodex stützen kann.

Brüssel, den 13. Juni 2003

Für die Gruppe

Der Vorsitzende

Stefano RODOTÀ