BIOMETRISCHE IDENTIFIKATIONSVERFAHREN

Rechtliche Bestimmungen & Datenschutzanforderungen

Gordon Kunkel

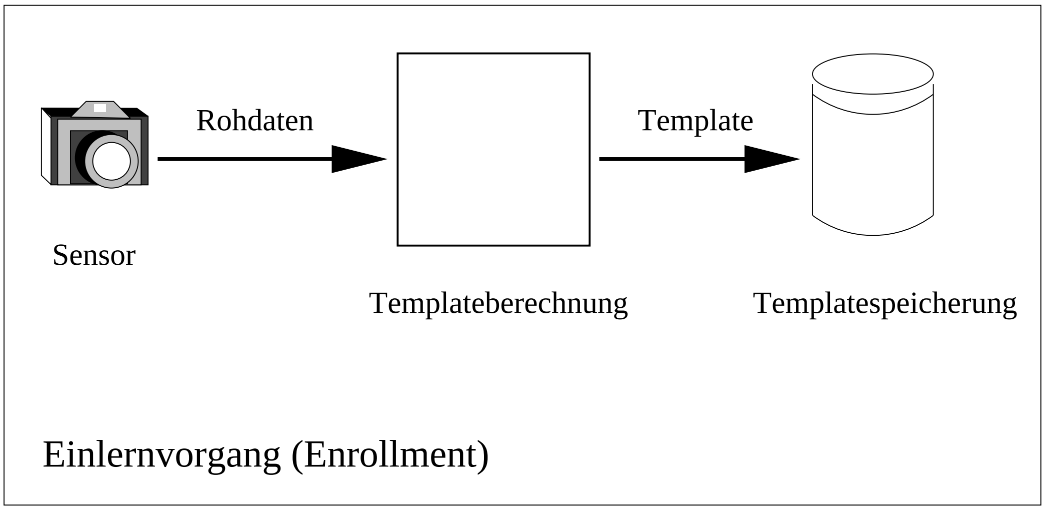
31. Dezember 2004

Inhaltsverzeichnis

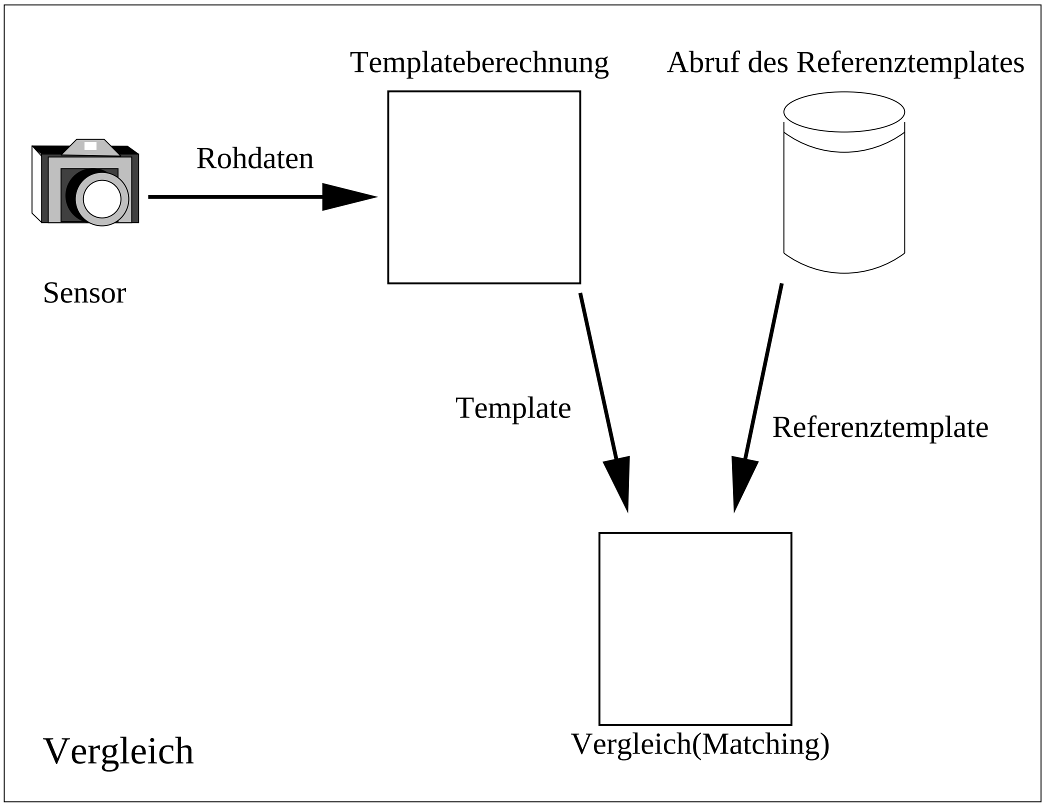
1 Grundsätzliches zu biometrischen Daten

1.1 Art der Daten

Mit Hilfe von Sensoren, die unterschiedlich sensibel reagieren, werden zunächst biometrische Rohdaten erfasst. Es gibt statische Verfahren die physiologische Merkmale und dynamische Verfahren, die verhaltensbasierende Merkmale in Rohdaten abbilden. Zu den physiologischen Merkmalen zählen Gesicht- Hand- Ohrmuschelform, der Fingerabdruck, das Handvenenmuster, das Iris- oder Retinamuster und der Geruch. Zu den verhaltensbasierenden (behaviorale) Merkmalen, die durch Verhalten oder Aktion gezeichnet sind, gehören die Stimme, die Lippenbewegung, die Schriftdynamik, der Tipprhythmus und die Gangdynamik.
Aus den Rohdaten entstehen nach Weiterverarbeitung Templates, die üblicherweise keine Rückschlüsse auf die beschriebenen Rohdaten einer Person erlauben.
Das Template wird bei der erstmaligen Benutzung eines Gerätes (Einlernvorgang ; Enrollment) als Referenzdatum gespeichert.



Bei der weiteren Verwendung des Gerätes werden wiederum Rohdaten erfasst und mit dem gleichen Algorithmus wie vorher ein Template berechnet. Ein Vergleichsalgorithmus überprüft, ob dieses Template mit dem abgespeicherten Referenzdatum übereinstimmt. Trifft dies zu, werden die Rohdaten als gleichartig erkannt, was zu einer positiven Rückmeldung führt.



Für den Vergleich gibt es zwei grundsätzliche Betriebsarten. Zum einen die Verifikation und zum anderen die Identifikation. Bei der Verifikation wird ein 1:1 Vergleich durchgeführt, bei der die behauptete Identität nachgewiesen wird.
Die Identifikation vergleicht das Template eines Benutzers mit allen gespeicherten Templates. Es wird ein 1:n Vergleich durchgeführt. Man findet dieses häufig bei forensischen Anwendungen (z.B. AFIS[1]), und auch bei Zugangskontrollverfahren, die auf Eingabe einer Nutzerkennung verzichten.

Zusammenfassend werden folgende Daten verwendet und gespeichert:

- biometrische Rohdaten
- Template
- Rohdaten und Template
- Klartext-Chiffrat-Paare : Templatefreie Verfahren [2]

[1]Automatisches Fingerabdruck-Identifizierungssystem
[2]http://www.cifro.com/produkt.html – 11.12.2004

Zu den templatefreien Verfahren möchte ich hier einige kurze Erläuterungen geben, da sie in den anderen Vorträgen nicht oder kaum behandelt wurden. Man konstruiert aus einem biometrischen Merkmal einen kryptographischen Schlüssel. Mit ihm wird nun ein zufälliger Klartext verschlüsselt. Gespeichert werden der Klartext sowie sein Chiffrat, nicht aber der Schlüssel. Bei einer erneuten Autorisierung erzeugt man nun wieder einen biometrischen Schlüssel, verschlüsselt den abgespeicherten Klartext. Das entstandene Chiffrat vergleicht man mit dem abgespeicherten Referenzchiffrat. Die Übereinstimmung beweist die Korrektheit des biometrischen Schlüssels und somit die Authentizität der Person. Aus dem Klartext-Chiffrat-Paar ist bei der Verwendung von geeigneten kryptographischen Verfahren kein Rückschluß auf die biometrischen Rohdaten möglich.

1.1.1 Personenbezogene Daten

Lassen sich Informationen einer bestimmten natürlichen Person zuordnen, spricht man von personenbezogenen Daten. Personenbezogene biometrische Daten sind im allgemeinen lebenslang an die Person gebunden und lassen sich nicht wie beispielsweise Namen, Adressen oder Passwörter ändern. Es finden lediglich alterungsbedingte Änderungen statt, die aber durch entsprechende Verfahren ausgeglichen werden können, um eine korrekte Authentifizierung zu gewährleisten.
Dieses Problem der lebenslangen Zuordnung von Daten läßt sich durch anonyme und pseudonyme Biometrie begegnen.
Das staatliche Erheben, Verarbeiten und Nutzen von personenbezogenen Daten stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Eingriffe sind nur dann zulässig, wenn eine gesetzliche Grundlage als verfassungsmäßige Rechtfertigung des Eingriffs vorliegt. Für private Stellen besteht keine unmittelbare Relevanz. Hier stehen den Betroffenen zivilrechtliche Abwehransprüche zur Verfügung. Der Einsatz biometrischer Verfahren kann noch weitere Grundrechtseingriffe mit sich bringen. Dies wird in Abschnitt 1.2 noch näher erläutert.

Aus Rohdaten können weitere Informationen über Personen gewonnen werden, die nicht zur Identifizierung verwendet werden, also Daten mit einem sogenannten überschießenden Informationsgehalt. Folgende Zuordnungen werden gemacht, obwohl die Verfahren zum Teil nicht wissenschaftlich gesichert sind:

Rohdaten	Folgerung
Gesicht und Sprache	Geschlecht, Alter, ethnische Herkunft
Augenhintergrund	Arteriosklerose, Diabetes
Fingerabdruck	chronische Magen-Darm-Beschwerden, Leukämie, Brustkrebs

Rückschlüsse aus dem Template ohne Detailkenntnisse des Konstruktionsprinzips sind sehr schwierig.
Die EG-Datenschutzrichtlinie schützt sensible personenbezogene Daten wie rassische und ethnische Herkunft, Gesundheit und Sexualleben. Dies gilt nicht für Daten, die durch die Person bereits öffenlich gemacht worden sind.

Biometrie kann aber auch zur Erhöhung des Datenschutzes führen, in dem personenbezogene Daten mit Hilfe von „biometrischen“ Passwörtern geschützt werden.

1.2 Gewinnung von Daten

1.2.1 Menschenwürdegarantie

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(Art. 1 Abs. 1 GG)

Die in Artikel 1 Absatz 1 des Grundgesetzes garantierte Menschenwürde stellt den höchsten Rechtswert innerhalb der verfassungsmäßigen Ordnung dar. Sie ist die Basis des allgemeinen Persönlichkeitsrechts, auf das später noch näher eingegangen wird, und der anderen Grundrechte.

Es gibt keine verfassungsrechtliche Legitimation für die Einschränkung der Menschenwürde. Das unterscheidet sie von den anderen Grundrechten des Grundgesetzes, die sehr wohl durch andere Gesetze beschränkt werden können. Wird ein Verstoß gegen die Menschenwürde festgestellt, so folgt daraus unabweislich ihre rechtliche Unzulässigkeit.

Was genau ist denn nun die Menschenwürde?
Wann liegt eine Verletzung derselben vor?

Im Allgemeinen wird dies mit der sogenannten Objektformel festgestellt. Wird der Mensch zum Objekt, zu einem bloßen Mittel, zu einer vertretbaren Größe herabgewürdigt, dann ist die Menschenwürde betroffen. Diese Darstellung ist naturgemäß kein präzises Instrument, um Verstöße gegen die Würde des Menschens zu ermitteln. Sie zeigt allerdings die Richtung an, in der Fälle der Verletzung der Menschenwürde zu finden sind.

Die Besonderheit in der Datenerhebung liegt darin, in welcher Weise individuelle oder/und natürlich-kreatürliche Verhaltensformen als Informationsquellen genutzt werden.

Der zwangsweise Einsatz des Lügendetektors als technisches Hilfsmittel zur Gewinnung und Messung von physiologischen Daten eines Menschen wird in der Literatur als Verstoß gegen die Menschenwürde angesehen. Bewertung und Beobachtung durch andere Menschen, zum Beispiel durch das Gericht, entsprechen einer normalen kommunikativen Situation, die als solche erkennbar ist. Bei dem Dazwischenschalten einer Maschine, dem Lügendetektor beispielsweise, tritt eine einseitige Abnahme von physiologischen Reaktionsmustern auf. Der Getestete wird somit von einer normalen Kommunikation ausgeschlossen, vom Subjekt zum Objekt degradiert, was unmittelbar eine Verletzung der Menschenwürde darstellt.

Die meisten heute im Einsatz befindlichen biometrischen Verfahren werden lediglich eingesetzt, um ein Individuum zu re-identifizieren. Sie berühren nicht den Kernbereich menschlicher Existenz. Solange biometrische Verfahren nur zum Zwecke der (Wieder-)Erkennung von Personen eingesetzt werden scheidet ein Verstoß gegen die Menschenwürde aus. Werden darüber hinausgehende Informationen gewonnen, rückt ein Würdeverstoß in greifbare Nähe.

Die Erhebung und Verarbeitung eines isolierten biometrischen Merkmales stellt keinen Würdeverstoß dar. Eine Bestandsaufnahme von Daten über eine Person, um diese in ihrer gesamten Persönlichkeit zu registrieren und zu katalogisieren, verletzt hingegnen die Würde des Menschen. Das Bundesverfassungsgericht sieht vielmehr sogar schon eine Gefahr für die Menschenwürde in der möglichen Verknüpfung unterschiedlicher Datenbestände. Die fortschreitende Standardisierung von biometrischen Verfahren erleichtert die übergreifende Profilbildung. Aus diesem Grund kann es geboten sein, in verschiedenen staatlichen Verfahren mit unterschiedlichen biometrischen Merkmalen zu arbeiten oder durch andere technische Vorkehrungen diese Gefahr zu verringern bzw. zu beseitigen.

Bisher wurden ausschließlich Ausführungen zum hoheitlich-staatlichen Einsatz biometrischer Verfahren erläutert. Die Menschenwürdegarantie entfaltet unmittelbare Drittwirkung und gilt damit auch im privaten Bereich. Der Staat hat sogar die ausführliche Pflicht nach Artikel 1 Absatz 1 Satz 2 des Grundgesetzes (siehe 5.1, S. 16), die Grundrechtsträger vor drohenden Würdeverletzungen durch Private zu schützen und bereits stattfindende Verletzungen zu unterbinden.

Biometrische Verfahren, die einen Verstoß der Menschenwürde beinhalten, sind sowohl den staatlichen Stellen als auch den privaten Bereichen verboten. Der Staat wäre verpflichtet einzuschreiten, um den verfassungswidrigen Zustand zu beenden.

1.2.2 Persönlichkeitsrecht

Als ein weiterer Prüfungsmaßstab staatlicher Eingriffe wird häufig das allgemeine Persönlichkeitsrecht herangezogen.

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(Art. 2 Abs. 1 GG)

Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

(Art. 2 Abs. 2 GG)

Das Persönlichkeitsrecht ist somit das Recht des einzelnen auf Unantastbarkeit seiner Menschenwürde und auf Achtung seiner individuellen Persönlichkeit. Dies ist durch den Artikel 1 und 2 des Grundgesetzes verfassungsmäßig gewährleistet. Das Persönlichkeitsrecht umfaßt das Recht auf freie Entfaltung der Persönlichkeit, auf Achtung der Ehre, der Privatsphäre, des Namens und das Recht am eigenen Bild und Wort. Es können also die biometrischen Verfahren der Gesichtserkennung oder der Spracherkennung betroffen sein.

Schwere Ehrenverletzung führt nach der Rechtsprechung des BGH[3] zu Schadensersatz in Geld. Aus dem Persönlichkeitsrecht wird auch das Recht auf informationelle Selbstbestimmung hergeleitet. Dieses ist ein grundgesetzlich geschütztes Persönlichkeitsrecht, wonach jeder grundsätzlich selbst über Preisgabe oder Verwendung seiner persönlichen Daten bestimmt.

Aus diesem Grund bedürfte der staatlich angeordnete Einsatz biometrischer Verfahren einer besonderen parlamentsgesetzlichen Rechtsgrundlage. Diese müßte den spezifisch biometrischen Eingriff abdecken.
Die (Weiter-)Verarbeitung personenbezogener Daten sind schon durch das Bundesdatenschutzgesetz (BDSG 14.01.2003) erfaßt. Im Hinblick auf das europäische Gesetz ist eine besondere Rechtsgrundlage erforderlich.

[3]BGH – Bundesgerichtshof

Die verdeckte Aufnahme von Rohdaten widerspricht dem in den Datenschutzgesetzen festgeschriebenen „Grundsatz der offenen Datenerhebung“ beim Betroffenen (§ 4, § 4a BDSG - siehe S. 17ff)

Abweichende Regelungen für öffentliche Stellen finden sich im § 13 und § 14 des BGSD (siehe S. 18ff) . Verdeckte Erhebungen kommen zum Beispiel bei folgenden Fällen in Betracht:

- Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit
- Verfolgung von Straftaten und Ordungswidrigkeiten
- Arbeitsrechtlichen Rechtsverhältnissen

Für nicht-öffentliche Stellen ist § 28, 29 BGSD anzuwenden. Voraussetzung zur weiteren Verarbeitung von Daten ist, daß diese nach Treu und Glauben auf rechtmäßige Weise erhoben wurden. (§ 28 Abs. 1 Satz 2 – S. 21, § 29 Abs. 1 Satz 2 BDSG – S. 25)
Die verdeckte Erhebung biometrischer Rohdaten ist ein Verstoß gegen Treu und Glauben, die Weiterverarbeitung dieser Daten ist ebenfalls nach geltendem Recht nicht zulässig.

1.3 Technische Sicherheit und Zuverlässigkeit

Aufgenommene Rohdaten von einer Person, gleichen sich niemals eindeutig, da sie oft mit Meßfehlern behaftet sind, oder sich im Laufe der Zeit verändern. Eine Veränderung kann zum Beispiel hervorgerufen werden durch den einsetzenden Stimmbruch, eine Frisuränderung oder aber auch eine Verletzung am Finger. Durch diese Veränderung sind auch die entsprechenden Templates nicht mehr gleich und müssen bei einem Vergleich (Matching) berücksichtigt werden. Ab welchem Übereinstimmungsgrad eine positive Identifikation gemeldet werden soll, kann mit Hilfe eines Parameters eingestellt werden.

Weiterhin können absichtliche und unabsichtliche Bedienungsfehler oder eine ungeschickte Ausgestaltung des Systems dazu führen, daß die biometrischen Merkmale nicht völlständig erhoben werden. Der fragmentarische Fingerabdruck, Teilaufnahmen des Gesichtes, unvollständige Sprachaufnahmen können hier als Beispiele genannt werden. Eine automatische Qualitätskontrolle, die zur nochmaligen Eingabe der Daten auffordert, könnte hier Abhilfe schaffen. Jedoch besitzt diese nicht jedes Gerät. Letztendlich hängt das Ergebnis des Vergleichs ganz empfindlich von dem Parameter ab, der den Übereinstimmungsgrad beeinflußt.

Bei der Verwendung biometrischer Verfahren stellt die Überwindungssicherheit einen weiteren Aspekt dar, der im Hinblick auf die technische Sicherheit und Zuverlässigkeit eines Gerätes genannt werden muss.

Das Ziel ist es, ein Gerät gegen gefälschte biometrische Merkmale immun zu machen. Darunter fallen zum einen die natürlichen Fälschungen, wie Frisuränderungen, Aussehensveränderungen, Stimmverstellungen und Unterschriftsnachahmungen, und zum anderen künstliche Fälschungen. Zu den Artefakten zählen zum Beispiel Fotos für Gesichtserkennungssysteme, Tonbandaufnahmen, Silikonabgüsse von Fingerabdrücken, Kontaktlinsen mit fremdem Irismuster und Tipp- oder Schreibautomaten um Tipprhythmuserkennungssysteme zu umgehen.

Einige Geräte beinhalten bereits Lebenderkennungssysteme, um diesem Problem entgehen zu können. Beispielsweise durch die Messung der Leitfähigkeit der Haut oder des Pulses bei Fingerabdrucksystemen kann Abhilfe, mehr Zuverlässigkeit und Sicherheit geschaffen werden.

Ein weiterer Aspekt, der hierbei nicht unbeachtet bleiben darf, ist die Erkennungsgüte. Dies schließt Fehlerraten, aber auch die Robustheit der Geräte gegen äußere Einflüsse, die Haltbarkeit der technischen Komponenten usw. ein. Fingerabdrucksensoren, die nach einiger Zeit der Benutzung ausgetauscht werden müssen, werden hierbei in der Literatur genannt.

2 Szenarien

2.1 Öffentlicher Bereich

2.1.1 Pass- und Personalausweiswesen

In diesem Bereich kann der Einsatz biometrischer Daten zum einen die bereits bekannten Angaben über die Person ergänzen, zum anderen können sie verwendet werden, um den Ausweisinhaber bei der Ausweisausstellung zu identifizieren und um eine Ausstellung von mehreren Ausweisen unter verschiedenen Namen zu unterbinden.
Eine Idee, bereits bekannte Daten durch biometrische Daten zu ergänzen und diese elektronisch zu speichern, ist beispielsweise durch sogenannte Identitätskarten in Form von Chipkarten erfüllbar. Bei einer möglichen Identitätskontrolle werden so biometrische Daten der kontrollierenden Person erfaßt und mit dem Template auf der Karte verglichen.

Biometrische Merkmale sollen also im Bereich der Ausweiserstellung Erleichterung schaffen. Üblicherweise wird bei einer Ausstellung von Personaldokumenten und Führerscheinen die Identität mit Hilfe von bereits ausgestellten Ausweisen sowie weiteren Papieren (z.B. Geburtsurkunde) überprüft. Die biometrischen Daten eines Antragsstellers für eine biometrische Überprüfung zu erfassen und diese mit einer Datenbank abzugleichen stellt eine Erleichterung und eine höhere Sicherheit für staatliche und private Bereiche dar.

2.1.2 Strafverfolgung

Für die Strafverfolgung bzw. für den Strafvollzug finden weitere Gesetze Anwendung. Regelungen dazu findet man im § 14 Absatz 2, Nummer 7 des BDSG und § 28 Absatz 3, Nummer 2 BDSG-E:
§ 14 Absatz 2, Nr. 7 des BDSG: *Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1, Nummer 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist.*

§ 28 Absatz 3, Nr. 2 BDSG-E:
Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

Außerdem gilt § 31 BDSG (auch § 14 Abs. 4 BDSG) „Besondere Zweckbindung“:
Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

Wann eine „Rasterfandung“ eingeleitet werden darf, personenbezogene Daten also maschinell mit anderen Datensätzen verglichen werden, steht in § 98a StPO (S. 27). Angeordnet werden darf sie nur durch einen Richter bzw. bei Gefahr in Verzug durch einen Staatsanwalt (S. 29).
Die Sicherstellung bzw. Beschlagnahme von Informationen/Daten ist in § 94 StPO (S. 27) geregelt.

Mit der erkennungsdienstlichen Erfassung von Daten beschäftigt sich § 81 b StPO (S. 27), in wieweit der Beschuldigte Eingriffe in seine Körperlichkeit erdulden muß, beschreibt § 81 a StPO (S. 27).
Im Strafvollzug erfolgt ebenfalls eine erkennungsdienstlichen Erfassung (§ 86 Abs. 2 StVollzG, S. 29), hier ist auch geregelt wie mit den gewonnen Daten nach Entlassung aus dem Vollzug umzugehen ist.

2.1.3 Asylverfahren

Im Asylverfahren kommt das schon in Abschnitt 1.1 erwähnte AFIS-System[4] zur Anwendung, um Mehrfachantragsteller zu erkennen. Jeder Asylbewerber muß sich erkennungsdienstlich behandeln lassen (§ 16 Abs. 1 AsylVfG, S. 30), um seine Identität festzustellen. Diese Regelung wurde 1997 auf Kriegs- und Bürgerkriegsflüchtlinge ausgeweitet (§ 41a AuslG, S. 31). Die Datenbestände der Asylsuchenden und Ausländer werden zwar getrennt von anderen erkennungsdienstlichen Datenbeständen gehalten (§ 16 Abs. 4 AsylVfG), stehen aber der Polizei zur Recherche zur Verfügung sofern bestimmte Tatsachen dies rechtfertigen (§ 16 Abs. 5 AsylVfG).
Problematisch erscheint hier, daß flächendeckend eine bestimmte Gruppe einem staatlichen Verfahren unterworfen wird, da Art. 1 Abs. 1 GG (siehe S. 16) natürlich auch für Asylsuchende und Ausländer gilt.
Es gibt weiterhin Bestrebungen ein System für den gesamten EU-Raum einzurichten, um Mehrfachanträge länderübergreifend zu erkennen.

2.1.4 Kassenautomaten - Sozialamt

In Sozialämtern könnten zur Auszahlung von Barmitteln Geldautomaten instaliert werden, die durch ein biometrisches Merkmal statt einer PIN abgesichert werden. Geräte an verschiedenen Standorten müssen nicht kompatibel sein; so wären die technischen Schwierigkeiten, die sich bisher bei der Umsetzung von biometrischen Sicherheitskonzepten bei Geldautomaten ergeben haben, erheblich geringer. In Berlin sind seit 1997 Geldautomaten ohne Biometrie im Einsatz, eine zusätzliche Absicherung scheint nicht norwendig zu sein.

[4] Automatisches Fingerabdruck-Identifizierungssystem

2.2 Nichtöffentlicher Bereich

2.2.1 Banken

Auf der Chipkarte des Kunden wird das Referenztemplate gespeichert. Es ist erstrebenswert, daß der Vergleich zwischen Template und Referenztemplate auf der Karte stattfindet (on-card-matching).Desweiteren wäre es von Vorteil, wenn sich der Sensor auch auf der Karte befinden würde (zum Beispiel Fingererkennung). Der Einsatz von biometrischen Verfahren bei Bankgeschäften setzt eine datenschutzrechtlich wirksame Einwilligung voraus, was eine Aufklärung über die verwendeten Verfahren und abgespeicherten Daten beinhaltet.

2.2.2 Einsatz in privater Sphäre

Biometrische Verfahren sind natürlich auch für den privaten Einsatz interessant. Sie können zum Beispiel zur Absicherung von Haus-, Wohnungs- und Kfz-Türen genutzt werden oder auch zur Identifizierung an Mobiltelefonen und Computern. Allerdings sind die Verfahren mit Vorsicht zu benutzen, da Dritte betroffen sein können. Zum Beispiel können Daten absichtlich oder zufällig erhoben werden zum Beispiel bei einem Gesichtserkennungsverfahren an einer Haustür.

3 Internationale Vorschriften

In den USA gibt es kein allgemeines, bundeseinheitliches Datenschutzrecht. Es existieren nur Verbraucherschutzgesetze, die der Gesetzgebung der einzelnen Bundesstaaten unterliegen. Eine Kontrollinstanz, wie in Deutschland, ist also nicht vorhanden.
Im Vergleich zu den USA gibt es in Kanada Regeln für die sozialstaatlichen Einrichtungen, um Doppelbezüge zu vermeiden. Für den privaten Bereich findet man keine gesetzlichen Vorschriften, es werden nur Empfehlungen des Datenschutzbeauftragten ausgesprochen.

4 Fazit

Die bedeutende positive Eigenschaft biometrischer Verfahren, vor allem des Authentifizierungsmechanismus, besteht also darin, unmittelbar personenbezogene körperliche Merkmale zu erkennen, zu verwenden, und damit eine wirkliche Verifikation der Person zu erreichen. Es muß in jedem Fall bei der Verwendung biometrischer Daten eine sorgfältige Abwägung zwischen den schutzwürdigen Interessen der betroffenen Person und den berechtigten Interessen der verantwortlichen Stellen erfolgen.

Insbesondere in Hinblick auf die Terrorismusbekämpfung und die mit ihr einsetzende Welle der Aufnahme und Verarbeitung von biometrischen Merkmalen ist darauf zu achten, daß die biometrischen Daten wirklich nötig sind und nicht zur globalen Überwachung von Menschen gebraucht werden. Weltweit sollen und werden dann standardisierte Daten verarbeitet. Ob diese Daten tatsächlich zur Bekämpfung des Terrorismus dienen, ist fraglich. Insgesamt wird dieses Problem in der Öffentlichkeit zu wenig diskutiert, und zu wenig Aufklärung in der Bevölkerung betrieben. Die Politiker nutzen zum Teil die Angst der Menschen vor dem Terror und machen ihnen Glauben, daß man mit Hilfe von Biometrie Terroristen erkennen und so Anschläge verhindern könnte. Dabei vergißt man allerdings, daß dieses Problem vielschichtiger und wesentlich komplexer ist.

Der Einsatz von Biometrie sollte also für jedes Problem gut durchdacht und die involvierten Personen umfassend und ausreichend aufgeklärt werden. Der Mißbrauch von personenbezogenen Daten wird so verringert und der postive Aspekt der Nutzung von biometrischen Daten in den Vordergrund gerückt.

5 Gesetzestexte

Die hier abgedruckten Gesetzestexte stammen aus den im Literaturverzeichnis angegebenen Quellen. Alle in dieser Ausarbeitung verwendeten Gesetzestexte habe ich hier nochmal in kompakter Form angegeben, sodaß man sich das „Durchwälzen“ vieler Paragraphen ersparen kann. Für ein intensives Studium sollte man aber auch die kompletten Gesetzbücher durcharbeiten.

5.1 Grundgesetz

I. Die Grundrechte

Artikel 1 – [Menschenwürde; Grundrechtsbindung der staatlichen Gewalt]

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.
(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2 – [Allgemeine Handlungsfreiheit; Freiheit der Person; Recht auf Leben]

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.
(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

5.2 Bundesdatenschutzgesetz (BDSG)

in der Fassung der Bekanntmachung vom 14. Januar 2003

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1 a) Werden personenbezogene Daten statt beim Betroffenen bei einer nichtöffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,

2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,

3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,

7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,

8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder

9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die

sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichtsund Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die

verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürren nur für diese Zwecke verwendet werden.
(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder

2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass

das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.

(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder

2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder

3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   b) Berufs-, Branchen- oder Geschäftsbezeichnung,
   c) Namen,
   d) Titel,
   e) akademische Grade,
   f) Anschrift und
   g) Geburtsjahr
   beschränken und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

In den Fällen des Satzes 1 Nr. 3 ist anzunehmen, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich

1. auf strafbare Handlungen,
2. auf Ordnungswidrigkeiten sowie
3. bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

beziehen.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten nach Absatz 3 übermittelt werden, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nichtöffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürren die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt

nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4aAbs. 3 zulässig. Absatz 3 Nr. 2 gilt entsprechend.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt und Meinungsforschung dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

§ 28 Abs. 1 Satz 2 ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
   b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 3 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden

Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 31 Besondere Zweckbindung Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

5.3 Strafprozeßordnung (StPO)

§ 81a [Körperliche Untersuchung und Eingriffe]

(1) Eine körperliche Untersuchung des Beschuldigten darf zur Feststellung von Tatsachen angeordnet werden, die für das Verfahren von Bedeutung sind. Zu diesem Zweck sind Entnahmen von Blutproben und andere körperliche Eingriffe, die von einem Arzt nach den Regeln der ärztlichen Kunst zu Untersuchungszwecken vorgenommen werden, ohne Einwilligung des Beschuldigten zulässig, wenn kein Nachteil für seine Gesundheit zu befürchten ist.
(2) Die Anordnung steht dem Richter, bei Gefährdung des Untersuchungserfolges durch Verzögerung auch der Staatsanwaltschaft und ihren Hilfsbeamten (§ 152 des Gerichtsverfassungsgesetzes) zu.

§ 81b [Aufnahme von Lichtbildern, Fingerabdrücken und Messungen]

Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen und ähnliche Maßnahmen an ihm vorgenommen werden.

§ 94 [Beschlagnahme]

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.

(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.

§ 98a [Datenabgleich bei bestimmten Straftaten]

(1) Liegen zureichende tatsächliche Anhaltspunkte dafür vor, daß eine Straftat von erheblicher Bedeutung

1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),
3. auf dem Gebiet der gemeingefährlichen Straftaten,
4. gegen Leib oder Leben, die sexuelle Selbstbestimmung oder die persönliche Freiheit,
5. gewerbs- oder gewohnheitsmäßig
6. oder von einem Bandenmitglied oder in anderer Weise organisiert

begangen worden ist, so dürfen, unbeschadet §§ 94, 110, 161, **personenbezogene Daten** von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, **mit anderen Daten maschinell abgeglichen werden**, um Nichtverdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.

(2) Zu dem in Absatz 1 bezeichneten Zweck hat die speichernde Stelle die für den Abgleich erforderlichen Daten aus den Datenbeständen auszusondern und den Strafverfolgungsbehörden zu übermitteln.

(3) Soweit die zu übermittelnden Daten von anderen Daten nur mit unverhältnismäßigem Aufwand getrennt werden können, sind auf Anordnung auch die anderen Daten zu übermitteln. Ihre Nutzung ist nicht zulässig.

(4) Auf Anforderung der Staatsanwaltschaft hat die speichernde Stelle die Stelle, die den Abgleich durchführt, zu unterstützen.

(5) § 95 Abs.2 gilt entsprechend.

§ 98b [Anordnungsbefugnis für den Datenabgleich]

(1) Der Abgleich und die Übermittlung der Daten dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft angeordnet werden. Hat die Staatsanwaltschaft die Anordnung getroffen, so beantragt sie unverzüglich die richterliche Bestätigung. Die Anordnung tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird. Die Anordnung ergeht schriftlich. Sie muß den zur Übermittlung Verpflichteten bezeichnen und ist auf die Daten und Prüfungsmerkmale zu beschränken, die für den Einzelfall benötigt werden. Die Übermittlung von Daten, deren Verwendung besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen, darf nicht angeordnet werden. Die §§ 96, 97, 98 Abs.1 Satz 2 gelten entsprechend.

(2) Ordnungs- und Zwangsmittel (§ 95 Abs.2) dürfen nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft angeordnet werden; die Festsetzung von Haft bleibt dem Richter vorbehalten.

(3) Sind die Daten auf Datenträgern übermittelt worden, so sind diese nach Beendigung des Abgleichs unverzüglich zurückzugeben. Personenbezogene Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden. Die durch den Abgleich erlangten personenbezogenen Daten dürfen in anderen Strafverfahren zu Beweiszwecken nur verwendet werden, soweit sich bei Gelegenheit der Auswertung Erkenntnisse ergeben, die zur Aufklärung einer in § 98a Abs.1 bezeichneten Straftat benötigt werden.

(4) § 163d Abs.5 gilt entsprechend. Nach Beendigung einer Maßnahme gemäß § 98a ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

5.4 Strafvollzugsgesetz (StVollzG)

§ 86 [Erkennungsdienstliche Maßnahmen]

(1) Zur Sicherung des Vollzuges sind als erkennungsdienstliche Maßnahmen zulässig

1. die Abnahme von Finger- und Handflächenabdrücken,

2. die Aufnahme von Lichtbildern,
3. die Feststellung äußerlicher körperlicher Merkmale,
4. Messungen.

(2) Die gewonnenen erkennungsdienstlichen Unterlagen werden zu den Gefangenenpersonalakten genommen. Sie können auch in kriminalpolizeilichen Sammlungen verwahrt werden. Die nach Absatz 1 erhobenen Daten dürfen nur für die in Absatz 1, § 87 Abs.2 und § 180 Abs.2 Nr.4 genannten Zwecke verarbeitet und genutzt werden.

(3) Personen, die aufgrund des Absatzes 1 erkennungsdienstlich behandelt worden sind, können nach der Entlassung aus dem Vollzug verlangen, daß die gewonnenen erkennungsdienstlichen Unterlagen mit Ausnahme von Lichtbildern und der Beschreibung von körperlichen Merkmalen vernichtet werden, sobald die Vollstreckung der richterlichen Entscheidung, die dem Vollzug zugrunde gelegen hat, abgeschlossen ist. Sie sind über dieses Recht bei der erkennungsdienstlichen Behandlung und bei der Entlassung aufzuklären.

5.5 Asylverfahrensgesetz (AsylVfG)

§ 16 [Sicherung der Identität]

(1) Die Identität eines Ausländers, der um Asyl nachsucht, ist durch erkennungsdienstliche Maßnahmen zu sichern, es sei denn, daß er eine unbefristete Aufenthaltsgenehmigung besitzt oder noch nicht das 14.Lebensjahr vollendet hat. Nach Satz 1 dürfen nur Lichtbilder und Abdrucke aller zehn Finger aufgenommen werden.

(2) Zuständig für erkennungsdienstliche Maßnahmen sind das Bundesamt und, sofern der Ausländer dort um Asyl nachsucht, auch die in den §§ 18 und 19 bezeichneten Behörden sowie die Aufnahmeeinrichtung, bei der sich der Ausländer meldet.

(3) Das Bundeskriminalamt leistet Amtshilfe bei der Auswertung der nach Absatz 1 gewonnenen Fingerabdruckblätter zum Zwecke der Identitätssicherung. Es darf hierfür auch von ihm zur Erfüllung seiner Aufgaben aufbewahrte erkennungsdienstliche Unterlagen verwenden. Das Bundeskriminalamt darf den in Absatz 2 bezeichneten Behörden den Grund der Aufbe-

wahrung dieser Unterlagen nicht mitteilen, soweit dies nicht nach anderen Rechtsvorschriften zulässig ist.

(4) Die nach Absatz 1 gewonnenen Unterlagen werden vom Bundeskriminalamt getrennt von anderen erkennungsdienstlichen Unterlagen aufbewahrt und gesondert gekennzeichnet. Entsprechendes gilt für die Verarbeitung in Dateien.

(5) Die Verarbeitung und Nutzung der nach Absatz 1 gewonnenen Unterlagen ist auch zulässig zur Feststellung der Identität oder der Zuordnung von Beweismitteln, wenn bestimmte Tatsachen die Annahme begründen, daß dies zur Aufklärung einer Straftat führen wird, oder wenn es zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist. Die Unterlagen dürfen ferner für die Identifizierung unbekannter oder vermißter Personen verwendet werden.

(6) Nach Absatz 1 gewonnene Unterlagen sind zu vernichten

1. nach unanfechtbarer Anerkennung,
2. nach Ausstellung eines Reiseausweises nach dem Abkommen über die Rechtsstellung der Flüchtlinge,
3. nach Erteilung einer unbefristeten Aufenthaltsgenehmigung,
4. im Falle einer Einreiseverweigerung (§ 18 Abs.2) oder einer Zurückschiebung (§ 18 Abs.3) nach drei Jahren,
5. im übrigen acht Jahre nach unanfechtbarem Abschluß des Asylverfahrens,

die entsprechenden Daten sind zu löschen.

5.6 Ausländergesetz (AuslG)

§ 41a [Sicherung der Identität von Ausländern aus Kriegs- oder Bürgerkriegsgebieten]

(1) Die Identität eines Ausländers aus einem Kriegs- oder Bürgerkriegsgebiet, der das 14.Lebensjahr vollendet hat, ist durch erkennungsdienstliche Maßnahmen zu sichern, sofern ihm eine Aufenthaltsbefugnis nach §32 oder

§32a oder eine Duldung nach §54 erteilt wird oder seine Zurü,ckschiebung oder Abschiebung in Betracht kommt. Nach Satz 1 dürfen nur Lichtbilder und Abdrucke aller Finger aufgenommen werden.

(2) Zuständig für erkennungsdienstliche Maßnahmen sind die zentrale Verteilungsstelle nach §32a Abs.11 Satz 2, die Ausländerbehörden, die Grenzbehörden und die Polizeien der Länder.

(3) §16 Abs. 3 bis 5 des Asylverfahrensgesetzes findet entsprechende Anwendung.

(4) Nach Absatz 1 gewonnene Unterlagen sind nach Erteilung einer unbefristeten Aufenthaltsgenehmigung und im übrigen acht Jahre nach Einreise zu vernichten; die entsprechenden Daten sind zu löschen.

Literatur

[AsylVfG] : *Asylverfahrensgesetz.* – URL http://www.datenschutz-berlin.de/recht/de/rv/sich_o/asylvfg.htm. – Zugriffsdatum: 21.11.2004

[AuslG] : *Ausländergesetz.* – URL http://www.datenschutz-berlin.de/gesetze/auslg/auslg.htm. – Zugriffsdatum: 21.11.2004

[BDSG] : *Bundesdatenschutzgesetz.* – URL http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg03.htm. – Zugriffsdatum: 21.11.2004

[Bäumler u. a. 2001] Bäumler, Dr. H. ; Gundemann, Lukas ; Probst, Dr. T. ; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel (Hrsg.): *Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen.* August 2001

[StVollzG] : *Strafvollzugsgesetz.* – URL http://www.datenschutz-berlin.de/recht/de/rv/szprecht/stvollzg/. – Zugriffsdatum: 21.11.2004

[Thiel 2002] Thiel, Dr.: *Einsatz biometrischer Verfahren an Geldausgabeautomaten - Sicherheitsanforderungen.* März 2002

[Vogel u. a.] Vogel, Kolja ; Beinlich, Stephan ; Martini, Ullrich: *Die virtuelle PIN.* – URL http://www.cifro.com/download/weissbuch_vpin_v_1_0.pdf. – Zugriffsdatum: 21.11.2004