Deutscher Bundestag **Drucksache 14/10005**
14. Wahlperiode 10. 10. 2002

Bericht

des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (19. Ausschuss) gemäß § 56a der Geschäftsordnung

Technikfolgenabschätzung

hier: TA-Projekt: Biometrische Identifikationssysteme – Sachstandsbericht

Inhaltsverzeichnis

		Seite
Vorwort des Ausschusses		3
Zusammenfassung		4
I.	**Einleitung**	8
II.	**Biometrie: Merkmale, Verfahren und Systeme**	9
1.	Allgemeines zu biometrischen Verfahren	9
2.	Biometrische Systeme im Einzelnen	11
2.1	Fingerbild	12
2.2	Handgeometrie	14
2.3	Iris	15
2.4	Retina	16
2.5	Gesicht	16
2.6	Unter-/Handschrift	17
2.7	Stimme	19
2.8	Kombinationen	19
2.9	Entwicklungslinien im Frühstadium	19
3.	Vorzüge und Nachteile der Systeme im Überblick	20
III.	**Forschungs- und Entwicklungsaktivitäten**	23
1.	Pilotprojekte und Entwicklung von Testkriterien	23
1.1	BioIS-Projekt	23

		Seite
1.2	BioTrusT (TeleTrusT Deutschland e.V.)	25
1.3	Standardisierung und Evaluierung biometrischer Systeme	26
2.	FuE-Projekte in Deutschland und international	27
IV.	**Biometrische Verfahren in der Praxis**	33
1.	Anwendungsfelder und -beispiele	33
1.1	Benutzerzugangssicherung	34
1.2	Personenidentifikation	34
1.3	Gerätezugangskontrolle	35
1.4	Elektronischer Zugang zu Informationen und Dienstleistungen	36
1.5	Conveniencebereiche	36
1.6	Internetanwendungen und das Problem der Referenzdaten	37
2.	Markteinschätzung	38
V.	**Verbraucherpolitik, Recht, Datenschutz**	39
1.	Verbraucherpolitische Anforderungen an die Biometrie	39
2.	Elektronische Signaturen und Biometrie – rechtliche Aspekte	41
3.	Datenschutz	44
3.1	Biometrische Daten als personenbezogene Daten	44
3.2	Grundrechtsbezug biometrischer Daten und Verfahren	45
3.3	Folgerungen für rechtliche Regelungen und die Praxis biometrischer Verfahren	46
4.	Das Terrorismusbekämpfungsgesetz	47
VI.	**Perspektiven der weiteren Entwicklung – Forschungs- und Handlungsbedarf**	48
Literatur		52
1.	Vergebene Gutachten	52
2.	Weitere Literatur	52
Anhang		54
1.	Tabellenverzeichnis	54
2.	Abbildungsverzeichnis	54
3.	Biometrie und Internet – Projekte und Produkte	55
4.	Marktabschätzungen zur Biometrie	56

Vorwort des Ausschusses

Die zweifelsfreie Bestimmung der Identität von Personen stellt insbesondere im elektronischen Geschäfts- und Rechtsverkehr eine zentrale Herausforderung dar. Die Schwächen bislang üblicher Systeme zur Überprüfung der Zugangs- und Handlungsberechtigung, die persönliche Kennziffern oder Passwörter benutzten, sollen durch den Einsatz „biometrischer Verfahren“ überwunden werden. „Biometrie“ bezeichnet in diesem Zusammenhang die automatisierte Messung von natürlichen, hoch charakteristischen physiologischen oder verhaltensabhängigen Merkmalen von Menschen wie Handgeometrie, Fingerabdruck, Stimme, Gesicht, Iris oder Handschrift. Bis zum Sommer 2001 wurde das Thema „biometrische Identifikationssysteme“ vor allem mit Blick auf kundenorientierte Anwendungen z. B. im Rahmen des E-Commerce, als PIN-Ersatz für Geld- und Kreditkarten oder als Zugangssicherung für PCs und Mobiltelefone diskutiert. In der Folge der Terroranschläge in den USA vom 11. September 2001 sind die möglichen Beiträge biometrischer Verfahren zur Verbesserung der öffentlichen Sicherheit in den Vordergrund der Überlegungen gerückt.

Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung hat das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) beauftragt, das Feld der biometrischen Verfahren und Systeme einer ersten Sichtung zu unterziehen und den Versuch einer Bestandsaufnahme sowie einer vorläufigen Beurteilung der FuE-Aktivitäten, der Marktentwicklung und der augenblicklichen und zukünftigen Anwendungsfelder und -potenziale zu unternehmen. Als besonders relevante Fragestellungen wurden Diffusionsperspektiven, Verlässlichkeit und Manipulationssicherheit, Datenschutz und informationelle Selbstbestimmung, Verbraucherschutz, Rechtsfragen und die Rolle der Politik definiert.

Der vorliegende Bericht des TAB bietet einen Überblick über biometrisch genutzte menschliche Merkmale sowie die entsprechenden technischen Verfahren der Identifizierung, skizziert den nationalen und internationalen Stand der Forschungs- und Entwicklungsaktivitäten und fasst Anwendungsmöglichkeiten und -beispiele aus der Praxis zusammen. Nach einer Erörterung von Fragen des Verbraucher- und Datenschutzes und weiterer rechtlicher Aspekte werden mögliche Entwicklungstendenzen der Biometrie und der daraus resultierende politische und rechtliche Handlungsbedarf umrissen.

Der Deutschen Bundestag erhält mit diesem Bericht einen hoch aktuellen, umfassenden wie kompakten Überblick zum Thema „biometrische Identifikationssysteme“. Die Autoren des TAB kommen zu dem Schluss, dass auf der Basis der bislang verfügbaren – oftmals äußerst widersprüchlichen – Informationen die Leistungsfähigkeit verfügbarer biometrischer Systeme zurzeit noch nicht seriös einzuschätzen ist. Mit dem „Gesetz zur Bekämpfung des internationalen Terrorismus“ ist die Möglichkeit geschaffen worden, über die bisherigen Angaben zu Größe und Augenfarbe sowie das Lichtbild hinaus biometrische Merkmale in Ausweispapiere in verschlüsselter, maschinenlesbarer Form aufzunehmen. Arten, Einzelheiten, Einbringung und die Technik der Speicherung biometrischer Merkmale werden durch ein Bundesgesetz geregelt. Vor diesem Hintergrund gilt es, die Voraussetzungen und möglichen Auswirkungen einer solchen Maßnahme genauer zu untersuchen. Neben der Frage nach der Alltagstauglichkeit und Sicherheit sind viele rechtliche Implikationen der Biometrie heute noch weitgehend unklar, aus juristischer und politischer Sicht aber von hoher Relevanz.

Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages hat das TAB daher beauftragt, im Hinblick auf den zu erwartenden Informationsbedarf des 15. Deutschen Bundestages in einem weiteren Projekt vertiefende Untersuchungen durchzuführen. Thematische Schwerpunkte werden die Leistungsfähigkeit biometrischer Systeme sowie Rechtsfragen und Datenschutzaspekte sein.

Berlin, den 3. September 2002

Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

Ulrike Flach Vorsitzende/Berichterstatterin	**Ulla Burchardt** Berichterstatterin	**Axel E. Fischer** Berichterstatter
	Hans-Josef Fell Berichterstatter	**Angela Marquardt** Berichterstatterin

Zusammenfassung

Aufgabe des TAB war es, im Rahmen einer „Vorbereitenden Untersuchung“ das Feld der biometrischen Verfahren und Systeme einer ersten Sichtung zu unterziehen und den Versuch einer Bestandsaufnahme sowie einer vorläufigen Beurteilung der FuE-Aktivitäten, der Marktentwicklung und der augenblicklichen und zukünftigen Anwendungsfelder (und -potenziale) zu unternehmen. Aus rechtlicher, insbesondere datenschutzrechtlicher, und verbraucherpolitischer Sicht sollte eine erste Einschätzung biometrischer Verfahren und Systeme erfolgen.

Merkmale, Verfahren und Systeme

„Biometrie“ bezeichnet die Erfassung und (Ver-)Messung von Lebewesen und ihren Eigenschaften. Im vorliegenden Zusammenhang meint Biometrie bzw. Biometrik die (automatisierte) Messung eines individuellen – physiologischen oder verhaltenstypischen – Merkmals einer Person zum Zweck der (biometrischen) Identifikation und damit zur Unterscheidung von anderen Personen.

Um „biometrisch optimal genutzt“ werden zu können, müssten Merkmale des Menschen – ob physiologische (passive) oder verhaltensabhängige (aktive) – universell, einzigartig, beständig und (technisch) erfassbar sein. Die biometrischen Verfahren bzw. Systeme wiederum, die mit diesen Merkmalen arbeiten, müssen in praktischer Hinsicht schnell, kompatibel mit vorhandenen Sicherheitselementen, robust, genau, sicher, wirtschaftlich und zuverlässig sein. Keines der derzeit genutzten „biometrischen Merkmale“ bzw. keines der verfügbaren Systeme genügt allen Anforderungen vollständig. Dennoch sind weltweit zahlreiche Systeme in unterschiedlichen Anwendungskontexten in Betrieb, z. B. zur Überprüfung der Handlungsberechtigung von Personen bei E-Banking- und E-Commerce-Transaktionen oder im Rahmen von Zugangskontrollen zu sicherheitsrelevanten Bereichen (Kapitel IV.1). Am häufigsten eingesetzt werden die Erkennung von Fingerbild, Handgeometrie, Gesicht, Stimme, Iris/Retina und Unter-/Handschrift, die in Kapitel II.2 nach physiologischen, technischen, ökonomischen und Nutzeraspekten beschrieben werden.

Konventionelle Systeme können verwendete Passwörter oder PIN-Chipkarten nicht daraufhin überprüfen, ob der Nutzer, der die korrekten Daten liefert, auch deren rechtmäßiger Inhaber ist. Da biometrische Verfahren mit personengebundenen Merkmalen (die weder verloren noch vergessen und auch nicht so leicht gestohlen werden können) arbeiten, versprechen sie neue Qualitäts-, Komfort- und Sicherheitsdimensionen bei der Personenauthentifizierung.

Leistungsfähigkeit biometrischer Verfahren

Die Leistungsfähigkeit verfügbarer biometrischer Systeme ist auf der Basis der – oftmals äußerst widersprüchlichen – Informationen nicht seriös einzuschätzen (Kapitel II.3). Für Verwirrung sorgt häufig die unscharfe Trennung zwischen möglichem Potenzial und augenblicklicher tatsächlicher Kapazität. Trotz erreichter Verbesserungen und sicherlich weiter zunehmender technischer Fortschritte ist daher Berichten über mittlerweile erreichte hohe Standards bei Genauigkeit und Zuverlässigkeit biometrischer Systeme nach wie vor mit Skepsis zu begegnen.

Auf nationaler und internationaler Ebene sind mehrere Gremien damit befasst, Kriterien für eine zukünftige Evaluation biometrischer Systeme zu definieren, die vorhandenen Verfahren (oft eher Prototypen) werden in verschiedenen Pilotprojekten vergleichenden Praxistests unterzogen (Kapitel III.1). Ein allgemein anerkanntes Vorgehen beim Vergleich der Stärken und Schwächen der verschiedenen biometrischen Systeme ist aber noch nicht etabliert. Darüber hinaus macht die unterschiedliche Entwicklungs- bzw. Praxisreife der verschiedenen biometrischen Systeme eine vergleichende Evaluation schwierig. Eine solche müsste nachvollziehbare und aussagekräftige Daten u. a. zu Zuverlässigkeit, Genauigkeit, Empfindlichkeit, Akzeptanz, Robustheit, Kompatibilität, Einfachheit und Kosten umfassen. Eine genaue Beurteilung von Stärken und Schwächen eines Verfahrens kann nur in einem spezifischen Anwendungskontext, empirisch angelegt und in ihren Einzelschritten nachvollziehbar, erfolgen.

Insbesondere dann, wenn es um einen weit reichenden, große Nutzergruppen – ob freiwillig oder verpflichtend – einbeziehenden Einsatz biometrischer Systeme geht, z. B. im Rahmen der Ausrüstung von Ausweispapieren, müssen höchste Ansprüche an eine substanziierte Evaluation der infrage kommenden Systeme gestellt werden. Eine regelmäßige Berichterstattung zum Stand der laufenden Pilotprojekte und der (internationalen) Standardisierungsbemühungen wäre als Basis für die weitere politische Behandlung des gesamten Themenkomplexes sicherlich nützlich.

FuE-Aktivitäten

Der Stand der Forschung und Entwicklung im Bereich biometrischer Systeme konnte für Deutschland etwas umfassender erhoben werden, ebenso auch die Förderaktivitäten der EU, allenfalls exemplarisch jedoch auf internationaler Ebene. Gerade im nordamerikanischen und asiatischen Raum gibt es eine kaum überschaubare Vielzahl von Aktivitäten im privatwirtschaftlichen und öffentlichen Sektor.

Von besonderem Interesse sind die so genannten „Pilotprojekte“ zur Evaluierung biometrischer Systeme, die sowohl technische Fragestellungen als auch Verbraucher- und Datenschutzaspekte untersuchen. In Deutschland waren bzw. sind dies insbesondere das u. a. vom BMWi

geförderte Projekt BioTrust und das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geförderte BioIS-Projekt (Kapitel III.1).

Nachdem bereits seit längerer Zeit insbesondere in mehreren Fraunhofer-Instituten Forschung zur Biometrie betrieben wurde, sind die Förderaktivitäten seitens des Bundes in den vergangenen zwei Jahren insgesamt intensiviert worden. Auch die industriellen Aktivitäten rund um biometrische Anwendungen haben in Deutschland an Dynamik gewonnen, dabei werden zunehmend die Möglichkeiten von Kooperationen im Rahmen von EU-Projekten genutzt. Die Telekom-Tochter T-Systems Nova hat 1999 ein eigenes Pilotprojekt gestartet, die Firma ekey biometric systems 2001 eines in Österreich. Unter den europäischen Ländern gilt Großbritannien als besonders engagiert in öffentlicher und privater FuE. Die EU fördert im aktuellen IST-Programm derzeit sieben größere Projekte zur Biometrie mit über 10 Mio. Euro (Kapitel III.2).

Anwendungen biometrischer Verfahren

Es existiert eine große und ständig wachsende Zahl von Berichten über konkrete Nutzungen in zahlreichen Einsatzfeldern, insbesondere aus den USA, aber auch aus europäischen und asiatischen Ländern. Der Einsatz biometrischer Identifikationssysteme erfolgte bis vor einigen Jahren fast ausschließlich zu Sicherheitszwecken, bevor nach und nach weitere Anwendungsfelder in Unternehmen und Behörden erschlossen wurden. Bisherige und absehbare Einsatzfelder können in fünf Gruppen eingeteilt werden (Kapitel IV.1):

– Benutzerzugangssicherung,
– Personenidentifikation,
– Gerätezugangskontrolle,
– elektronischer Zugang zu Dienstleistungen (E-Banking und E-Commerce),
– sonstige „Conveniencebereiche“.

Markteinschätzung

Vorliegende ökonomische Daten und Einschätzungen zum Einsatz biometrischer Systeme wirken häufig sehr punktuell und zufällig (Kapitel IV.2). In der Regel sind sie wenig transparent, auf keinen Fall geben sie ein vollständiges Bild. Allerdings ist es methodisch auch schwierig, den eigentlichen „biometrischen“ Anteil einer Gesamttechnologie zu definieren, abzugrenzen und wertmäßig zu beziffern. Auch die Daten der amtlichen Statistiken liefern keine Grundlage, um relevante Kennziffern für biometrische Produkte und Dienstleistungen (Produktionsumfang, Umsätze, Beschäftigte u. Ä.) zu erhalten. Darüber hinaus verfolgen die beteiligten Firmen oft eine eher restriktive Informationspolitik. Der Stand der Diffusion, der Umsätze und der Marktanteile (national wie international) bleibt daher äußerst unscharf.

Festgestellt werden können allenfalls tendenziell steigende Umsätze in den vergangenen Jahren: Die USA stellen dabei den dominierenden Markt dar (auf dem ca. zwei Drittel der Umsätze erzielt werden), gefolgt von Europa, Asien und Lateinamerika. Wie so oft gilt Asien als bedeutender Zukunftsmarkt, doch auch in Europa wird eine zunehmende Nachfrage vermutet. Derzeit anscheinend führende Technologie, sowohl umsatzbezogen als auch hinsichtlich der Zahl der Anbieter und Systeme, sind die Fingerbildverfahren; besonders der Gesichtserkennung wird zunehmendes Potenzial eingeräumt. Angenommen wird eine Konsolidierung des Marktes, sobald einzelne Systeme und Anbieter größere Marktanteile erlangen.

Im Hinblick auf eine mögliche gezieltere Förderung im Bereich Biometrie wären genauere Daten vonnöten. Voraussetzung hierfür wäre allerdings die Entwicklung von Konzepten und Methoden zur besseren Erfassung relevanter wirtschaftlicher Kennziffern, differenziert nach eigentlichem biometrischen System, peripheren Geräten sowie Art und Umfang der Anwendung.

Verbraucherschutz

Die weltweiten Forschungs- und Entwicklungsaktivitäten sowie die zunehmend erkennbare Ausweitung von Einsatzfeldern signalisieren die Möglichkeit, dass biometrische Verfahren schon bald den gesellschaftlichen Alltag durchdringen werden. Deshalb gewinnen Fragen des Verbraucherschutzes, der rechtlichen Rahmenbedingungen sowie insbesondere des Datenschutzes an Bedeutung.

Will man die Chancen der Biometrie nutzen und die Risiken beherrschen, so müssen Gestaltung und Anwendung biometrischer Systeme bestimmte Kriterien erfüllen. Dazu zählen vor allem hohe Sicherheit, umfassende Vertrauenswürdigkeit, ausreichende Nutzerfreundlichkeit sowie weitgehende Sozialverträglichkeit (Kapitel V.1).

Sicherheit und Vertrauenswürdigkeit

Sollen biometrische Verfahren zur Sicherheit elektronischer Anwendungen beitragen, müssen sie selbst hohen Sicherheitsanforderungen genügen. Um das zu gewährleisten, sollten die unterschiedlichen biometrischen Verfahren je nach Merkmal, Risikopotenzial und Anwendungsfeld differenziert bewertet und vor einer breiten Markteinführung einer umfassenden Risikoanalyse unterzogen werden. Schlüssige Sicherheitskonzepte für einzelne Anwendungsszenarien unter Beachtung verbraucher- und datenschutzrechtlicher Erfordernisse sind aber noch nicht weit entwickelt.

Um eine möglichst große Vertrauenswürdigkeit zu erreichen, wird beispielsweise vorgeschlagen, Vertrauensinstanzen einzurichten, die – fachlich kompetent, unabhängig und neutral – ein im Zusammenwirken von Nutzern, Herstellern, Betreibern und Staat vereinbartes Sicherheitsniveau umfassend prüfen und gewährleisten.

Eine Voraussetzung für die Überprüfung und entsprechende Zertifizierung biometrischer Systeme ist die Entwicklung zuverlässiger Evaluierungskriterien, anhand derer unterschiedliche Verfahren objektiv verglichen werden können. Die (weltweiten) Bemühungen hierzu

sind noch nicht abgeschlossen. Anwender und Nutzer bekämen durch allgemein anerkannte Kriterien einen Leitfaden für die Auswahl eines sicheren Produktes an die Hand; zugleich würde eine Richtschnur für die Entwicklung sicherer, vertrauenswürdiger Systeme geboten. Damit solche Evaluierungskriterien breite Akzeptanz finden, sollten sie – unter Einbezug der Entwickler – von anbieterunabhängigen Stellen entwickelt werden.

Nutzerfreundlichkeit und Sozialverträglichkeit

Ausreichende Nutzerfreundlichkeit biometrischer Verfahren setzt voraus, dass diese robust und alltagstauglich sind, d. h. im massenhaften Gebrauch über lange Zeit zuverlässig funktionieren. Dies ist häufig noch nicht der Fall. Die Sozialverträglichkeit biometrischer Verfahren wird sich zum einen daran erweisen müssen, dass ihre breite Implementierung nicht zur weiteren „digitalen Spaltung" der Gesellschaft beiträgt, zum andern daran, dass kein „Zwang zur Biometrie" entsteht. Aus verbraucherpolitischer Sicht müssten also Vorkehrungen getroffen werden, die gewährleisten, dass kein Nutzer von biometrischen Anwendungen ausgeschlossen wird, z. B. wären (biometrische und herkömmliche) Ausweichverfahren bereitzustellen.

Einschlägige rechtliche Regelungen

Regelungen, die sich ausdrücklich mit dem Einsatz biometrischer Verfahren befassen, lagen in Deutschland bis vor kurzem nur hinsichtlich ihrer Verwendung im Rahmen elektronischer Signaturen vor (Kapitel V.2). Im Mai 2001 trat ein neues Signaturgesetz (SigG) in Kraft, im Juli 2001 folgte das „Formgesetz", mit dem die „qualifizierte elektronische Signatur" wie eine handschriftliche Signatur als formgebundene Erklärung anerkannt wird.

Während das Signaturgesetz bewusst technikoffen formuliert ist, wird in der Verordnung zum Gesetz (SigV) ausdrücklich der Einsatz biometrischer Verfahren ermöglicht: In Bezug auf die Sicherung des Signaturschlüssels hat der Signaturschlüssel-Inhaber die Wahl, sich vor der Anwendung des Schlüssels entweder in herkömmlicher Weise durch „Besitz und Wissen" (etwa Karte und Geheimzahl) oder aber „durch Besitz und ein oder mehrere biometrische Merkmale" zu identifizieren. Ergänzend gibt die Verordnung ein bestimmtes Sicherheitsniveau vor: Bei der Anwendung eines biometrischen Verfahrens muss „hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist, und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein" (§ 15 Abs. 1 SigV).

Aus Verbraucherschutzsicht ist diese vergleichende Bezugnahme auf Verfahren nach dem Prinzip von „Besitz und Wissen" schon seit längerem kritisch kommentiert worden. Dabei wird vor allem auf den Umstand hingewiesen, dass die Sicherheit solcher Verfahren heute weithin umstritten ist.

Mit den genannten Regelwerken gibt es in Deutschland einen gesetzlichen Rahmen für den Einsatz biometrischer Verfahren im Zusammenhang mit der elektronischen Signatur und dem elektronischen Rechts- und Geschäftsverkehr. Das Recht eröffnet dabei ausdrücklich der Biometrie ein Anwendungsfeld von zukünftig wahrscheinlich wachsender Bedeutung. In der Praxis wird sich zeigen, ob dieser Rechtsrahmen ausreicht und geeignet ist oder fortentwickelt werden sollte.

Datenschutz

Insofern biometrische Verfahren auf persönliche körperliche Merkmale zurückgreifen, sind Fragen des Datenschutzes berührt (Kapitel V.3).

Wichtigste rechtliche Grundlage für die Bewertung von biometrischen Verfahren unter Aspekten des Datenschutzes ist das neugefasste Bundesdatenschutzgesetz (BDSG). Zweck des Gesetzes ist es, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird" (§ 1 Abs. 1 BDSG). Im Zusammenhang mit Daten in biometrischen Verfahren ist speziell § 3 Abs. 9 BDSG von Interesse, der „besondere Arten personenbezogener Daten" benennt und sie unter erhöhten Schutz stellt. Unter diesen Begriff fallen „Angaben über rassische und ethnische Herkunft, über politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". Bestimmte Daten in biometrischen Verfahren können einen Informationsgehalt haben, der in diesen besonderen Schutzbereich fällt.

Soweit mithilfe biometrischer Verfahren personenbezogene Daten erzeugt werden, unterliegen diese Verfahren den Regelungen des allgemeinen Datenschutzes. Das gilt sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich. Für den öffentlichen Bereich sind darüber hinaus spezielle, bereichsspezifische Regelungen erforderlich.

Grundrechtsbezug der Biometrie

Datenverarbeitung mittels biometrischer Verfahren greift in einen speziellen Aspekt des Allgemeinen Persönlichkeitsrechts ein: das Recht auf informationelle Selbstbestimmung. Dieser Eingriff ist durch die Datenschutzgesetzgebung erfasst. Auch die Menschenwürde kann als herausragendes Schutzgut betroffen sein.

Das Grundrecht auf informationelle Selbstbestimmung garantiert die Befugnis des Einzelnen, prinzipiell selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Zugleich sind begrenzte staatliche Eingriffe in dieses Recht zulässig. Staatlich angeordneter Einsatz biometrischer Verfahren greift aber nicht nur in diesen speziellen Schutzbereich ein. Indem er körperliche Merkmale und Verhaltensweisen als Informationsquelle nutzt, dürfte ein weiterer Bereich des Allgemeinen Persönlichkeitsrechtes zumindest tangiert sein. Die Grenzen zu einem Würdeverstoß wären dann berührt oder überschritten, wenn durch den Staat eine weit reichende Erfassung und Verarbeitung biometrischer Merkmale verlangt würde und damit die Möglichkeit einer „Registrierung" und „Katalogisierung der Persönlichkeit" eröffnet wäre.

Teilt man die Einschätzung, dass biometrische Verfahren u. U. über den Bereich des Rechtes auf informationelle Selbstbestimmung hinaus in einen weiteren Bereich des Allgemeinen Persönlichkeitsrechts eingreifen, so folgt daraus, dass die bestehenden gesetzlichen Erlaubnisse zur Datenverarbeitung nicht ausreichen, diesen doppelten Eingriff abzudecken. Das heißt in der Konsequenz, dass für die Implementierung biometrischer Komponenten in staatliche Verfahren eine eigenständige Entscheidung des Gesetzgebers erforderlich ist, der beide Aspekte des Eingriffs – den spezifischen biometrischen ebenso wie den in das Recht auf informationelle Selbstbestimmung – legitimiert.

Systemdatenschutz

Ob und wieweit eine bestimmte Praxis des Einsatzes biometrischer Verfahren datenschutzrechtlichen Vorgaben genügt, hängt grundlegend ab von der Eingriffsintensität. Hier macht das Datenschutzgesetz Vorgaben, die als Richtschnur für möglichst eingriffsarme Verfahren gelten können:

– Grundsätzlich sind Daten offen zu erheben, unmittelbar beim Betroffenen, unter seiner Mitwirkung und mit seiner Unterrichtung bzw. seiner Kenntnis u. a. bezüglich der Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung (§ 4 Abs. 2 und 3 BDSG). Unter diesem Gesichtspunkt sind Verfahren, die einen hohen Grad der Mitwirkung bezüglich der Erfassung der Rohdaten verlangen, solchen, die weniger beteiligen oder gar unbemerkt arbeiten, vorzuziehen.

– Gefordert ist, unter dem Stichwort „Datenvermeidung und Datensparsamkeit“, schon bei der Auswahl und Gestaltung eines Datenverarbeitungssystems darauf zu achten, dass keine bzw. möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden (§ 3a BDSG).

– Anzustreben ist ferner, zum Zwecke des Datenschutzes, von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen (§ 3a BDSG).

Aktive Mitwirkung der Betroffenen, sparsame Erhebung und Verwendung von Daten sowie technikbedingt hohe Sicherheit in der Vermeidung von Personenbezug: Damit sind wichtige Komponenten eines Systemdatenschutzes als (materielle) Grundlage effektiven Datenschutzes benannt. Entscheidend dazu beitragen können templatefreie Verfahren. Sie ermöglichen „Anonymisierung“ und „Pseudonymisierung“ von Daten und sorgen dafür, dass die Möglichkeit, Personenbezug herzustellen, praktisch ausgeschlossen ist. Einen weiteren Beitrag leistet die dezentrale Ablage der Daten entweder in autonomen Geräten oder auf einer Chipkarte unter persönlicher Kontrolle der Betroffenen.

Neuere rechtliche Entwicklungen

Im Zuge der intensiven Diskussionen um Maßnahmen zur Verbesserung der Sicherheitslage seit dem 11. September 2001 wurde auch der Einsatz biometrischer Verfahren erörtert. Der Gesetzgeber ist hier entsprechend tätig geworden (Kapitel V.4). Insbesondere im Pass- und Personalausweisrecht werden durch das kürzlich verabschiedete „Terrorismusbekämpfungsgesetz“ („Gesetz zur Bekämpfung des internationalen Terrorismus“) die Möglichkeiten computergestützter Identifizierung von Personen durch biometrische Daten in Ausweisdokumenten eröffnet. Durch ein zukünftiges Bundesgesetz geregelt werden die „Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form […] sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung“.

Im Ausländergesetz wird ebenfalls die Nutzung biometrischer Merkmale in der o. g. Art und Weise als Möglichkeit eröffnet: Einzelheiten bestimmt das Bundesministerium des Innern durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf.

Mit dem „Terrorismusbekämpfungsgesetz“ hat der Gesetzgeber eine parlamentsgesetzliche Grundlage geschaffen, aus der (auch für den Bürger) Voraussetzungen, Ziel und Umfang des Eingriffes in das Recht auf informationelle Selbstbestimmung klar hervorgehen:

– Die zu nutzenden biometrischen Merkmale werden alternativ explizit genannt.

– Der Zweck der gespeicherten Daten ist ausdrücklich bestimmt.

– Für die Einführung von mit biometrischen Merkmalen versehenen Ausweisdokumenten deutscher Staatsbürger ist ein Gesetzesvorbehalt vorgesehen. Anders bei den Ausweispapieren von Ausländern: Hier soll eine Rechtsverordnung die Grundlage bilden.

Den Anliegen des BDSG wurde vor allem dadurch entsprochen, dass dem Pass- oder Ausweisinhaber auf Verlangen von den zuständigen Behörden Auskunft über den Inhalt der – verschlüsselten – Daten zu erteilen ist. Es ist ferner ausdrücklich vorgesehen, dass keine „bundesweite Datei“ eingerichtet werden soll.

Perspektiven der weiteren Entwicklung

Biometrische Systeme und Verfahren befinden sich weltweit vermutlich in einer entscheidenden Phase der Diffusion. Zahlreiche Indizien lassen ihre Expansion in weitere öffentliche und private Anwendungsfelder erwarten: Die technologischen Fortschritte sind unübersehbar. Die technischen Funktionalitäten einzelner Systeme werden zunehmend ausgereift und weisen eine verbesserte Leistungsfähigkeit auf. Die Preisentwicklung bei vielen Systemen dürfte ihre weitere Verbreitung befördern. Einzelne Basiskomponenten wie Sensoren oder Chips sind zunehmend preisgünstig am Markt verfügbar, ein erhöhter Produktionsausstoß ermöglicht darüber hinaus weitere Preissenkungen. Mittlerweile stellt sich das Angebot qualitativ verbessert dar, sodass die Nachfrage besser stimuliert und befriedigt werden kann.

Die geltenden rechtlichen Rahmenbedingungen (insbesondere das Signaturgesetz und die Signaturverordnung) eröffnen der Biometrie im Bereich elektronisch getätigter Transaktionen und Rechtsgeschäfte einen riesigen Markt. Durch das „Terrorismusbekämpfungsgesetz“ ist die Tür zum Markt der Sicherheitstechnologien weiter geöffnet worden. Sollte in Deutschland (und Europa) durch staatliche Verfahren ein Masseneinsatz von biometrischen Systemen angestoßen werden, so würde dies voraussichtlich Signalwirkungen für andere Anwendungsfelder in der Wirtschaft und im privaten Bereich haben. Von Verbraucherverbänden und Datenschützern ist die Biometrie zwar stets kritisch, zugleich aber auch positiv bewertet worden: Das Potenzial der Biometrie als verbraucher- und datenschutzfreundliche Technologie wird herausgestrichen – allerdings verbunden mit der Aufforderung an Entwickler und Anwender, für technische und organisatorische Lösungen zu sorgen, die den Kriterien eines fortgeschrittenen Daten- und Verbraucherschutzes genügen.

Forschungs- und Handlungsbedarf

Angesichts der wahrscheinlich wachsenden Bedeutung biometrischer Systeme in Wirtschaft und Gesellschaft ist erheblicher Bedarf an Forschung, Information, Diskussion und Aufklärung vorhanden. In Kapitel VI wird dieser Bedarf zusammenfassend dargestellt.

Die Verbesserung der Informationslage angesichts der Dynamik der Entwicklung erscheint besonders dringlich. Zur weiteren Abklärung der zukünftigen Entwicklung biometrischer Systeme könnte beispielsweise eine umfassende Technikfolgenabschätzung durchgeführt werden. Erforderlich wäre eine systematische, zukunftsorientierte Analyse und Beurteilung der gesellschaftlichen, ökonomischen und rechtlichen Voraussetzungen und Folgen einer weiter zunehmenden Verbreitung biometrischer Verfahren, die einen Zeithorizont bis 2010 aufspannen sollte. Die Analyse hätte darüber hinaus politischen Gestaltungsbedarf zu identifizieren. Integriert werden könnte ein moderierter Expertendiskurs, dessen Ausrichtung und Aufgabenstellung in Kapitel VI skizziert werden.

I. Einleitung

Im Juni 2000 wurde das TAB durch den Ausschuss für Bildung, Forschung und Technikfolgenabschätzung beauftragt, vorbereitende Untersuchungen zum Thema „biometrische Systeme“ in Angriff zu nehmen. Als besonders relevante Fragestellungen wurden

– Diffusionsperspektiven,

– Verlässlichkeit und Manipulationssicherheit,

– Datenschutz und informationelle Selbstbestimmung,

– Verbraucherschutz, Rechtsfragen und die Rolle der Politik

definiert. Auftrag des TAB war es, durch Expertengespräche und Kurzgutachten das Untersuchungsfeld aufzuhellen, den Forschungsstand zu erheben und gegebenenfalls zentrale Fragen einer vertiefenden TA-Analyse zu definieren.

Bis zum Sommer 2001 wurde das Thema „biometrische Identifikationssysteme“ – auch kurz: „Biometrie“ – zunehmend im Hinblick auf kundenorientierte Anwendungen z. B. im Rahmen des E-Commerce, als PIN-Ersatz für Geld- und Kreditkarten oder als Zugangssicherung für PCs und Mobiltelefone diskutiert. In der Folge der Terroranschläge in den USA vom 11. September 2001 sind mittlerweile die möglichen Beiträge biometrischer Verfahren zur Verbesserung der öffentlichen Sicherheit in den Vordergrund gerückt. Dies hat auch bereits im deutschen „Terrorismusbekämpfungsgesetz“ seinen Niederschlag gefunden. Die veränderte und weitaus intensivere Diskussionslage seit Herbst 2001 hat die Bearbeiter des TAB veranlasst, die aktuellen Entwicklungen aufzugreifen und die ursprünglich geplante Berichterstattung etwas zu erweitern: Zum einen wurde ein Kommentierungs- und Ergänzungsgutachten eingeholt (Platanista 2001a und b), zum andern wurden die rechtlichen Entwicklungen einer vertieften Betrachtung unterzogen (Kapitel V.2 bis V.4). Dennoch kann und will der vorliegende Bericht lediglich eine vorläufige Bestandsaufnahme zum Stand von Forschung, Entwicklung und Anwendung biometrischer Systeme leisten. Auch die Beurteilung der verbraucherpolitischen und rechtlichen Anforderungen an eine sozialverträgliche Ausgestaltung dieser zukunftsträchtigen, aber auch umstrittenen Technologie ist nur als erste Annäherung an eine umfassende Bewertung ihrer Chancen und Risiken zu verstehen.

Eine wichtige Informationsgrundlage für den Bericht des TAB bildeten folgende fünf Gutachten:

– Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren unter Berücksichtigung der Situation in den USA (Astrid Albrecht; Arbeitsgemeinschaft der Verbraucherverbände [AgV] e.V.), Bonn 2001;

– Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt. Eine Bestandsaufnahme – unter Berücksichtigung der USA (Michael Behrens, Richard Roth; TransMIT-Zentrum, Institut für biometrische Identifikationssysteme), Gießen 2001;

– Biometrische Systeme – FuE, Diffusionstendenzen und Anwendung. Kommentar- und Ergänzungsgutachten (Jana Dittmann, Astrid Mayerhöfer, Claus Vielhauer; Platanista GmbH), Darmstadt 2001;

– Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet – Kurzexpertise (Jana Dittmann, Astrid Mayerhöfer, Claus Vielhauer; Platanista GmbH), Darmstadt 2001;

– Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen (Helmut Bäumler, Lukas Gundermann, Thomas Probst; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein [ULD-SH]), Kiel 2001.

Der Aufbau des Berichtes ist wie folgt: Kapitel II liefert einen Überblick über biometrisch genutzte Merkmale sowie biometrische Verfahren und Systeme. Kapitel III widmet sich dem Stand der Forschungs- und Entwicklungsaktivitäten, national und international, beschreibt Pilotprojekte und Initiativen zur Standardisierung und Evaluierung biometrischer Systeme. Anwendungsmöglichkeiten und -beispiele aus der Praxis fasst Kapitel IV zusammen, bevor in Kapitel V Fragen des Verbraucher- und Datenschutzes und weitere rechtliche Aspekte erörtert werden. Das abschließende Kapitel VI skizziert mögliche Entwicklungstendenzen der Biometrie sowie resultierenden politischen und rechtlichen Handlungsbedarf, benennt vor allem aber – angesichts der insgesamt unbefriedigenden Datenlage und der Begrenztheit der bisherigen Analysen – verbleibenden Untersuchungs- und Forschungsbedarf.

Die Autoren des vorliegenden Berichts sprechen allen Gutachterinnen und Gutachtern ihren herzlichen Dank für die gute Zusammenarbeit aus, ebenso wie Constanze Scherz und Eva Johach, die durch ergänzende Literatur- und Internetrecherchen sowie Unterstützung bei Texterarbeitung und Abbildungserstellung zum Abschluss des Projektes beigetragen haben. Ein Hinweis zu den im Bericht aufgeführten Internetadressen: Deren Aktualität/Gültigkeit wurde Mitte Februar 2002 das letzte Mal überprüft.

II. Biometrie: Merkmale, Verfahren und Systeme

„Biometrie“ bezeichnet – v. a. in Biologie, Medizin, Pharmazie und Mathematik – die Erfassung und (Ver-)Messung von Lebewesen und ihren Eigenschaften. Im vorliegenden Zusammenhang meint Biometrie bzw. Biometrik die (automatisierte) Messung eines individuellen – physiologischen oder verhaltenstypischen – Merkmals einer Person zum Zweck der (biometrischen) Identifikation (bzw. Authentifizierung, s. u.) und damit zur Unterscheidung von anderen Personen (Behrens/Roth 2001, S. 1 f.). Die Begriffe Biometrie, Biometrik und biometrische Identifikation werden häufig synonym verwendet.

Zunehmend wichtige Einsatzfelder biometrischer Identifikationssysteme sind die Überprüfung der Handlungsberechtigung von Personen bei E-Banking- und E-Commerce-Transaktionen und im Rahmen von Zugangskontrollen zu besonders gesicherten Gebäuden, Räumen oder Gebieten (z. B. Flughafenbereiche). Die bislang vorwiegend verwendeten Passwörter oder Chipkarten in Verbindung mit Zahlencodes (PIN = Personal Identification Number), die auf „Wissen und/oder Besitz“ beruhen, weisen – vor allem durch ihre ausufernde Zunahme – Schwächen bzw. Risiken auf, die mit den Wörtern Verlieren – Vergessen – Stehlen anschaulich charakterisiert werden können (Behrens/Roth 2001, S. 1). Ob der Nutzer, der die korrekten Daten liefert, auch der rechtmäßige Inhaber derselben ist, kann von konventionellen Systemen nicht überprüft werden. Durch die individuelle Personengebundenheit und Einmaligkeit der biometrischen Merkmale soll dieses Problem gelöst werden.

Biometrie soll dabei neue Qualitäts-, Komfort- und Sicherheitsdimensionen bei der Personenauthentifizierung erschließen und wird häufig als alternativlose Technologie beschrieben, ohne deren Nutzung eine wirklich umfassende Ausdehnung des elektronischen Handels für Endverbraucher nicht vorstellbar erscheint (beispielhaft: Nolde/Leger 2002).

1. Allgemeines zu biometrischen Verfahren

Prinzipielle Anforderungen an Merkmale und Verfahren

Merkmale des Menschen, ob physiologische (passive) oder verhaltensabhängige (aktive), müssten folgende vier Eigenschaften aufweisen, um „biometrisch optimal genutzt“ werden zu können (Jain et al. 1999, S. 16, nach Behrens/Roth 2001, S. 3):

– Universalität (bei jedem Menschen vorhanden),

– Einzigartigkeit (bei jedem Menschen verschieden),

– Beständigkeit (ohne Veränderungen über die Zeit) und

– Erfassbarkeit (durch ein technisches System quantitativ messbar).

Die biometrischen Verfahren bzw. Systeme wiederum müssen eine Reihe von Kriterien der Praxistauglichkeit erfüllen, u. a. (Behrens/Roth 2001, S. 3; Scheuermann et al. 2000, nach Platanista 2001a)

– technische Umsetzbarkeit (Schnelligkeit, Kompatibilität),

– Robustheit (Wartungsaufwand), Empfindlichkeit (Genauigkeit) und Überwindungsresistenz (Sicherheit),

– ökonomische Machbarkeit (vertretbare Kosten für Betreiber) sowie

– Nutzerfreundlichkeit (Zuverlässigkeit, Einfachheit/Komfort, Hygiene/Gesundheit).

Wie im Weiteren gezeigt wird, genügt keines der derzeit genutzten „biometrischen Merkmale“ (Tabelle 1) bzw. keines der verfügbaren Systeme allen genannten Anforderungen vollständig, zum Teil aus praktischen, zum Teil aus prinzipiellen Gründen. Dennoch sind weltweit zahlreiche Systeme in unterschiedlichen Anwendungskontexten in

Tabelle 1

Derzeit vorrangig genutzte „biometrische Merkmale“ des Menschen

erfasstes Merkmal	gemessene Charakteristik
physiologisch (passiv)	
Fingerbild (Muster der Hautleisten auf der Fingerkuppe)	Verzweigungs- und Endpunkte der Fingerlinien („Minuzien“)
Handgeometrie	Länge, Dicke und Abstand der Finger, Profil der Hand, evtl. Venenmuster
Iris	Muster des Gewebes um die Pupille
Retina	Muster der Blutgefäße im Augenhintergrund
Gesicht	typische geometrische Merkmale des Gesichts (Augen, Kinn, Nase, Mund)
verhaltensabhängig (aktiv)	
Unterschrift (Schreibdynamik)	Schriftbild und Schriftzug, Geschwindigkeit, Druck, Beschleunigung
Handschrift (Schriftsemantik)	(wie Unterschrift, plus:) Syntax des Schriftbildes
Stimme	akustisches Spektrum (teils vorgegebene Wörter)
multimodale/hybride Systeme	
z. B. Gesicht-Mimik-Stimme	akustisches Spektrum und Lippenbewegung

Quelle: Behrens/Roth 2001, S. 4; Platanista 2001a

Betrieb (Kapitel IV.1). Ökonomisch bislang am erfolgreichsten sind die Erkennung von Fingerbild, Handgeometrie, Gesicht, Stimme, Iris und Unter-/Handschrift (Kapitel IV.2).

Grundlegende Begriffe: Enrolment – Template – Verifikation – Identifikation

Basis eines jeden biometrischen Verfahrens ist – unabhängig von dem genutzten Merkmal und der angewandten Technik – das so genannte Enrolment. Es umfasst das erstmalige Erfassen und (Ver-)Messen des biometrischen Merkmals der zukünftigen Nutzer, die Umwandlung der „Rohdaten“ in einen Referenzdatensatz und die Speicherung desselben, des so genannten Templates. Dieses stellt den Vergleichswert dar, mit dem bei allen darauf folgenden biometrischen Überprüfungen die neuen Messdaten (zumindest zu einem hohen Grad) übereinstimmen müssen, um den Nutzer identifizieren zu können (s. u.).

An diesen grundlegenden Vorgang des Enrolments müssen folglich sowohl höchste technische Anforderungen (bzgl. Empfindlichkeit und Genauigkeit, damit tatsächlich individuelle, aber auch reproduzierbare Datensätze entstehen) als auch höchste Sicherheitsanforderungen gestellt werden. Der Hauptzweck der Anwendung biometrischer Verfahren, d. i. die Erhöhung der Sicherheit eines Gesamtsystems (z. B. der Geldausgabe am Automaten), kann nur dann erreicht werden, wenn der Referenzdatensatz, das Template, dauerhaft geschützt gespeichert werden kann. Insbesondere im Hinblick auf zukünftige großflächige Einsätze sind noch viele Fragen offen (z. B. welche und wie viele Personen entsprechend qualifiziert werden müssen, um das Enrolment durchzuführen), deren Lösung aller Voraussicht nach mit hohem finanziellen und organisatorischen Aufwand verbunden sein wird (Platanista 2001a; vgl. Kapitel IV.1.6).

Bei einer biometrischen Überprüfung der Nutzer werden zwei „Betriebsarten“ unterschieden (Behrens/Roth 2001, S. 2):

– die biometrische Verifikation, d. h. die Bestätigung der behaupteten Identität des Individuums (1:1 = die vermessene Person ist tatsächlich die, die sie zu sein behauptet) und

– die biometrische Identifikation, d. h. die Erkennung eines Individuums aus einer (definierten) Menge biometrisch registrierter Personen (1:n = die vermessene Person ist XY).

Im Fall der Verifikation werden die aktuellen Messdaten verglichen mit den vorhandenen Daten der Einzelperson, die z. B. auf einer Chipkarte oder einem PDA (Personal Digital Assistant) dezentral (im Besitz der Person) abgelegt sind oder aber, verbunden mit einer vorgegebenen Benutzerkennung, zentral gespeichert sein können. Im Rahmen des Enrolments – z. B. bei einem großflächigen

Einsatz für Bankautomaten – wird es oftmals nötig sein, zumindest vorübergehend die biometrischen Daten an einer weiteren zentralen Stelle abzuspeichern, um sie auf die Chipkarte für den entsprechenden Benutzer zu laden („Personalisierung der Chipkarten"). Dem Vorteil aus der Sicht des Datenschutzes, dass sich bei einer dezentralen Verifikation das Template in der Verfügungsgewalt der Nutzer befindet, stehen Sicherheitsnachteile und damit verbundene mögliche Haftungsprobleme durch Verlust oder Beschädigung gegenüber (Platanista 2001a; vgl. Kapitel V.2).

Im Fall der Identifikation vergleicht das biometrische System die gemessenen Daten mit den – zentral gespeicherten – Daten aller zuvor Registrierten und prüft, welches Template am besten mit dem des aktuellen Nutzers übereinstimmt. Dadurch entstehen höhere Anforderungen hinsichtlich der benötigten Datenbankgröße und Identifikationszeit. Diese Art der biometrischen Erkennung wird derzeit vor allem in Hochsicherheitsbereichen mit einer geringen Anwenderanzahl oder zu polizeilichen Ermittlungszwecken eingesetzt (Platanista 2001a).

Als Oberbegriff gilt (biometrische Personen-)Authentifizierung/Authentifikation, der sich jedoch im deutschen Sprachraum – zumindest bislang noch – nicht durchgesetzt hat (Nolde/Leger 2002), sodass meist allgemein von „biometrischer Personenidenfikation" gesprochen wird, auch wenn lediglich eine Verifizierung stattfindet. Begrifflich abzusetzen ist die Autorisierung (als eigentliches Ergebnis der Überprüfung der Identität des Nutzers), also die Ermächtigung bzw. Bevollmächtigung für einen Zugang oder für eine Handlung (TeleTrust 1998, S. 4).

Probleme in der Praxis: Falsche Akzeptanz und falsche Zurückweisung

Idealerweise wäre jeder gewonnene biometrische Datensatz einzigartig für ein menschliches Individuum und diesem eindeutig zuzuordnen – ursprünglich erhobene Referenzdaten (Template) und jeweils gemessener Datensatz wären identisch. In der Praxis resultieren Einschränkungen dieser idealen Einzigartigkeit, Genauigkeit und Reproduzierbarkeit aus verschiedenen Gründen:

– Jeder Messvorgang bedeutet eine starke Informationsreduktion. Aus prinzipiellen (Kapazitäts-)Gründen muss die erhobene Datenmenge begrenzt werden. Hinzu kommt die jeweilige Messgrenze (Empfindlichkeit) und Genauigkeit des Sensors bzw. des Gesamtsystems sowie das nicht zu vermeidende „Rauschen". Die zu speichernde Datenmenge des Templates sollte aus technischen Gründen (Speichergröße, Übertragungsraten) weitestgehend minimiert werden, wodurch aber die Genauigkeit reduziert wird.

– Verhaltensabhängige Merkmale weisen aufgrund der Natur der menschlichen Motorik immer eine mehr oder weniger große Varianz auf. Doch auch physiologische Merkmale sind nur eingeschränkt zeitlich konstant. Sie können durch Alterungsprozesse, Krankheiten oder Verletzungen vorübergehend oder dauerhaft verändert werden. Leichte Veränderungen müssen daher sowohl bei „aktiven" als auch bei „passiven" Verfahren vom System toleriert werden.

– Hinzu kommen störende Umwelteinwirkungen während der Messung, z. B. unterschiedliche Lichtverhältnisse oder Temperaturveränderungen, welche die Leistungsfähigkeit von Sensoren beeinflussen können (Platanista 2001a).

Mit dem biometrischen System wird ein statistischer Vergleich der Datensätze von Template und Messung durchgeführt. Das Ergebnis benennt einen prozentualen Wert der Übereinstimmung. Eine hundertprozentige Übereinstimmung wird sowohl aus den genannten prinzipiellen technischen und physiologischen als auch aus den situationsbedingten Einschränkungen praktisch nie vorkommen. Für jedes System muss daher eine Schwelle (ein Wert für den Grad der Übereinstimmung von Referenz- und Messwert) definiert werden (z. B. 95 %), ab der Identifikation bzw. Verifikation als erfolgt betrachtet werden und der Nutzer als berechtigt akzeptiert wird. Diese Toleranzschwelle hat großen Einfluss darauf, wie viele Nutzer entweder fälschlicherweise akzeptiert werden oder aber fälschlicherweise zurückgewiesen werden (bzw. gezwungen sind, den Vorgang mehrfach zu wiederholen). Die Raten falscher Ablehnung bzw. falscher Akzeptanz eines biometrischen Systems (FRR = False Rejection Rate; FAR = False Acceptance Rate) können nicht theoretisch berechnet werden, sondern müssen empirisch ermittelt werden.

FAR und FRR beeinflussen sich dergestalt, dass eine Absenkung der falschen Akzeptanz die falsche Zurückweisung erhöht und umgekehrt. Die absolute Höhe der Fehlerraten ist allerdings abhängig von der Empfindlichkeit und Genauigkeit, also der Trennschärfe, des Gesamtsystems und wird daher von der Wahl der o. g. Toleranzschwelle direkt beeinflusst. Weniger präzise Systeme wie die Stimmerkennung werden entweder viele Nutzer fälschlicherweise akzeptieren (bei niedrig eingestellter Toleranzschwelle) oder aber fälschlicherweise zurückweisen. Der Iris-Scan hingegen weist aufgrund seiner großen Trennschärfe sowohl eine niedrige FAR als auch eine niedrige FRR auf. Je nach praktischer Anwendung soll durch die Wahl und Einstellung der Toleranzschwelle des Systems die Rate falscher Ablehnung minimiert werden (meist aus Komfortgründen, d. h. Vermeidung frustrierender Fehlversuche) oder aber die Rate falscher Akzeptanz (vor allem im Hinblick auf eine Sicherheitserhöhung) (Kapitel IV.1.5). FAR und FRR gelten als mit die wichtigsten Kenngrößen für die Leistungsfähigkeit eines biometrischen Systems. Bei Gleichheit der Werte spricht man von EER = Equal Error Rate.

Ein selbst in Testszenarien bislang selten behandelter, für die Praxis aber sehr wichtiger weiterer Parameter ist die Rate fehlerhafter Registrierungs- bzw. Enrolmentversuche (FER = False Enrolment Rate), die großen Einfluss auf die Nutzerakzeptanz ausüben kann (Vielhauer 2000).

2. Biometrische Systeme im Einzelnen

Die folgenden (Kurz-)Beschreibungen der biometrischen Merkmale und Systeme behandeln physiologische,

technische, ökonomische und Nutzeraspekte. Eine Gegenüberstellung der Eigenschaften und Kenngrößen der Verfahren (FAR und FRR, Registrierungs- und Verifikationszeit, Templategröße), ihrer Stärken und Schwächen wird in Kapitel II.3 vorgenommen.

2.1 Fingerbild

Die Fingerbilder jedes Menschen gelten als völlig einzigartig. Selbst eineiige Zwillinge können anhand der Fingerabdrücke unterschieden werden. Zur Unterscheidung werden entweder das gesamte Graubild („Pattern Matching“) oder die so genannten Minuzien („Kleinigkeiten“; hier: endende Täler, Verzweigungen, Schweißporen der Fingeroberfläche) herangezogen. Die letztgenannte Methode wird von der Mehrzahl der Hersteller von Fingerbilderkennungssystemen genutzt. In beiden Fällen werden vergleichbare Sicherheitswerte erreicht; die Verifikationszeit kann jedoch beim Pattern Matching etwas länger sein. Bei dieser Methode sind die Templates häufig um den Faktor zwei bis drei größer, zurzeit typischerweise etwa 900 bis 1 200 Bytes pro Fingerbild (Behrens/Roth 2001, S. 6).

Bei der kriminaltechnischen (forensischen) Verarbeitung der Fingerabdrücke geht es im Unterschied zu den biometrischen Fingerbild-Erkennungen um die Erfassung der Gesamtbilder, vor allem zu Vergleichszwecken. Das bedeutet, dass die von den Scannern erfassten Bilder als hochwertige Schwarz-Weiß-Bilder mit z. B. 250 KByte (pro Finger!) gespeichert werden, während für die biometrische Identifikation Datensätze verwendet werden, die um den Faktor 250 bis 1 000 kleiner sind und sich auf die zur Unterscheidung benötigten Merkmale reduzieren. Daher kann bei einer biometrischen Identifikation der Fingerabdruck aus den gespeicherten Daten nicht eindeutig rekonstruiert werden, was eine Verwendung vor Gericht kaum möglich macht (Behrens/Roth 2001, S. 10).

Abbildung 1 demonstriert die Gewinnung der biometrischen Fingerbildinformation, des so genannten Minuzienbildes. Die einzelnen Schritte sind (Behrens/Roth 2001, S. 8):

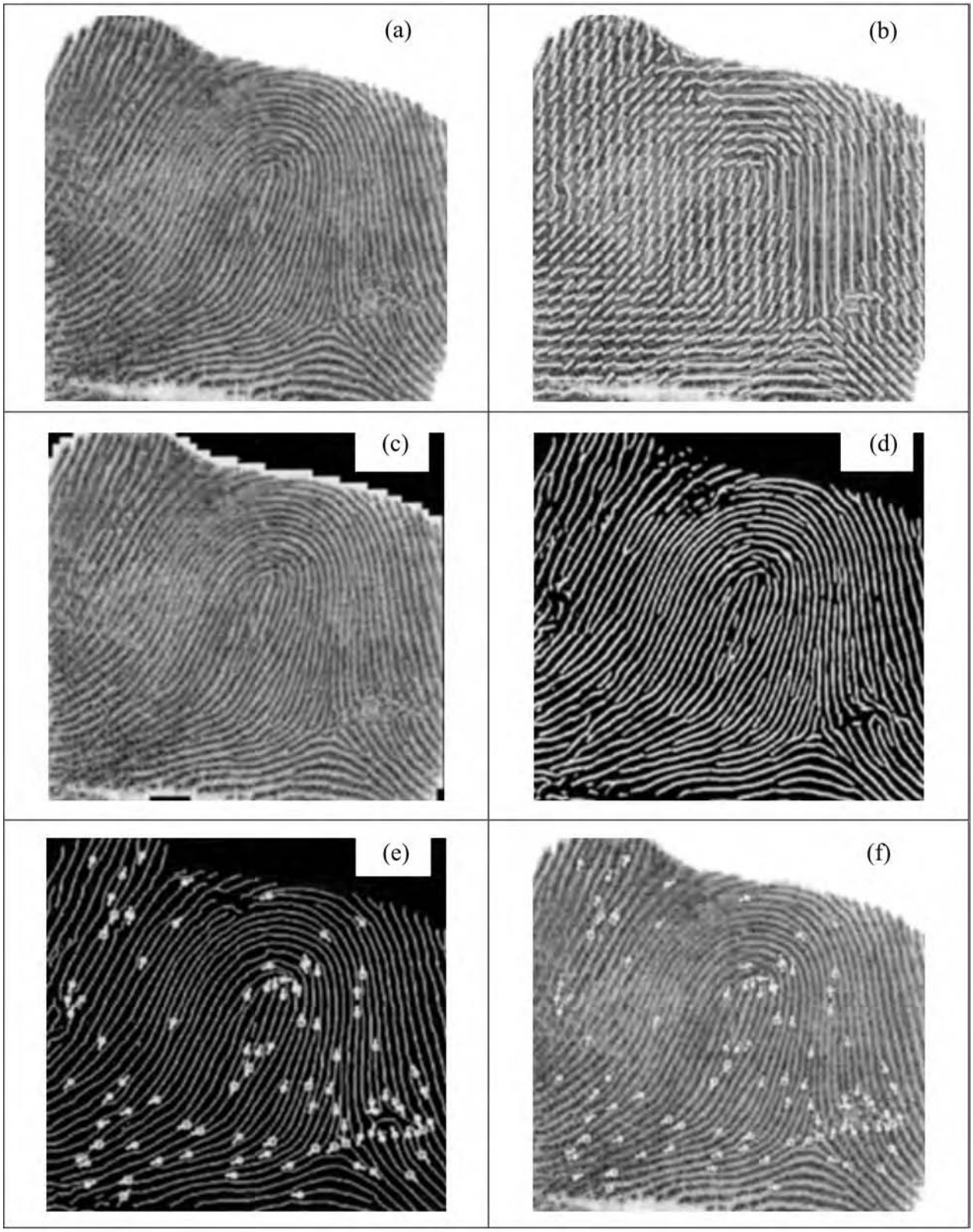
- Gewinnung des Original-Graustufenbildes des Fingers (a),
- Berechnung des Richtungsfeldes aus dem Originalbild (b),
- Extraktion des Vordergrundanteils (c),
- Herausfilterung des Hintergrundes (d),
- Berechnung des Skelettes mit den markierten Minuzien (e),
- Überlagerung der Minuzien mit dem Original-Graustufenbild (f).

Derzeit sind drei Technologien im Gebrauch bzw. in der Erprobung: optische Sensoren, Halbleiterlösungen und Ultraschall (Behrens/Roth 2001, S. 6 f.).

- Lösungen mit optischen Sensoren haben sich in der Vergangenheit zwar durchaus bewährt, sind aber wenig verbreitet. Sie bestehen aus einer Kamera, zumeist in Form eines CCD-(Charged Coupled Device)Sensors, einer Prismenoptik und einer Hartplastik- oder Glasfläche als Auflagefläche für den Finger in definiertem Kameraabstand. Anstelle von sichtbarem Licht kann auch Infrarot benutzt werden. Die Auflösung ist mit bis zu 500 dpi (dot per inch) und aufgrund relativ großer nutzbarer Auflagefläche oft deutlich besser als bei den u. g. Halbleiterlösungen. Auch sind die optischen Sensoren in einem weiten Bereich unempfindlich gegen Temperaturschwankungen und elektrostatische Aufladung. Schwierigkeiten gibt es allerdings durch latente Fingerabdrücke aus der vorhergehenden Benutzung. Bei verschiedenen Modellen besteht auch die Gefahr eines Leistungsabfalls infolge der Alterung des CCD-Chips, Ausfall der Beleuchtung oder durch Beschädigung der Oberfläche der Aufnahmefläche.
- Immer wichtiger wird die Halbleiterlösung (kapazitative Sensoren). Seit einiger Zeit sind Chips verfügbar, die mittels Messung der Gleichstromkapazität zwischen der Chipoberfläche und der Fingeroberfläche digitale Graustufenbilder mit 200 bis 300 Linien – bei einer nutzbaren Fläche von ca. 10 x 15 mm bis max. 13 x 18 mm – mit 8-Bit-Auflösung erzielen (Infineon, Sony, ST-Microelectronics, Veridicom). Ein System (des Herstellers Authentec) kann durch eine modifizierte Kapazitätsmessung auch die lebende Schicht des Fingers unter der Oberfläche vermessen, was theoretisch deutliche Vorteile hat, da sich zum Beispiel Verletzungen weniger auswirken. Mit latenten Fingerabdrücken aus der vorhergehenden Benutzung kämpfen allerdings auch viele der Halbleiterlösungen, und wie haltbar und zuverlässig sie sind, ist noch offen. Die Angaben der Hersteller sind viel versprechend, indem sie eine hundertfach bessere Haltbarkeit als bei den optischen Systemen behaupten. Charakteristisch ist eine, durch die relativ kleine Aufnahmefläche bedingte, sehr große Abhängigkeit der Gesamtqualität der Erkennung von der Qualität des Enrolments. Der Benutzer muss immer die gleiche Teilfläche des Fingers wie beim Enrolment benutzen, was eine unrealistische Disziplin des Nutzers erfordert, der oft schon Schwierigkeiten hat, sich daran zu erinnern, welchen Finger er beim Enrolment benutzt hat. Chips zur Fingerbilderfassung werden zukünftig weitaus preiswerter sein und vermutlich immer häufiger eingesetzt werden. Schon jetzt sind sie in Smartcards integriert verfügbar.
- Große Hoffnung wird auf die Verwendung von Ultraschalltechnologie gesetzt, wenn auch nur wenige Geräte bisher Marktreife erreicht haben (http://www.ultra-scan.com). Vorteilhaft ist, dass Schmutz oder Rückstände (latente Fingerabdrücke) keine Rolle spielen, da der akustische Widerstand der Haut (Kanten, Senken usw.) gemessen wird, und eine große Aufnahmefläche wie bei optischen Systemen möglich ist. Die Überlistung derartiger Sensoren dürfte schwieriger sein. Über die Langzeitleistungsfähigkeit ist bisher allerdings wenig bekannt.

Abbildung 1

Gewinnung des Minuzienbildes bei der Fingerbilderkennung



Quelle: Behrens/Roth 2001, S. 9, nach GMD/Infineon Technologie AG

Ein so genannter Life-Test (Lebenderkennung) wird bisher nur von wenigen Herstellern angeboten. Damit soll verhindert werden, dass bei optischen Sensoren mit einer Fingerprofilattrappe oder einem abgeschnittenen Finger eine Authentifizierung erzielt werden kann. Ansätze für solch eine Lebenderkennung sind die Messung des Fingerpulses oder die Erfassung der Farbe der Haut, ihrer elektrischen Eigenschaften oder ihrer Reflexionseigenschaften (Behrens/Roth 2001, S. 7).

Für die Nutzer ist die Fingerbilderkennung recht einfach und bequem handhabbar. Allerdings wird vermutet, dass die Assoziation des „traditionellen" Einsatzes im Rahmen der Strafverfolgung bei Nutzern zu Vorbehalten führen kann (Platanista 2001a). Hinzu kommen hygienische Bedenken bei Verwendung im öffentlichen Bereich.

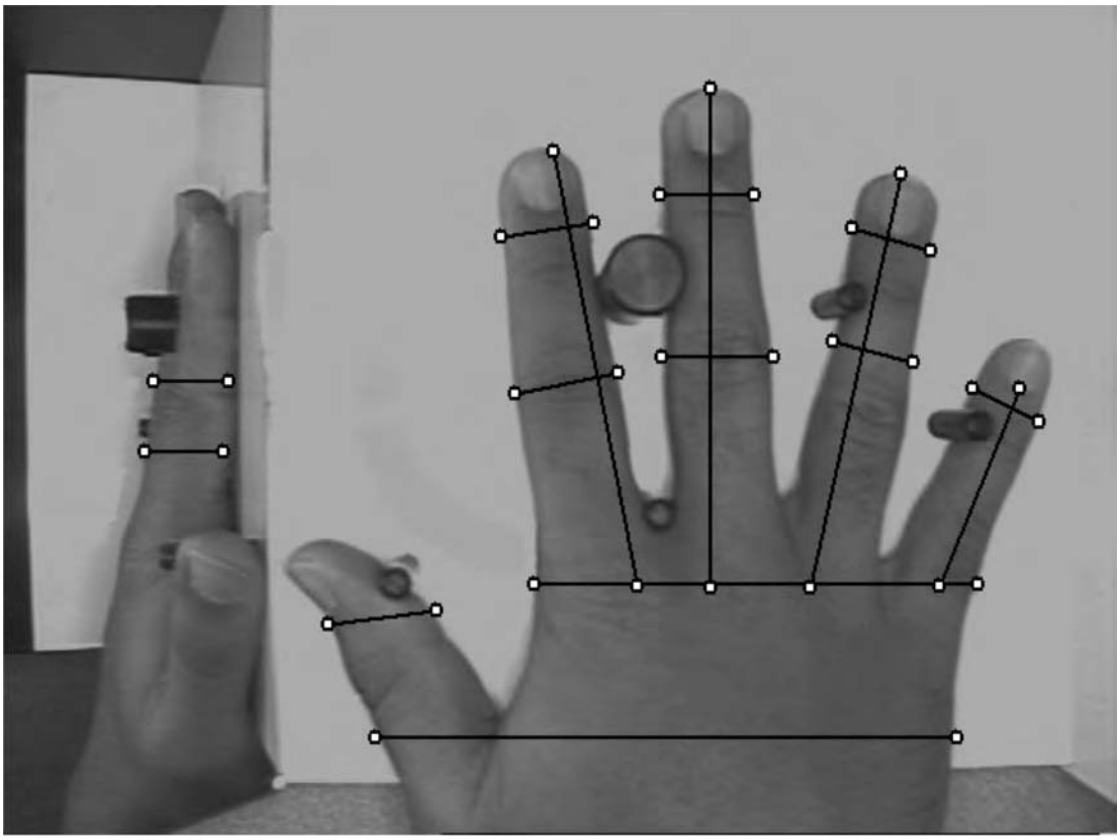
2.2 Handgeometrie

Die Erfassung der Handgeometrie ist eines der ältesten biometrischen Verfahren. Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Bereits der Schatten einer Hand gilt als einzigartig. Für die biometrische Vermessung werden bis zu 90 Werte für Dicke, Länge, Breite und Fläche der Hand bzw. der Finger ermittelt (Abbildung 2). Theoretisch nutzbare Charakteristiken der Handoberfläche, wie die Verteilung der Hautporen, werden bislang nicht herangezogen (Behrens/Roth 2001, S. 12).

Die Bedienung der Systeme ist einfach, teilweise aber unbequem (wenn z. B. für die richtige Positionierung die Hand fest an starre Anschlagstifte gedrückt werden muss, Abbildung 2). Da aufgrund der Dickenmessung dreidimensionale Aufnahmen benötigt werden, sind komplizierte Optiken erforderlich. Die Sensortechnik und mit ihr das Gesamtsystem ist daher meist recht voluminös, sodass die Technik bislang überwiegend bei der räumlichen Zugangskontrolle oder zur Zeiterfassung eingesetzt wurde. Die Templategröße ist mit 10 bis 20 Bytes klein, Angaben zur erzielbaren Genauigkeit schwanken (mittel bis hoch) (Behrens/Roth 2001, S. 12). Ein Life-Test zur Erhöhung der Überwindungssicherheit wird – wie bei der Fingerbilderkennung – bislang kaum angeboten.

Abbildung 2

Erfassen der Handgeometrie



Quelle: Michigan State University (http://biometrics.cse.msu.edu/hand-proto.html), nach Behrens/Roth 2001, S. 12

2.3 Iris

Die Iris oder „Regenbogenhaut“ ist der farbige Gewebering, der die Pupille umschließt. Sie regelt wie eine Blende die Weite der Pupille und damit den Lichteinfall. Die charakteristischen, biometrisch nutzbaren Merkmale der Iris werden als Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen und Streifen bezeichnet (Abbildung 3). Die Farbe wird nicht berücksichtigt.

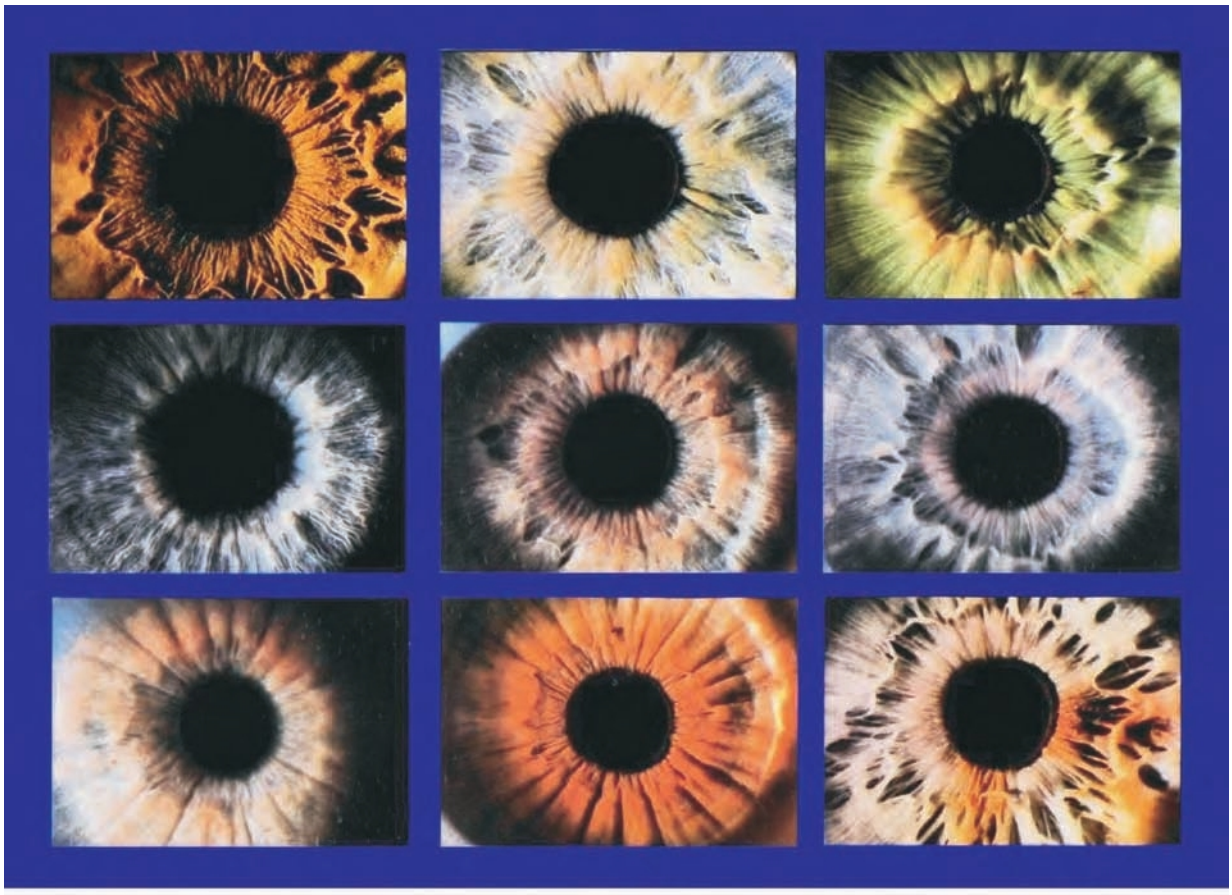
Die Einzigartigkeit von Irismustern ist unbestritten. Sie gilt nicht nur für eineiige Zwillinge, sondern sogar für die zwei Augen einer Person. Veränderungen über die Zeit werden als vernachlässigbar eingestuft. Allerdings können Krankheiten des Auges, z. B. Schädigungen der Hornhaut, zu deutlichen Veränderungen führen, was eine neue Registrierung erforderlich macht (Behrens/Roth 2001, S. 14).

Zur Erfassung der Irismuster werden Schwarz-Weiß-CCD-Kameras eingesetzt, ähnlich handelsüblichen Videokameras. Laser finden keine Verwendung. Die Aufnahme kann „aktiv“ oder „passiv“ erfolgen. Im zweiten Fall müssen die Nutzer in einem Abstand zwischen 15 und 35 cm von der Aufnahmeeinrichtung – gegebenenfalls geleitet von einer Sprachausgabe – eine passende Position zur Kameralinse einnehmen. Bei der „aktiven“ Aufnahme findet eine motorisch bewegte Weitwinkel-Kamera mit Hilfe von Stereoaufnahmen des Gesichtes selbstständig die Iris. Mit 30 bis 100 cm ist der Abstand deutlich benutzerfreundlicher (Behrens/Roth 2001, S. 14). Das Template hat typischerweise eine Größenordnung von 512 Bytes (Abbildung 4).

Der Iris-Scan gilt als eines der genauesten biometrischen Identifikationsverfahren (Kapitel III.1.1) und wird bereits vielfach bei Zugangskontrollen im Hochsicherheitsbereich

Abbildung 3

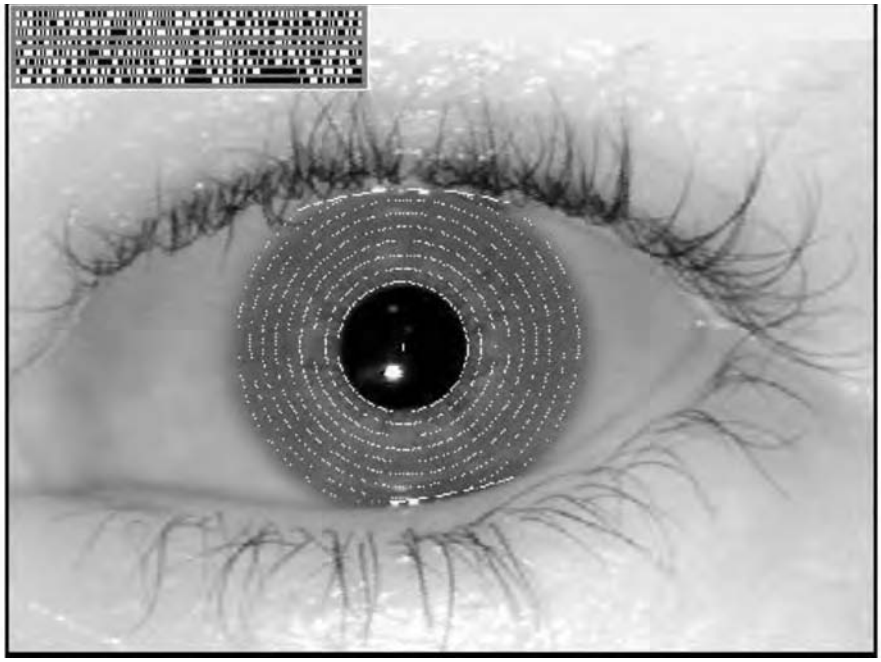
Iris-Muster



Quelle: Fa. Iridian (http://www.iridiantech.com), nach Behrens/Roth 2001, S. 14

Abbildung 4

Iris mit Iris-Code



Quelle: Fa. Iridian (http://www.iridiantech.com), nach Behrens/Roth 2001, S. 17

verwendet, mehrere Pilotanwendungen bei Geldautomaten sind bekannt. Eine Lebenderkennung (z. B. durch Erfassung der Pupillenbewegung und der damit einhergehenden kontinuierlichen elastischen Verformung der Irisstruktur) kann die ohnehin hohe Überwindungssicherheit noch weiter steigern (Breitenstein 2002, S. 50). Einem verbreiteteren Einsatz stehen derzeit noch die hohen Anschaffungskosten entgegen, die allerdings bei einer Steigerung der Produktion wohl deutlich gesenkt werden könnten (Behrens/Roth 2001, S. 16). Die Nutzerakzeptanz gilt als eher verhalten, da häufig die Befürchtung von Augenschäden geäußert wird (Platanista 2001a), in der fälschlichen, aber nach wie vor verbreiteten Annahme, dass ein Laser eingesetzt werde (Breitenstein 2002, S. 51).

2.4 Retina

Wie das Fleckenmuster der Iris gilt auch die Anordnung der Blutgefäße in bzw. hinter der Netzhaut oder Retina, also dem lichtempfindlichen Bereich im Augeninneren, als individuell einzigartig (auch bei Zwillingen). Ebenfalls wie das Irismuster bleibt das Adernmuster der Netzhaut weitgehend konstant, kann sich aber durch Krankheiten oder Verletzungen vorübergehend oder andauernd verändern.

Seit 1985 gibt es (mit dem EyeDentify 7.5) ein Gerät, das mittels Infrarot-Laser die Blutgefäße der Netzhaut scannt. Dabei werden etwa 400 charakteristische Punkte festgehalten (Abbildung 5). Relativ aufwendige Spezialtechnik ist erforderlich, um durch die Pupille hindurch die Netzhaut aufzunehmen. Das Auge muss sich sehr nahe an der Aufnahmeoptik befinden (1 bis 2 cm) und während des Scannens ruhig gehalten werden. Der Nutzer blickt dann auf ein rotierendes grünes Licht, während das tatsächlich zum Abtasten benutzte Infrarotlicht für ihn unsichtbar ist. Die Templates sind mit 40 bis 96 Bytes mittelgroß. Die Zeit für eine Messung beträgt ca. 1,5 Sekunden (Behrens/Roth 2001, S. 17 f.).

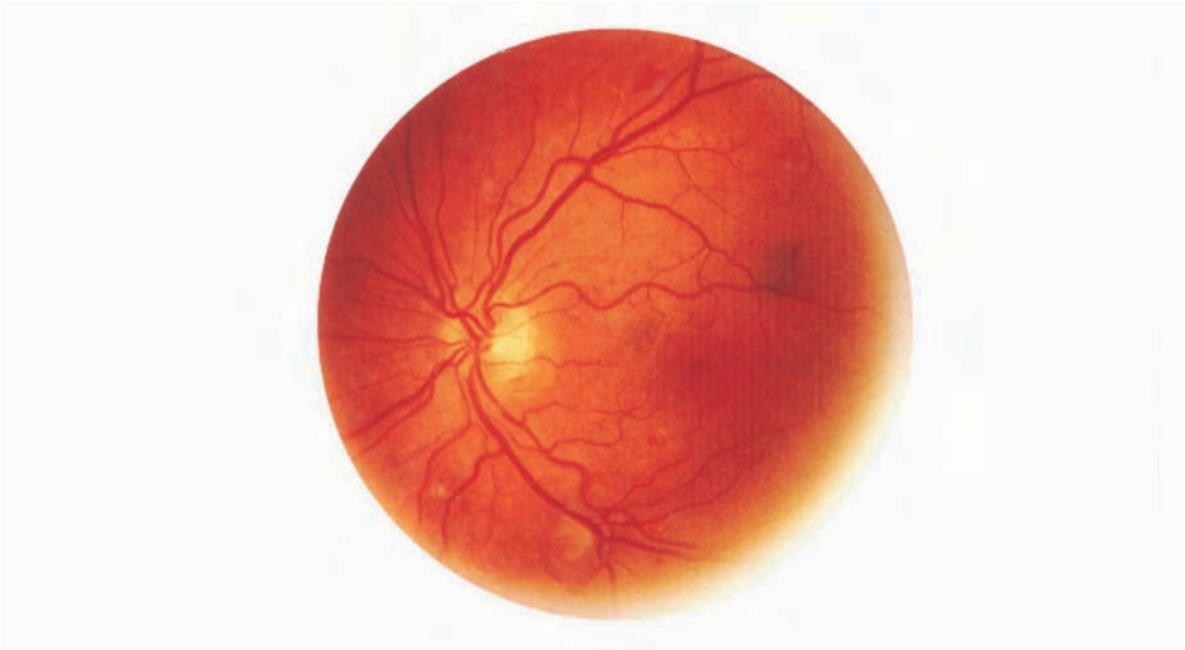
Wie der Iris-Scan hat der Retina-Scan als sehr empfindliches Verfahren bei der Zutrittssicherung zu Hochsicherheitseinrichtungen sowohl im öffentlichen als auch im privaten Bereich Verbreitung gefunden (Behrens/Roth 2001, S. 18). Eine Überlistung des Systems durch Attrappen wird kaum für möglich gehalten (Breitenstein 2002, S. 54). Nicht nur der hohe Preis, sondern auch die bislang recht hohe Rückweisungsrate (von ca. 12 % beim ersten Versuch lt. Herstellerangabe) stellten ein Verbreitungshemmnis dar. Hinzu kommen Nutzervorbehalte, da eine Verursachung von Augenschäden durch den Laser befürchtet wird, auch wenn es hierfür bislang keinerlei Hinweise gibt. Konkrete Einschränkungen der Nutzbarkeit ergeben sich für Träger von Kontaktlinsen (ab einer bestimmten Dioptrienzahl), außerdem gibt es Probleme bei Astigmatismus (Hornhautverkrümmung, eine recht häufige Ursache für Fehlsichtigkeit).

2.5 Gesicht

Für die Gesichtserkennung existieren verschiedene Methoden und Systeme. Die meisten analysieren diejenigen Bereiche des Gesichtes, die sich nicht aufgrund der Mimik ständig verändern (Behrens/Roth 2001, S. 19). Dazu

Abbildung 5

Infrarot-belichtete Retina



Quelle: Fa. EyeDentify (http://www.eyedentify.com), nach Behrens/Roth 2001, S. 18

gehören die oberen Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes. Die zwei wichtigsten Systeme sind die Eigengesichts- und die Eigenschaftsanalyse.

Bei der Eigengesichtstechnik handelt es sich um ein ursprünglich vom Massachusetts Institute of Technology (MIT) entwickeltes Verfahren, das in zweidimensionalen Graustufenbildern die Charakteristika des Gesichts abbildet (Abbildung 6). 100 bis 125 Eigenbilder sind bei der Mehrheit der Gesichter nötig, um die jeweils typischen Eigenschaften zu erfassen. Wie bei allen Gesichtserkennungssystemen ist der Betrachtungswinkel und der Detailreichtum wichtig. Die besten Ergebnisse werden bei frontaler Bildaufnahme erzielt (Behrens/Roth 2001, S. 21). Diese Gesichtserkennungstechnik wird oft in Kombination mit weiteren biometrischen Verfahren benutzt.

Eigenschaftsanalyse (Feature analysis) ist das wohl verbreitetste System zur Gesichtserkennung. Gegenüber dem Eigengesicht-Verfahren gilt die Methode als vielseitiger, da sie Variationen der Mimik, etwa beim Sprechen oder Lächeln, akzeptiert (Behrens/Roth 2001, S. 21).

Neben diesen beiden dominierenden Systemen gibt es eine Reihe weiterer Varianten, die als Neural Network Mapping Technology oder Automatic Face Processing bezeichnet werden, ferner erste Versuche zur Nutzung anderer Parameter, wie dreidimensionales Scannen oder das Erfassen der Wärmeverteilung im Gesicht (Abbildung 7) (Behrens/Roth 2001, S. 21 f.).

Äußere Einflüsse, z. B. unterschiedliche Lichtverhältnisse oder Temperaturschwankungen, beeinflussen die Funktionalität der Gesichtserkennung. Ohne Lebenderkennung (z. B. durch Registrierung intrinsischer Mund- oder Augenbewegungen) ist die Überwindung der Systeme äußerst einfach – meist genügen bereits Fotos oder Videos (Breitenstein 2002, S. 45). Vor allem bei Kindern und Jugendlichen, aber auch in späteren Lebensphasen verändert sich das Merkmal relativ stark (Platanista 2001a). Die Templategröße beträgt bis zu 1.300 Bytes.

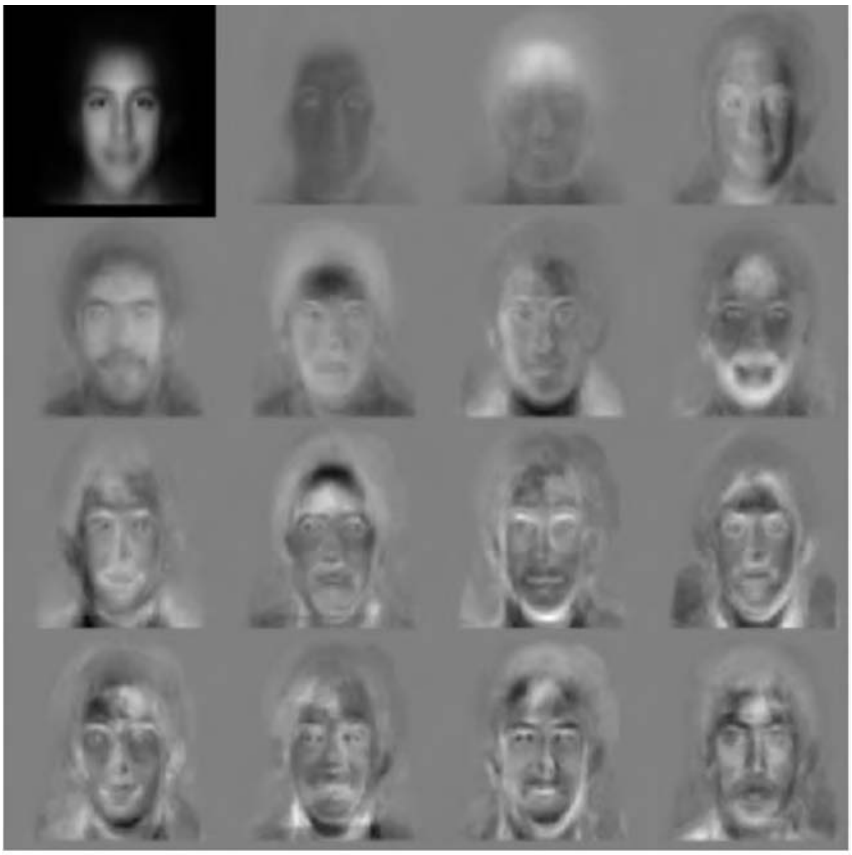
Je nach Anwendungszweck und Perspektive (z. B. Komfort vs. Datenschutz) erscheinen zwei Charakteristika der Gesichtserkennung als Vor- oder Nachteil: die Passivität der Nutzer (keine aktive Mitwirkung erforderlich) und die mögliche Kontinuität gegenüber einem Nutzer (permanente Überprüfung der Zugangsberechtigung z. B. während der Benutzung eines PCs).

2.6 Unter-/Handschrift

Bei der Unterschrifts- bzw. Handschriftenerkennung ist nicht nur das optische Erscheinungsbild der Signatur (Schriftzug als „Offline-Parameter“) entscheidend, sondern es werden Merkmale wie Druck, Geschwindigkeit, Beschleunigung, Auf- und Absetzpunkte sowie Stiftwinkelpositionen beim Schreiben (als „Online-Parameter“) gemessen. Aufgenommen wird die Unter-/Handschrift heute meistens mit einem handelsüblichen Grafiktablett oder einem PDA bzw. Touchscreen. Alternativ sind auch Spezialstifte mit Sensoren in Verwendung, welche die

Abbildung 6

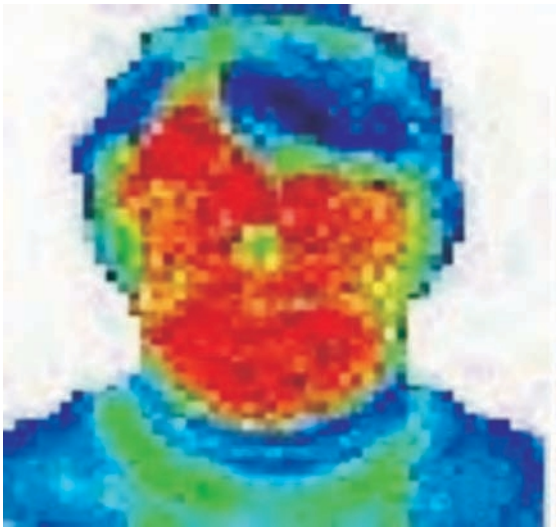
Einzelbilder der Eigengesichtstechnik



Quelle: MIT Face Recognition Demo Page, nach Behrens/Roth 2001, S. 21

Abbildung 7

Thermogramm eines Gesichts



Quelle: Michigan State University (http://biometrics.cse.msu.edu/), nach Behrens/Roth 2001, S. 22

Parameter bei der Leistung der Unter-/Handschrift aufnehmen und zur Auswertung übertragen (Behrens/Roth 2001, S. 22 f.).

Eine Erweiterung der Unterschriftanalyse liefert ein Handschriftensystem, bei welchem nicht allein die Unterschrift, sondern so genannte „Semantiken“ (Vielhauer 2000) zur handschriftlichen Authentifizierung herangezogen werden. Dies können vordefinierte Wörter, ganze Sätze oder sogar kleine Zeichnungen (Sketches) sein (Abbildung 8). Ein Vorteil des Einsatzes von „Semantiken“ liegt in der Anonymität – selbst bei zentral abgespeicherten Datensätzen kann diese gewahrt werden. Die Verfahren können so eingerichtet werden, dass sie vom Nutzer selbst gesteuert werden können, indem der hinterlegte Referenzdatensatz relativ kurzfristig verändert wird. Hierdurch ist eine klarere Koppelung an eine Willenserklärung möglich. Die „Beherrschbarkeit“ durch den Nutzer dürfte außerdem förderlich für die Akzeptanz sein. Da die Erfassung der dynamischen Parameter eine Lebenderkennung darstellt, ist die Fälschungssicherheit ziemlich hoch (Breitenstein 2002, S. 58 f.). Wegen der (noch) hohen Fehlerraten sind die Systeme bislang allerdings nur sehr eingeschränkt einsetzbar (Platanista 2001a).

2.7 Stimme

Es existieren verschiedene Methoden bzw. Verfahren zur Analyse von personenbezogenen Sprachmustern. Erfasst werden unterschiedliche Parameter der Sprechcharakteristik, so die Tonhöhe, die Dynamik oder die Wellenform. Die Templategröße liegt in der Regel zwischen 1 500 bis 3 000 Bytes (Behrens/Roth 2001, S. 23). Grundsätzlich ist die Sprechererkennung, verglichen mit anderen biometrischen Systemen, ein weniger genaues Verfahren. Sprachsysteme sind anfällig für äußere Einwirkungen, z. B. Straßengeräusche oder laute Unterhaltungen, und bei (Hals-)Erkrankungen häufig nicht einsetzbar. Hinzu kommt die prinzipiell simple Überwindbarkeit durch Stimmaufnahmen (Platanista 2001a). Trotz dieser Nachteile ergibt sich insbesondere im Bereich der Telekommunikation ein interessantes Anwendungsspektrum, da hier keine zusätzlichen Hardwarekosten für die Nutzer entstehen.

2.8 Kombinationen

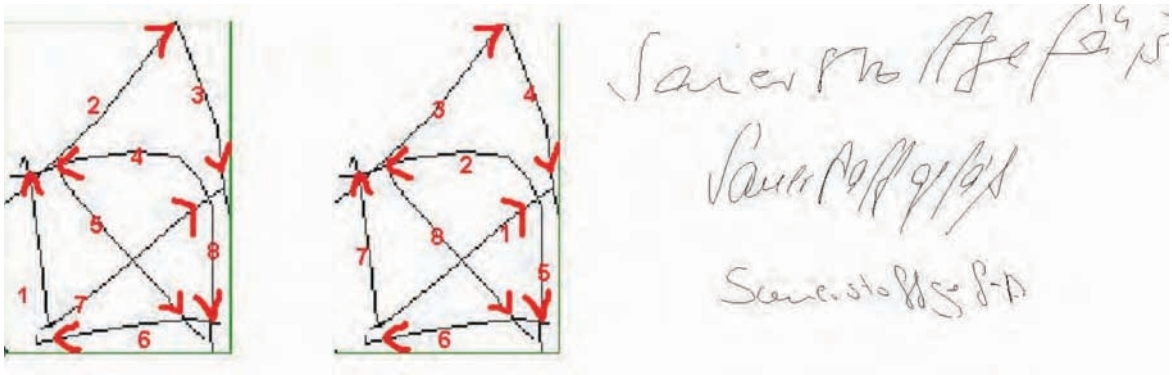
Die Voraussetzung für die Anwendung einer Kombination verschiedener biometrischer Authentifizierungssysteme (auch von verschiedenen Herstellern) ist eine standardisierte Schnittstelle, ein so genanntes Application Programming Interface (API). Die Entwicklung eines solchen „BioAPI“ und eine entsprechende internationale Vereinbarung stehen kurz vor ihrem Abschluss (Kapitel III.1.3) Damit rücken multimodale Systeme näher, die eine größere Genauigkeit und Zuverlässigkeit (bezüglich der FRR) als Einzelverfahren versprechen. Einen entscheidenden Vorteil könnten multimodale Systeme vor allem dann bieten, wenn bei einem Nutzer ein bestimmtes biometrisches Merkmal aktuell oder generell nicht messbar ist, da dann auf ein anderes Merkmal „ausgewichen“ werden kann. Nachteilig ist das aufwendigere Enrolment einschließlich der Speicherung einer größeren Datenmenge, wodurch auch die Authentifizierungsvorgänge zeit- und kostenintensiver werden dürften (Platanista 2001a). Bereits in der Erprobung befindet sich ein kombiniertes System von Stimm- und Gesichtserkennung einschließlich der Lippenbewegung (BioID der Firma DCS) (Behrens/Roth 2001, S. 23).

2.9 Entwicklungslinien im Frühstadium

Eine Reihe biometrischer Identifikationsverfahren befindet sich noch in einem so frühen Entwicklungsstadium, dass insbesondere eine Prognose über die zukünftige Umsetzung und Anwendung nur schwer möglich ist. Hierzu gehören unter anderem (Behrens/Roth 2001, S. 24; Breitenstein 2002):

Abbildung 8

Online-Handschriften („Haus von Nikolaus“ und vorgegebener Schriftzug)



Quelle: Vielhauer 2000

- Geruchsidentifikation: Mit „künstlichen Nasen“ könnte in Zukunft das einzigartige Geruchsmuster flüchtiger chemischer Substanzen des menschlichen Körpers erfasst und ausgewertet werden. Eine britische Firma, Mastiff Electronic Systems Ltd., arbeitet an einem solchen System mit Namen „Scentinel“.
- DNA-Analyse: Angesichts der Fortschritte in der DNA-Chip-Technologie ist eine vollautomatisierte DNA-Analyse technisch durchaus vorstellbar. Diese Automatisierung wird in Anwendungsfeldern wie der Medizin oder auch der Lebensmittelanalytik intensiv vorangetrieben, und eine Umsetzung in biometrische Systeme dürfte auf längere Sicht technisch kein großes Problem darstellen. Wegen der allseits anerkannten Sensibilität genetischer Daten erscheint jedoch eine Anwendung zur bloßen biometrischen Identifikation auf absehbare Zeit wenig wahrscheinlich.
- Tastendruckdynamik (Schreibrhythmus): Das System misst zum einen die so genannten Tastenverweildauer, zum anderen die Länge der Zeit, die zwischen zwei Tastenanschlägen liegt. Eine charakteristische Tippdynamik existiert allerdings nur bei geübten Schreibenden.
- Handflächenerkennung: Ähnlich der Fingerbilderkennung misst das System das Linienmuster der Handinnenfläche einer Person.
- Gefäßmuster (vaskuläre Muster): Biometrisch erfasst werden kann das charakteristische Venenmuster an verschiedenen Stellen des Körpers, z. B. an Handgelenk und Handrücken oder im Gesicht.
- Ohrgeometrie: Abbildung bzw. Verlauf der Ohrmuschel sind hinreichend individuell. Die Messung erfordert allerdings eine hohe Positionsgenauigkeit (Platanista 2001a).

Zunehmend wichtig wird bei allen Systemen die so genannte Lebenderkennung, die eine Überwindung der Systeme durch simple Imitate verhindern soll. Als eine verbesserte Technologie für die Lebenderkennung bei Fingerbildsensoren wird z. B. die Pulsoxymetrie verfolgt, also die Messung des Blutsauerstoffgehaltes.

3. Vorzüge und Nachteile der Systeme im Überblick

Auf nationaler und internationaler Ebene sind mehrere Gremien damit befasst, Kriterien für eine zukünftige Evaluation biometrischer Systeme zu definieren (Kapitel III.1.3), die vorhandenen Verfahren (oft eher Prototypen) werden in verschiedenen Pilotprojekten vergleichenden Praxistests unterzogen (Kapitel III.1.1. u. III.1.2). Ein allgemein anerkanntes Vorgehen zum Vergleich der Stärken und Schwächen der verschiedenen biometrischen Systeme ist aber noch nicht etabliert. Darüber hinaus macht die unterschiedliche Entwicklungs- bzw. Praxisreife der verschiedenen biometrischen Systeme eine vergleichende Evaluation schwierig. Eine solche müsste nachvollziehbare und aussagekräftige Daten u. a. zu Zuverlässigkeit, Genauigkeit, Empfindlichkeit, Akzeptanz, Robustheit, Kompatibilität, Einfachheit und Kosten umfassen. Die folgenden Tabellen geben einen Überblick zu vergleichenden Beschreibungen und Bewertungen der wichtigsten biometrischen Systeme, wie sie in der Literatur zu finden sind. Tabelle 2 listet die technischen Kennwerte auf (zu FAR/FRR; s. Kapitel II.1).

Tabelle 3 fasst „Stärken und Schwächen“ zusammen, wie sie in den Kapiteln II.2.1 bis II.2.7 beschrieben worden sind. Die Tabellen 4 und 5, Seite 22, entstammen Einzelquellen und dokumentieren die vergleichende Bewertung der biometrischen Verfahren durch die Autoren Jain et al. (1999) und Scheuermann et al. (2000). Es sei aus-

Tabelle 2

Technische Angaben zu biometrischen Systemen/Verfahren

Merkmal	Templategröße (Bytes)	Verifikations-/ Registrierungszeit (sec)	FAR (%)	FRR (%)
Fingerbild (Minuzien)	900–1 200	0,5–20/10–30	*0,01–0,0001*	*1,0–5,0*
Handgeometrie	10–20	2–5/k. A.	*0,1–5,0*	*0,2–5,0*
Iris	bis 512	0,5–10/k. A.	*0,01–1,0*	*0,1–2,0*
Retina	40–96	ab 1,5/bis 30	*0,0001*	*bis 12*
Gesicht	bis 1 300	1–5/bis 30	*0,5–2,0*	*1,0–3,0*
Unter-/Handschrift	400–1 500	5–15/30	*1,6–20*	*2,8–25*
Stimme	1 500–3 000	ab 1,5/k. A.	*k. A.*	*k. A.*

Quelle: Behrens/Roth 2001; Platanista 2001a

drücklich betont, dass die wiedergegebenen Bewertungen nur unter großen Vorbehalten interpretiert werden können, da sie aus vielerlei Gründen unvollständig, vorläufig und teilweise subjektiv bzw. nicht überprüfbar (z. B. Herstellerangaben) sind. Dazu kommt, dass die Beurteilung von Stärken und Schwächen eines Verfahrens nur in einem spezifischen Anwendungskontext und in Abhängigkeit von den zu erfüllenden Funktionen (z. B. Identifikation oder Verifikation) erfolgen kann. Eine solche Evaluierung muss empirisch angelegt und in ihren Einzelschritten nachvollziehbar erfolgen (Platanista 2001a; Kapitel III.1.1). Von einer Einschätzung der Eignung und Leistungsfähigkeit der verschiedenen Systeme für konkrete Einsatzszenarien muss daher an dieser Stelle Abstand genommen werden. Diese Aufgabe bleibt einer bei weitem umfangreicheren Analyse vorbehalten, als sie im vorliegenden Bericht geleistet werden konnte. Insgesamt sollen die Tabellen lediglich eine grobe Orientierung bieten.

Tabelle 3

Vorzüge und Nachteile biometrischer Verfahren/Systeme

Merkmal	„Stärken“	„Schwächen“
Fingerbild	– einzigartig – beständig – einfache Bedienung – preisgünstig – recht überwindungsresistent	– abhängig von Hautzustand – Positionierung nötig – Systeminkompatibilitäten – Lebenderkennung fehlt – Assoziation der Strafverfolgung
Handgeometrie	– unabhängig von Hautzustand – niedrige Fehlerrate beim Enrolment (FER) – einfache Bedienung – schnell	– nicht sehr charakteristisch – beständig nur bei Erwachsenen – Lebenderkennung fehlt – teuer, da Großgeräte nötig – Hygieneaspekte
Iris/Retina	– einzigartig – beständig – berührungslos – sehr überwindungsresistent (Retina: „nicht offenes“ Merkmal)	– Retina: Störung durch Kontaktlinsen und Astigmatismus – Positionierung nötig – teuer, da Großgeräte nötig – Gesundheitsbedenken
Gesicht	– berührungslos – Standardgeräte verwendbar – teils kompatibel zu Papierdokumenten – kontinuierliche Kontrolle möglich	– unbeständig bei Alterung – empfindlich gegenüber Licht- und Temperaturveränderungen – teils Positionierung nötig – Überwachungsproblematik
Stimme	– ortsunabhängig – einfache Bedienung – Standardgeräte verwendbar – Willenserklärung integrierbar, Nutzersteuerung möglich	– nicht sehr charakteristisch – unbeständig (Alterung) und störungsanfällig (Krankheit) – zeitaufwendiges Enrolment – leicht überwindbar
Unter-/Handschrift	– an konventionelle Systeme anschließbar – akzeptiert, da vertraut – Willenserklärung, Nutzersteuerung	– nicht sehr charakteristisch – unbeständig – zeitaufwendiges Enrolment

Quelle: Behrens/Roth 2001, S. 25 f.; firstsurf 1999; Platanista 2001a; Wirtz 1999

Tabelle 4

Bewertung biometrischer Verfahren nach Jain et al. 1999

Merkmal	Universalität	Einzigartigkeit	Beständigkeit	Messbarkeit	Leistung	Akzeptanz	Resistenz*
Fingerbild	mittel	**hoch**	**hoch**	mittel	**hoch**	mittel	**hoch**
Handgeometrie	mittel	mittel	mittel	**hoch**	mittel	mittel	mittel
Iris	**hoch**	**hoch**	**hoch**	mittel	**hoch**	*gering*	**hoch**
Retina	**hoch**	**hoch**	mittel	*gering*	**hoch**	*gering*	**hoch**
Gesicht	**hoch**	*gering*	mittel	**hoch**	*gering*	**hoch**	*gering*
+Thermogramm	**hoch**	**hoch**	*gering*	**hoch**	mittel	**hoch**	**hoch**
Unterschrift	gering	*gering*	*gering*	**hoch**	*gering*	**hoch**	*gering*
Stimme	mittel	*gering*	*gering*	mittel	*gering*	**hoch**	*gering*
Handvenen	mittel	mittel	mittel	mittel	mittel	mittel	**hoch**
Tastenanschlag	*gering*	*gering*	*gering*	mittel	*gering*	mittel	mittel

* gegen Überwindungsversuche/Angriffe

Quelle: Jain et al. 1999, nach Platanista 2001a

Tabelle 5

Bewertung biometrischer Verfahren nach Scheuermann et al. 2000

Merkmal	Kostenfaktor	Anwenderfreundlichkeit	Wartungsanforderungen
Fingerbild	mittel	*gering*	mittel bis **hoch**
Handgeometrie	**hoch**	mittel	mittel
Iris	**hoch**	**hoch**	mittel
Retina	**hoch**	**hoch**	mittel
Gesicht	mittel	**hoch**	mittel
+Thermogramm	mittel	**hoch**	mittel
Unterschrift	mittel	*gering*	mittel
Stimme	*gering*	*gering*	*gering*
Handvenen	mittel	*gering*	mittel
Tastenanschlag	*gering*	*gering*	*gering*

Quelle: Scheuermann et al. 2000, nach Platanista 2001a

Bei einer Gruppierung und Gegenüberstellung der verschiedenen Systeme nach aktiven und passiven Merkmalen können folgende Einschätzungen zusammengefasst werden (Platanista 2001a):

– Die passiven, physiologischen Merkmale sind meist „offen", d. h. von außen erkennbar (Ausnahme: Retina) und daher potenziellen „Angreifern" leichter zugänglich. Sie können anwendungsfreundlich im Sinne von bequem sein, damit verbunden ist dann die Möglichkeit einer unbemerkten, nicht autorisierten Identifikation zum Zweck der Überwachung. Die Erfassung passiver Merkmale kann auch trotz Widerstand durch physische Gewalt erzwungen werden, was z. B. für Zwecke der Strafverfolgung durchaus als Vorteil angesehen werden kann, im Hinblick auf kriminellen Missbrauch aber als Nachteil gelten muss.

– Die aktiven Merkmale (Stimme und Unter-/Handschrift) können mit einer Willenserklärung verbunden werden, welche die Verbindlichkeit und Nichtabstreitbarkeit des jeweiligen Authentifizierungsvorgangs erhöht. Darüber hinaus können sie bei entsprechender Auslegung vom Nutzer immer wieder (durch Enrolment einer neuen gesprochenen oder geschriebenen Wortfolge) verändert werden, womit das System zumindest in gewissem Umfang vom Nutzer kontrolliert und gesteuert würde. Im Gegensatz zu den nicht beeinflussbaren passiven Merkmalen können die flexiblen, anpassbaren aktiven Merkmale daher auch nicht dauerhaft „kompromittiert", sondern allenfalls – vergleichbar der PIN – vorübergehend missbraucht werden. Diese Vorteile der Variabilität und Flexibilität gehen allerdings einher mit großen Einschränkungen bei Genauigkeit und Zuverlässigkeit: Die aktiven Merkmale sind vergleichsweise uncharakteristisch und unbeständig, die entsprechenden biometrischen Systeme bislang recht störungsanfällig und leicht zu überwinden, hinzu kommt häufig ein aufwendiges Enrolment. Durch entsprechende Androhung von Gewalt oder sonstiger Repressalien sind natürlich auch die verhaltensgesteuerten Merkmale erzwingbar.

– Kombinationssysteme (z. B. Stimme und Gesicht) können Vorteile der aktiven und passiven Merkmale zusammenführen und dadurch fehler- und somit benutzerfreundlicher gestaltet werden. Mehrfach multimodale Systeme könnten den Ausfall bzw. Mangel einzelner Merkmale tolerieren – immerhin wird davon ausgegangen, dass jedes einzelne biometrische Merkmal bei ca. 5 % der Bevölkerung nicht genutzt werden kann (Morgan Keegan 2000, nach Platanista 2001a), unabhängig von dem benutzten Verfahren. Nutzernachteile entstehen allerdings durch aufwendige Enrolmentverfahren, ein möglicher Eindruck der „Totalerfassung" könnte starke Anwendervorbehalte provozieren.

III. Forschungs- und Entwicklungsaktivitäten

Den Stand von Forschung und Entwicklung im Bereich biometrischer Systeme allein für Deutschland erschöpfend zu erheben, erweist sich als äußerst aufwendig. Zum einen sind aussagekräftige Informationen der entsprechenden Firmen nur schwer zu erhalten, zum anderen gibt es nur wenige öffentlich geförderte Forschungsprojekte. Während es bis 1999 keine direkte Forschungsförderung seitens des Bundes gab (Bundesregierung 1999), sind in den vergangenen zwei Jahren entsprechende Förderaktivitäten begonnen worden. Das BMWi unterstützt beispielsweise aktuell das Projekt BioTrust (Kapitel III.1.2), das BMBF das Projekt H2O4M (Kapitel III.2), das Bundesamt für Sicherheit in der Informationstechnik das BioIS-Projekt (Kapitel III.1.1). Daneben wird Forschung zur Biometrie in mehreren Fraunhofer-Instituten betrieben, die mit Bundesmitteln bezuschusst werden.

Auf der internationalen Ebene bereitet es schon Schwierigkeiten, überhaupt einen Überblick zu erlangen. Gerade im nordamerikanischen und asiatischen Raum existiert eine kaum überschaubare Vielzahl von Aktivitäten im privatwirtschaftlichen und öffentlichen Sektor.

Für den Blickwinkel der Technikfolgenabschätzung zur Feststellung des politischen Gestaltungsbedarfs sind besonders die so genannten „Pilotprojekte" zur Evaluierung biometrischer Systeme von Interesse, die mit Unterstützung öffentlicher Institutionen durchgeführt werden. Sie sind zum einen als vergleichende Untersuchungen verschiedener technischer Systeme angelegt und behandeln zum andern die gesellschaftlich relevanten Aspekte wie Verbraucher- und Datenschutz.

Im folgenden Kapitel III.1 werden die wichtigsten Ergebnisse der – deutschen – Pilotprojekte vorgestellt, und es wird ein kurzer Überblick zu laufenden Aktivitäten gegeben. Kapitel III.2 fasst zusammen, was zum Stand von FuE durch die Gutachter Behrens und Roth (Behrens/Roth 2001) und die Platanista GmbH (Platanista 2001a) sowie durch die Autoren dieses Berichts v. a. im Internet recherchiert werden konnte. Die Ergebnisse insgesamt sind unvollständig bzw. unsystematisch und bezüglich der einzelnen FuE-Projekte von äußerst unterschiedlichem Informationsgehalt. Dennoch ermöglichen sie zumindest einen ersten, exemplarischen Einblick in die weltweiten Forschungs- und Entwicklungsaktivitäten. Eine systematische Erhebung, einschließlich einer Identifikation von Schwerpunkten und erwartbaren Entwicklungstrends, bleibt eine Aufgabe für die Zukunft.

1. Pilotprojekte und Entwicklung von Testkriterien

1.1 BioIS-Projekt

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat gemeinsam mit dem Bundeskriminalamt (BKA)

in den Jahren 1999 und 2000 eine „Vergleichende Untersuchung biometrischer Identifikationssysteme – BioIS“ durchführen lassen, die erste ihrer Art in Deutschland. Das Fraunhofer-Institut für grafische Datenverarbeitung (IGD) in Darmstadt war für die technische Untersuchung – einen Praxisvergleich verschiedener Systeme – zuständig, das Modul Technikfolgenabschätzung wurde vom Wissenschaftlichen Institut für Kommunikationsdienste GmbH (WIK), Bad Honnef, bearbeitet. Über die Ergebnisse eines forensischen Gutachtens, das die Gerichtsverwertbarkeit der verschiedenen Erkennungsmerkmale untersuchen und beurteilen sollte (WIK 2000, S. 18), ist bislang nichts öffentlich bekannt geworden. Ein Ziel dieser und anderer Aktivitäten ist es, national und international abgestimmte (Kapitel III.1.3) Evaluierungs-, Normierungs- und Zertifizierungskriterien zu erarbeiten, die für den Einsatz, für die Anwendung und zur Bewertung biometrischer Verfahren, z. B. im Rahmen der gesetzeskonformen Digitalen Signatur (Kapitel V.2), notwendig sind (http://www.bsi.de).

Technische Untersuchung

Vom Fraunhofer-Institut für grafische Datenverarbeitung wurden zehn auf dem deutschen Markt erhältliche biometrische Geräte auf Alltagstauglichkeit und Verwendbarkeit für sicherheitskritische Anwendungen untersucht (IGD 2000). Getestet wurden drei Fingerbild- und ein Handgeometrie-Scanner, zwei reine Gesichtserkennungssysteme, zwei Unterschriftserkennungssysteme, ein multimodales System (Gesicht, Stimme, Lippenbewegung) sowie ein Iris-Scanner. 40 Testpersonen – Angestellte des Instituts – durchliefen ein halbes Jahr lang einen entsprechenden Testparcours. Die Systeme wurden hinsichtlich Bedienungsdauer, Erkennungsgüte bzw. Fehlerkennungsrate, Administrierbarkeit, Probleme bei der Nutzerregistrierung sowie auf Möglichkeiten und Schwierigkeitsgrad der Überwindung hin untersucht (Behrens/Roth 2001, S. 41). Lediglich zwei der getesteten biometrischen Identifikationssysteme, ein Gesichtserkennungssystem sowie der Iris-Scan, wurden für „alltagstauglich“ befunden.

Überwindungsversuche konnten nur bei sieben Systemen gestartet werden – ein System konnte unter den Versuchsbedingungen gar nicht installiert werden, vier Systeme wiesen auch nach fünf Zugangsversuchen so hohe falsche Ablehnungsraten (FRR) (über 40 %, einmal sogar über 60 %!) auf, dass ein Test sinnlos gewesen wäre. Von den getesteten sieben Systemen konnten durch Benutzung eines kopierten oder gefälschten biometrischen Merkmals fünf überwunden werden, durch einen „Angriff“ auf die Datenverbindung vom Sensor zur Verarbeitungseinheit (Abhören/Abgreifen der übertragenen Daten) sechs (IGD 2000, S. 44 ff.).

Eine Folgerung des IGD aus der technischen Untersuchung war, dass für verbesserte und aussagekräftigere Vergleiche biometrischer Systeme zukünftig ein detaillierter und verbindlicher Kriterienkatalog nötig ist. Entsprechende Aktivitäten sind aufgenommen worden (s. u.).

Teiluntersuchung Technikfolgenabschätzung

Ziel des Moduls Technikfolgenabschätzung von BioIS war es, „auf der Basis frühzeitiger und entscheidungsbezogener Analysen der Nutzerakzeptanz sowie der Chancen und Risiken auf gesamtgesellschaftlicher Ebene Gestaltungsspielräume bei der Implementierung und Anwendung von Biometrie aufzuzeigen, um positive Effekte biometrisch basierter IT-Sicherheit zu verstärken bzw. um negative zu vermeiden oder zu mildern“ (WIK 2000, S. 19). Neben Literaturauswertung und Internetrecherchen wurden die Testpersonen befragt, des Weiteren Firmenvertreter und andere Experten interviewt. Den Abschluss bildete ein (öffentliches) Symposium (WIK 2000, S. 20 f.).

Die Nutzerbefragung erbrachte einige überraschende Ergebnisse (WIK 2000, S. 36 ff.):

- 80 % der Befragten präferierten nach Abschluss der sechsmonatigen Testphase den Iris-Scan. Gesundheitsbedenken spielten entgegen den Erwartungen keine Rolle, sondern vielmehr die schnelle, bequeme und zuverlässige Handhabung.
- Mit großem Abstand wurden Fingerabdruck (48 %), Hand- (36 %) und Gesichtserkennung (20 %) als akzeptabel und geeignet eingeschätzt.
- Das Sprechen mit einer Maschine wurde, insbesondere im Fall notwendiger Mehrfachversuche, als unangenehm bis peinlich empfunden. Hygienische Bedenken (z. B. beim Fingerabdruck) wurden hingegen kaum geäußert.
- Keine/r der Befragten lehnte den Einsatz biometrischer Verfahren prinzipiell ab, wobei berücksichtigt werden muss, dass die Mitarbeiter des IGD sowohl technisch überdurchschnittlich kundig als auch prinzipiell gegenüber Technik eher positiv eingestellt sind.
- Insgesamt dominierten Komfortwünsche deutlich gegenüber Datenschutzaspekten. Diese würden z. B. eine möglichst aktive Teilnahme der Nutzer am Erkennungsprozess nahe legen, um die Gefahr einer unbemerkten Überwachung auszuschließen – die Probanden jedoch würden lieber so passiv wie möglich bleiben.[1] Auf allgemeiner, theoretischer Ebene zeigte sich allerdings sehr wohl ein entwickeltes Bewusstsein für Sicherheits- und Datenschutzprobleme (Sicherung der Referenzdaten, Risiko des Merkmalsverlustes, Abhängigkeit vom biometrischen System, „gläserner Mensch“).

Die Autoren der WIK-Studie konstatieren insgesamt einen sehr großen Informations- und Aufklärungsbedarf, sowohl im Hinblick auf die zukünftige Akzeptanz als auch auf Daten- und Verbraucherschutz. Für eine fundiertere Analyse

[1] Sehr deutlich formuliert wurde die Erwartung der Nutzer an Einfachheit und Zuverlässigkeit des biometrischen Systems durch einen der Befragten (WIK 2000, S. 32 f.): „Ein System wird nur dann akzeptiert, wenn es in der Lage ist, eine nicht ausgeschlafene, zerstreute, eventuell unter Restalkohol stehende Person zu authentifizieren.“

spezifischer Nutzungshemmnisse biometrischer Systeme war die Fallgruppe allerdings viel zu klein. Hierzu wäre eine Untersuchung mit mehreren Tausend Nutzern nötig (WIK 2000, S. 39) – dafür wiederum müsste die Biometrie schon eine Massenanwendung gefunden haben.

Die Experteninterviews auf Basis der Literaturanalyse behandelten die Themen Systemische Sicherheit, Daten- und Verbraucherschutz, Grundversorgung und Medienkompetenz. Wichtige Ergebnisse und abgeleitete Gestaltungserfordernisse sind (WIK 2000, S. 40 ff.):

- Biometrische Techniken können potenziell die Authentifizierung verbessern, entscheidend bleibt allerdings die gesamte Sicherheitsarchitektur eines IT-Systems.
- Für einen wirklich aussagekräftigen Vergleich vorhandener Systeme, ob zu Zuverlässigkeit, Bedienungsfreundlichkeit oder Überwindungssicherheit, fehlen bislang die Daten. Unabdingbar ist die Entwicklung international akzeptierter Standardtestverfahren.
- Zentrale Sicherheitsaspekte sind die Lebenderkennung sowie der Schutz vor Manipulation und Missbrauch der Template-Daten. Deshalb sollten die Referenzdaten dezentral, am besten in der Verfügung des Nutzers (z. B. auf einer Smartcard) gespeichert werden. Die Abhängigkeit von einem einzelnen biometrischen System muss vermieden, die Möglichkeit des Widerrufs eines Merkmals hingegen garantiert werden. Verifikation ist prinzipiell der Identifikation vorzuziehen.
- Effizienz- und Komfortkriterien dürfen Daten- und Verbraucherschutzaspekte nicht in den Hintergrund drängen, selbst wenn (nicht ausreichend informierte) Nutzer dies möglicherweise akzeptieren würden. Dies spricht tendenziell gegen die „passive" Aufnahme biometrischer Merkmale.
- Niemand darf zur Nutzung biometrischer Systeme gezwungen oder gedrängt werden. Da jedes biometrisch genutzte Merkmal bei überschlägig 5 % der Bevölkerung „versagt", müssen alternative Autorisierungsverfahren erhalten bleiben, die für die Nutzer keine Nachteile bedeuten. Im Rahmen einer Verbraucherschutzdiskussion ist zu klären, ob umgekehrt auch die Gewährung von Vorteilen als Anreiz für die Nutzung biometrischer Verfahren unterbunden werden soll und kann.
- Aus Verbrauchersicht wäre eine Umkehrung der Beweislast bei Missbrauch – hin zu den Banken und anderen Betreibern – als Folge der Sicherheitserhöhung zu fordern. Diese Maßnahme würde die Akzeptanz der Kunden sicherlich erhöhen, bedeutet allerdings weitere Kosten für die Betreiber.
- Vor der Einführung biometrischer Verfahren in Massenanwendungen werden umfangreiche Aufklärungsmaßnahmen nötig sein, sowohl in praktischer und technischer Hinsicht als auch zu Verbraucher- und Datenschutz. Die Verteilung der Lasten dieser Aufgabe bleibt zu klären.

Entwurf: Technische Evaluierungskriterien (TEK)

Nach Abschluss und als Folgeaktivität des BioIS-Projektes hat das BSI im September 2000 eine Entwurfsversion „Technische Evaluationskriterien zur Bewertung und Klassifizierung biometrischer Systeme" veröffentlicht, die primär für die Anwendung durch oberste (und nachgeordnete) Bundesbehörden konzipiert sind, aber auch privat bzw. gewerblich genutzt werden können (BSI 2000, S. 4). Die interessierte Öffentlichkeit ist zur Kommentierung aufgefordert (http://www.sit.gmd.de/SICA/papers/WS_01/Beitrag_Munde.pdf).

Definiert werden drei Prüfungstypen, wobei das Hauptunterscheidungskriterium der Zeitaufwand ist: die generelle Beurteilung (physikalische Robustheit, Hard- und Softwareanforderungen, Erweiterbarkeit), die Zuverlässigkeit der Erfassung (über Feldtests, 3 Klassen à 10, 100 und 1 000 Teilnehmern mit je mindestens 150 Versuchen) bzw. Erkennungsleistung (FAR/FRR) unter verschiedenen Umweltbedingungen sowie die Sicherheit bzw. Überwindbarkeit.

In dem laufenden Projekt „BioKrit – Prüfkriterien bzw. Prüfschritte für eine Common Criteria konforme Evaluierung biometrischer Systeme" sollen Weiterentwicklung und Anpassung der technischen Evaluationskriterien an die übergeordneten „Common Criteria for Information Technology Security Evaluation (CC)" untersucht werden, die unter Beteiligung Deutschlands, Frankreichs, Großbritanniens, Kanadas, der Niederlande und der USA entstanden und mittlerweile zur CC-ISO-Norm 15408 geworden sind („Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, Version 2.0", Mai 1998). Das BSI hat die Rolle des deutschen Partners übernommen und bei der Erarbeitung der Kriterien aktiv mitgewirkt (http://www.bsi.de/cc/ index.htm).

1.2 BioTrusT (TeleTrusT Deutschland e.V.)

Im 1989 gegründeten, gemeinnützigen Verein TeleTrust Deutschland e. V. haben sich Unternehmen, Forschungseinrichtungen, Verbände und öffentliche Institutionen zusammengeschlossen, „um die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung zu fördern". Aufgabe des Vereins ist es, „die Akzeptanz der digitalen Signatur als Instrument zur Rechtssicherheit einer Transaktion zu erreichen; die Forschung zur Sicherheit des elektronischen Datenaustausches (EDI) und die Anwendung ihrer Ergebnisse sowie die Entwicklung von Standards für dieses Gebiet zu unterstützen; mit Institutionen in anderen Ländern zusammen zu arbeiten, um Ziele und Standards innerhalb der Europäischen Union zu harmonisieren" (http://www.teletrust.de).

Da im Rahmen dieser Zielsetzung biometrische Verfahren eine wichtige Rolle spielen, hat sich eine spezielle Arbeitsgruppe (AG 6) des Themas angenommen. Ziel der AG 6 ist es, „den Einsatz geeigneter biometrischer Identifikationsverfahren zu fördern, die auf körpereigenen biometrischen Merkmalen eines Benutzers basieren, um die erforderlichen Sicherheitsverfahren der Informationstechnik, z. B. das PIN-Verfahren, zu ergänzen bzw.

abzulösen. Dazu gehört ganz wesentlich die Information einer breiten Öffentlichkeit über biometrische Verfahren, unterschiedliche Methoden, mögliche Anwendungsgebiete und damit eine Förderung der Akzeptanz für den Umgang mit biometrischen Identifikationsverfahren im alltäglichen beruflichen und privaten Gebrauch“ (http://www.teletrust.de/main/AG/ag6+.htm).

Kriterienkatalog

Im August 1998 hat die AG 6 einen so genannten Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren „als Hilfsmittel für die sachbezogene Arbeitsebene potenzieller Anwender oder Betreiber“ vorgelegt. Das Papier bietet in sehr komprimierter Form eine allgemeine Einführung in Prinzip und Varianten der Biometrie, beschreibt ausgewählte technische Merkmale (u. a. Fehlerraten, Trennfähigkeit und Sicherheitskennzahlen), umreißt juristische Aspekte und listet mögliche Fragen aus Betreiber- und Nutzersicht auf. Im Anhang findet sich eine Checkliste zu den behandelten Kriterien, anhand derer mögliche Anwender die Verfahren vergleichen und für die jeweilige Applikation ein geeignetes auswählen können (Teletrust 1998). Beabsichtigt war eine offene Kommentierung und regelmäßige Überarbeitung des Dokuments, doch ist bislang keine neue Version erschienen (Stand: Februar 2002).

BioTrusT-Projekt

Zeitlich parallel zum o. g. BioIS-Projekt wurde 1999 von der AG 6 das auf drei Jahre angelegte Projekt BioTrusT als interdisziplinärer Pilotversuch zur Anwendung biometrischer Verfahren im Bankenbereich initiiert. Das Projekt wird vom Bundesministerium für Wirtschaft und Technologie und von der S-Finanzgruppe der Sparkassen unterstützt. In mehreren Stufen sollen Erkenntnisse zur Zuverlässigkeit und Alltagstauglichkeit biometrischer Systeme wie auch zur Akzeptanz durch die Nutzer und Betreiber und deren Bedingungen gewonnen werden. Die Praxistests werden anfangs ausschließlich innerhalb der beteiligten Sparkassenunternehmen durchgeführt. Vier Phasen sind geplant: 1. Zutrittssicherung, 2. PC-Zugang, 3. Geldausgabeautomat, 4. Homebanking.

Partner des BioTrusT-Projektes sind vier Betreiber, zehn Hersteller und vier „Research Partner“, darunter die Fachhochschule Gießen-Friedberg, die folgende Fragestellungen wissenschaftlich bearbeiten soll (Behrens/Roth 2000, S. 329):

– „Komfort-/Convenience-Aspekte: Inwiefern bieten die biometrischen Verfahren den Nutzern Vorteile bezüglich Komfort und Bequemlichkeit? Wie bewertet der Benutzer Komfortelemente wie beispielsweise Schnelligkeit oder Einfachheit?

– Sicherheitsaspekte: Welche Sicherheit bieten die biometrischen Verfahren, absolut und im Vergleich zum Prinzip Besitz und Wissen? Dabei müssen objektive Sicherheit und subjektive Wahrnehmungen gegeneinander abgeschätzt werden. Für einen Einsatz im Bankenbereich stellt sich unter Berücksichtigung von Verbraucher- und Datenschutzaspekten die Frage, wie Sicherheitsmerkmale von den Nutzern in Relation zur PIN wahrgenommen werden.

– Vielfältigkeitsaspekte: Welche Einsatzfelder sind, vornehmlich im elektronischen Zahlungsverkehr, besonders geeignet für welche biometrischen Verfahren? Gibt es dabei Unterschiede im Akzeptanzniveau bei potenziellen Nutzern?

– Einsatzempfehlungen: Die Bedingungsfaktoren für Vor- und Nachteile der einzelnen biometrischen Verfahren sind herauszuarbeiten.“

Aspekte des Daten- und Verbraucherschutzes werden vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD-SH; http://www.rewi.hu-berlin.de) und von der Arbeitsgemeinschaft der Verbraucherverbände e.V. (AgV, http://www.agv.de; seit 2001 Verbraucherzentrale Bundesverband e.V., http://www.vzbv.de) untersucht. Zwischenergebnisse des BioTrusT-Projektes wurden auf zwei Workshops, im Mai 2000 und im Juni 2001, präsentiert. Sie werden an dieser Stelle nicht weiter behandelt, da der aktuelle Erkenntnisstand im BioTrusT-Projekt durch die Gutachterinnen und Gutachter in die entsprechenden Kapitel des vorliegenden Berichtes eingeflossen ist.

1.3 Standardisierung und Evaluierung biometrischer Systeme

Über 85 Unternehmen und Organisationen weltweit haben sich im 1998 gegründeten BioAPI Consortium zusammengeschlossen. Vorrangiges Ziel ist, durch die Entwicklung einer standardisierten Schnittstelle zwischen biometrischem System und anwendungsbezogener (elektronischer) Verarbeitung der erhobenen Daten die unterschiedlichsten Systeme kompatibel, „interoperationabel“ zu machen (http://www.bioapi.org). Diese Schnittstelle heißt BioAPI für „Biometric Application Programming Interface“. Im Rahmen des BioTrust-Projektes (s. o.) haben mehrere Hersteller die Integration der BioAPI-Schnittstelle realisiert. Als Beispiel-Anwendung ist dabei ein Bildschirmschoner entwickelt worden, der in diversen Systemkonfigurationen mit unterschiedlichen biometrischen Systemen einsetzbar ist (Platanista 2001a).

Microsoft hat im Mai 2000 ein Kooperationsabkommen mit dem Biometrie-Spezialisten I/O Software geschlossen, um Programmierschnittstellen für biometrische Verfahren zu standardisieren und in kommende Windows-Versionen zu integrieren. Die Biometric API, die Microsoft von I/O Software lizenziert hat, soll Windows-Programmierern als Anknüpfungspunkt für Eigenentwicklungen dienen. Das BioProtect-Plug-In (Oktober 2001) verschlüsselt Microsoft-Office-Dokumente per Fingerabdruck (Maus-integriert), um Transaktionen im E-Commerce zu bestätigen oder um sich an einem PC oder gegenüber einem Netzwerk zu authentifizieren (Platanista 2001a).

In den USA fördert das Biometric Consortium, eine gemeinsame Einrichtung von sechs Ministerien sowie des Militärs (das von jeher ein zentraler Motor der Biometrie gewesen ist), die Entwicklung und Standardisierung bio-

metrischer Systeme sowie von Test- und Evaluationsverfahren für den Einsatz in Regierungsbehörden (WIK 2000, S. 13; http://www.biometrics.org). Hinsichtlich der Verwendung in den US-amerikanischen Streitkräften hat das Verteidigungsministerium im Jahr 2000 das „Biometrics Management Office“ (BMO) gegründet. Im Geschäftsbereich des US Departments of Commerce arbeitet insbesondere das National Institute of Standards and Technology (NIST) auf internationale Standards hin (http://www.nist.gov). So wurde von der dort angesiedelten „Biometric Interoperability, Performance and Assurance Working Group“ in Koordination u. a. mit BioAPI Consortium und TeleTrusT ein „Common Biometric Exchange File Format“ (CBEFF, http://www.ibiometrics.net/CBEFF.htm) entwickelt.

Technische Erprobungen führt das US National Biometric Test Center an der Universität von San José in Kalifornien durch (http://www.engr.sjsu.edu/biometrics). Es arbeitet mit Industrie und Verteidigungsministerium zusammen. Das American National Standards Institute (ANSI, http://www.ansi.org) koordiniert Standardisierungsbemühungen im kommerziellen Bereich. US-amerikanische Hersteller, Entwickler und Betreiber biometrischer Systeme sind in der International Biometric Industry Association (IBIA, http://www.ibia.org) zusammengeschlossen (WIK 2000, S. 13). Das britische Pendant, die Association for Biometrics (AfB, http://www.afb.org.uk), hat in Zusammenarbeit mit der Biometrics Working Group der britischen Regierung im Januar 2000 Richtlinien zum Testen biometrischer Geräte (http://www.afb.org.uk/BWG/pestprac10.pdf) herausgegeben (BSI 2000, S. 23). Im Frühjahr 2001 veröffentlichte die Biometrics Working Group einen Testbericht, im Herbst weitere Dokumente (http://www.cesg.gov.uk/technology/biometrics/). Im Juli 2001 wurde vom „Australian Commonwealth Government“ das „Biometrics Institute“ gegründet, eine unabhängige und gemeinnützige Forschungs- und Beratungseinrichtung für biometrische Anwender, Hersteller und Regierungsbehörden im asiatisch-pazifischen Raum (Platanista 2001a).

Auch die Europäische Union (EU) hat im Rahmen des Forschungsprogramms ESPRIT (Unterprogramm: Human Comfort and Safety) unter der Bezeichnung BIOTEST von 1996 bis 1998 ein Projekt zur Entwicklung von Methoden vergleichender Bewertung biometrischer Systeme und zur Etablierung entsprechender Testeinrichtungen gefördert. Ergebnisse dieses mit 730 000 Euro geförderten Projektes, an dem neben kommunalen und Forschungseinrichtungen mehrere Unternehmen beteiligt waren, wurden bislang nur in sehr geringem Umfang veröffentlicht (http://www.prosoma.lu/Showcasee/Results/2118/HTML/descriptionx.html).

Der European Standard EN 5013 beschreibt Bewertungskriterien für Sicherheitsaspekte biometrischer Methoden und Verfahren, entsprechend den Technischen Evaluationskriterien des BSI in Deutschland (Kapitel III.1.1; Platanista 2001a).

2. FuE-Projekte in Deutschland und international

Ausgewählte Projekte biometrischer FuE und zugehörige Internetadressen, auf denen oder von denen aus weitere Informationen erschließbar sind, enthalten Tabelle 6, Seite 28 und 7, Seite 29, für Deutschland, Tabelle 8, Seite 31, für einige europäische und asiatische Länder sowie die USA (Behrens/Roth 2001, S. 29 ff.; Platanista GmbH 2001). Laufende EU-Projekte können Tabelle 9, Seite 32, entnommen werden.

Deutschland

Die verhältnismäßig große Zahl deutscher Projekte sollte nicht den Eindruck erwecken, dass hierzulande mit besonders viel Aufwand geforscht wird. Behrens und Roth bezeichnen die Zahl der involvierten deutschen Hochschuleinrichtungen als eher klein und überwiegend an Detaillösungen orientiert (Behrens/Roth 2001, S. 74). Auch das Engagement der Fraunhofer-Institute (Tabelle 6) sei in personeller und finanzieller Hinsicht eher begrenzt. Eine Schwerpunktsetzung in der deutschen Forschungslandschaft sei nicht auszumachen.

Allerdings zeigt die hohe Beteiligung deutscher Institute und Unternehmen an EU-Projekten (Tabelle 9) eine zunehmende Aktivität hierzulande. Auch das BMBF hat mit entsprechender Projektförderung begonnen, so im Projekt H2O4M des Fraunhofer-Institutes IPSI in Darmstadt (Tabelle 6) mit dem Ziel, digitale Wasserzeichen zum Nachweis der Authentizität und Integrität von Multimediadokumenten und -objekten zu klassifizieren und zu bewerten. Dabei wird auch der Einsatz biometrischer Merkmale zur Benutzerauthentifizierung und damit Erhöhung der Fälschungssicherheit untersucht (Platanista 2001a).

Für die deutsche Privatwirtschaft schätzen Behrens und Roth aufgrund ihrer Kontakte zu den Herstellern biometrischer Systeme, dass dort insgesamt 40 bis 60 Personen mit FuE befasst sind. Das FuE-Budget könnte sich auf 25 bis 50 Mio. DM belaufen (Behrens/Roth 2001, S. 74). Auf der Basis der vorhandenen Informationen ist es nicht möglich, den Stellenwert der privatwirtschaftlichen Forschung in Deutschland im internationalen Vergleich einzuschätzen.

Auf jeden Fall haben auch die industriellen Aktivitäten rund um biometrische Themen in den vergangenen Jahren in Deutschland an Dynamik gewonnen, dabei werden zunehmend die Möglichkeiten von Kooperationen im Rahmen von EU-Projekten genutzt (Tabelle 9). Tabelle 7 listet deutsche Herstellerfirmen/Entwickler biometrischer Systeme und ihre Schwerpunkte auf. Ein großer Teil der Firmen ist Mitglied der AG 6 von TeleTrusT (Kapitel III.1.2) und war bzw. ist an den Pilotprojekten BioIS und BioTrusT beteiligt.

Die Telekom-Tochter T-Systems Nova, Gründungsmitglied der AG 6 und Mitherausgeberin des Kriterienkatalogs „Biometrische Identifikationsverfahren“ (Kapitel III.1.2), hat im Januar 1999 ein eigenes Pilotprojekt gestartet, in dem insgesamt 800 Teilnehmer eingebunden und mehr als 30 biometrische Systeme untersucht werden (Laßmann 2001). Dabei wurden die Merkmale Fingerbild, Iris,

Tabelle 6

Öffentliche Forschungsaktivitäten zur Biometrie in Deutschland

Forschungseinrichtung	biometrisches Thema	Internetadresse
Ruhr-Universität Bochum (+ ZN-GmbH)	Gesichts- und Stimmerkennung	http://www.neuroinformatik.ruhr-uni-bochum.de/VDM/research/computerVision/contents_d.html
Fern-Universität Hagen	Tippdynamik	http://ks.fernuni-hagen.de/forschung/datensich/index_Sonja.html
Universität Karlsruhe (+ Robert Bosch GmbH)	Fingerbilderkennung	http://www-iiit.etec.uni-karlsruhe.de/~kroeni/
Universität Tübingen	Gesichtserkennung	http://www-ti.informatik.uni-tuebingen.de/deutsch/publikationen/jahresbericht9596/node40.html
TU Chemnitz	Bildverarbeitende Überwachungs- und Servicesysteme	http://www.tu-chemnitz.de/~svko/jobpage/Arbeitsgebiete/Bericht.html
TU Ilmenau	Biometrie und Smartcards	http://kb-bmts.rz.tu-ilmenau.de/kb-bmts/Leitprojekte/Komp_kurz.htm
FH Gießen-Friedberg	BioTrusT-Projekt	http://www.biometrie-info.de
FH Heilbronn	Softwareentwicklung	http://www.swl.fh-heilbronn.de/Jahresbericht/jahresbericht99v3.html#_Toc477768329
Fraunhofer-Institut für grafische Datenverarbeitung (IGD)	u. a. BioIS-Projekt	http://www.igd.fhg.de/igd-a8/projects/biois/biois_de.html
Fraunhofer-Institut für integrierte Schaltungen (IIS)	multimodales System: Gesicht, Stimme, Lippenbewegung	http://www.iis.fhg.de/propro/sesam/index.html
Fraunhofer-Institut für Integrierte Publikations- und Informationssysteme (IPSI)	Qualitätsevaluierung, speziell Handschriftenerkennung	http://www.ipsi.fraunhofer.de/mobile/projects/h2o4m/index.html
Fraunhofer-Institut für Sichere Telekooperation (SIT)	biometrische Systeme und Smartcards; EU-Studie „BioSig – Usability of biometrics in relation to electronic signatures“	http://sit.fraunhofer.de/cgi-bin/sit-frame/sica?link=/SICA/projects/bio_sig.html

Quelle: Behrens/Roth 2001, S. 29 ff.; Platanista 2001a

Gesicht, Stimme, Unterschriftdynamik und Handgeometrie insbesondere im Hinblick auf die Nutzerakzeptanz untersucht und bewertet. Ergebnisse wurden auf einem Kongress im Oktober 2001 vorgestellt (Platanista 2001a). Danach werden als grundlegende technische Probleme die häufig schwierige und unausgereifte Installation der Produkte, zu lange Reaktionszeiten der Systeme sowie die zum Teil sehr hohen Fehlerraten (FRR) angesehen. Prinzipielle Fragen betreffen den Datenschutz, vorhandene Betriebsvereinbarungen und notwendige Rückfallsysteme, welche den „biometrischen Sicherheitszuwachs“ dann infrage stellen, wenn sie doch wieder auf Besitz und Wissen basieren. Eine größere Nutzerakzeptanz setzt laut T-Nova substanzielle Verbesserungen bei Komfort und Sicherheit voraus (Laßmann 2001).

Weitere Länder und Europäische Union

Unter den europäischen Ländern verorten Behrens und Roth einen FuE-Schwerpunkt in Großbritannien. Außerhalb Europas werden in der Literatur umfangreiche Aktivitäten - neben den dominierenden USA – insbesondere in

Tabelle 7

Industrielle FuE/Beratung zum Thema Biometrie in Deutschland

Unternehmen (Beteiligung an Pilotprojekt)	biometrisches Verfahren oder verwandtes Thema	Internetadresse
ABDA	Smartcard	http://www.abda.de
ABS GmbH (BioTrusT)	Stimmerkennung	http://www.abs-jena.de
ACEM GmbH	Fingerbild-Scanner	http://www.acem.de
Add Trust	Digitale Signatur	http://www.addtrust.com
AlphaNet Online GmbH (BioIS)	Fingerbild-Scanner, BioMouse	http://www.alphanet.de
AMC-Assekuranz Marketing Circle GmbH	Unternehmensberatung	http://www.versicherungen.de/AMC
Applied Security GmbH	Smartcard, digitale Signatur	http://www.apsec.de
Baltimore Technologies	eSecurity	http://www.baltimore.com
BERGDATA (BioTrusT)	Fingerbild	http://www.bergdata.com
BGS Systemplanung	Digitale Signatur	http://www.bgs-ag.de
CAST-Forum	eSecurity (Consulting)	http://www.castforum.de
CCI (Competence Center Informatik GmbH)	IT-Consulting, Software	http://www.cci.de
Cherry GmbH (BioIS)	Tastatur-Fingerbild-Scanner	http://www.cherry.de
CogniTec AG	Gesichtserkennung	http://www.cognitec-ag.de
DataDesign AG	digitale Signatur	http://www.datadesignag.de
DCS AG (BioIS, BioTrusT)	BioID-Gesichtserkennung, Merkmals-kombinationen	http://www.bioid.com
De-Coda GmbH	digitale Signatur	http://www.de-coda.de
Dermalog Identification Systems GmbH	Fingerbild, ID-Cards mit biometrischen Merkmalen	http://www.dermalog.de
Dr. Fehr GmbH/Wondernet (BioAPI, BioTrusT)	Unterschrift/Handschriften	http://www.drfehr.de
Eutelis Consult	Markteinführung	http://www.eutelis.de
FAKTUM Softwareentwicklung GmbH	digitale Signatur	http://www.faktum.com
Fun Communications	digitale Signatur	http://www.fun.de
Gemplus GmbH	Smartcards	http://www.gemplus.com
Giesecke & Devrient GmbH (BioTrust)	Fingerbild	http://www.gdm.de
IKENDI (BioAPI, BioTrusT)	Fingerbild	http://www.ikendi.de
INFINEON Technologies AG (BioIS)	Unterschriftenprüfung, Fingerbild	http://www.infineon.com
INFORA GmbH	IT-Unternehmensberatung	http://www.infora.de
Kesberg, Bütfering & Partner (KB & P)	Markterschließung	http://www.kbp-bonn.de

noch Tabelle 7

Unternehmen (Beteiligung an Pilotprojekt)	biometrisches Verfahren oder verwandtes Thema	Internetadresse
NCR GmbH (BioIS)	Iris-Scanner	http://www.ncr.com
OMNEYKEY AG	Smartcard-Lesegeräte	http://www.omnikey.de
Platanista GmbH (H2O4M)	Handschriften-Software	http://www.platanista.com
plettac electronics (BioTrust)	Gesichtserkennung	http://www.plettac-electronics.de
Rainbow Technologies	eSecurity	http://www.rainbow.com
SD Industries GmbH	Iriserkennung	http://www.sd-industries.de
Secorvo Security Consulting GmbH	IT-Consulting	http://www.secorvo.de
Secude GmbH	Kryptografie	http://www.secude.com
SOFTPRO (BioAPI, BioTrusT)	Unterschriften-Software im Bankenbereich	http://www.softpro.de
SRC Security Research & Consulting GmbH	IT-Sicherheitsberatung	http://www.SRC-gmbh.com
Touchless Sensor Technology AG	Fingerbildsensoren	http://www.tst-ag.com
T-Systems NOVA (BioTrusT)	wissenschaftliche Gutachten (Prüfkriterien/ -siegel)	http://www.t-nova.de
Utimaco Safeware	Fingerbild, Smartcard, Sicherheitslösungen	http://www.utimaco.de
VoiceTrust AG	Stimmerkennungs-Software	http://www.voicetrust.de
Wincor Nixdorf GmbH & Co KG (BioTrusT)	Iriserkennung	http://www.wincor-nixdorf.com
ZN GmbH (BioIS, BioTrusT)	Gesichtserkennung	http://www.zn-gmbh.com

Quelle: Platanista 2001a; http://www.teletrust.de (-> Mitglieder)

Israel, aber auch in (Ost-)Asien beschrieben (Newham et al. 1999). Es wird jedoch nur ein geringer Teil dieser FuE öffentlich gemacht, u. a. weil häufig militärische Instanzen beteiligt sind. Eine vergleichende Bewertung der Forschungsaktivitäten ist aufgrund der unvollständigen Datenlage nicht möglich.

Auch in Österreich ist 2001 ein Pilotversuch angelaufen. Die Firma „ekey biometric systems“ hat ein fünfstufiges Projekt zur Nutzung des Finger-Scans (Bezahlen am Point of Sale ab 04/01; eTicketing ab 09/01; Business-Transaktionen und Zahlung im Internet mittels Kreditkarte ab 12/01; eBanking ab Frühjahr 2002) mit mehreren Kooperationspartnern begonnen (http://www.ekey.at).

Umfangreiche Aktivitäten förderte eine Recherche in der CORDIS-Datenbank der EU (ftp://ftp.cordis.lu) zutage (Tabelle 9). Neben dem bereits erwähnten, 1998 abgeschlossenen BIOTEST-Projekt (Kapitel III.1.3) und dem Projekt „BioSig“ des Fraunhofer-Institutes SIT zur Eignung biometrischer Methoden im Rahmen der elektronischen Signatur (Tabelle 6) wurden sieben laufende Projekte identifiziert (drei davon, „FINGER_CARD“, „PAIDFAIR“ und „SABRINA“, unter Leitung deutscher Unternehmen und weiterer deutscher Beteiligung), die im aktuellen „IST-Programm“ („Information Society Technologies“, deutsch auch: „Benutzerfreundliche Informationsgesellschaft“) mit insgesamt 10,8 Mio. Euro gefördert werden (Behrens/Roth 2001, S. 34 ff.; Platanista 2001a):

– Projekt „BANCA – Biometric access control for networked and e-commerce applications“ (Ref.-Nr. IST-1999-11159): Unter Benutzung von multimodaler biometrischer Identifikation (Gesicht- und Sprecherverifikation) sollen drei Demonstrationsobjekte aufgebaut werden: Telearbeitsplatz, Homebanking und ein biometrischer Geldausgabeautomat. Das Projekt wird im Rahmen des IST-Programmes mit 2,55 Mio. Euro gefördert. Die Laufzeit beträgt 30 Monate ab Januar 2001. Der „Prime-Contractor“ ist Matra Nortel

Communications S.A, Quimper (F), weitere beteiligte Firmen oder Organisationen sind: Ibermatica S. A., San Sebastian (E), University of Surrey, Guildford (UK), Ecole Polytechnique Fédérale de Lausanne (CH), Banco Bilbao Vizcaya, Bilbao (E), Oscard, Puteaux (F), Institut Dalle Molle d'Intelligence Artificielle Perceptive (CH), Université Catholique de Louvain, Louvain-La-Neuve (B), sowie Thomson Csf Communications, Colombes (F).

– Projekt „BEE – Business environment of biometrics involved in electronic commerce" (Ref.-Nr. IST-1999-20078): Aufgabe des Projektes ist es, behindernde und fördernde Elemente der biometrischen Identifikation als Sicherheitselemente innerhalb des E-Commerce zu identifizieren. Dazu soll ein Kosten-Nutzen-Modell entwickelt werden, das alle Aspekte (Technik, Organisation, Ökonomie, Herstelleraspekte, Standards und Gesetzeslage) berücksichtigt. Das Projekt hat im Dezember 2000 begonnen und soll 15 Monate dauern.

Tabelle 8

Exemplarische internationale Forschungsstandorte und -themen

Forschungseinrichtung	biometrisches Thema	Internetadresse
Ecole Polytechnique Fédérale, Lausanne (CH)	Gesichts- und Stimmerkennung	http://diwww.epfl.ch/lami/cvision/person_authentication.html
Università di Bologna (I)	Fingerbild, Gesicht, Handgeometrie	http://www2.csr.unibo.it/research/biolab/bio_tree.html
National Physical Laboratory, Centre for Mathematics and Scientific Computing, Middlesex (UK)	Biometric Product Testing (i. A. der Communication Electronic Security Group der brit. Regierung)	http://www.cesg.gov.uk/technology/ biometrics/media/Biometric%20Test% 20Report%20pt1.pdf
University of Cambridge (UK)	Iriserkennung	http://www.cl.cam.ac.uk/~jgd1000/
University of Kent at Canterbury (UK)	Gesichts- und Stimmerkennung	http://www.jtap.ac.uk/reports/htm/jtap-038.html
Trans-Eurasia Information Network TEIN (KOR)	Network Based User Authentication and Security Using Multiple Biometrics	http://www.transeurasia.org
Ministry of International Trade and Industry MITI (JPN)	National Project of Test and Evaluation for Biometric Technologies	http://www.miti.go.jp
University of Hong Kong, Centre of Asian Studies, The Telecommunications Research Project (VR China)	Biometric Solutions for E- & M-Commerce Security	http://www.trp.hku.hk
Peking University, Center for Information Studies (VR China)	The National Laboratory on Machine Perception	http://www.cis.pku.edu.cn/oldpage/introd.html
George Mason University (USA)	breit gefächerte Aktivitäten	http://www.cs.gmu.edu (search: „biometric")
Massachusetts Institute of Technology (USA)	breit gefächerte Aktivitäten	http://www.mit.edu (search: „biometric")
Michigan State University (USA)	diverse Systeme	http://biometrics.cse.msu.edu/

Quelle: Behrens/Roth 2001; Platanista 2001a

Tabelle 9

Laufende Biometrie-Projekte im Rahmen des IST-Programms der EU

Name*	Referenz-Nr.	Zahl der Partner*	Fördermittel	Laufzeit
BANCA – Biometric access control for networked and e-commerce applications	IST-1999-11159	9	2,55 Mio. €	01/01–06/03
BEE – Business environment of biometrics involved in electronic commerce	IST-1999-20078	4	0,55 Mio. €	12/00–05/02
FINGER_CARD – Biometric matching and authentication system on card	IST-2000-25168	9	1,93 Mio. €	01/01–06/02
E-POLL – Electronic polling system for remote voting operations	IST-1999-21109	7	1,7 Mio. €	09/00–08/02
PAIDFAIR – Protecting accumulated intellectual data for accounting in real time	IST-2000-29616	7	1,3 Mio. €	06/01–11/02
SABRINA – Secure authentication by a biometric rationale and integration into network applications	IST-2000-26273	7	2,09 Mio. €	01/01–12/02
U-FACE – User friendly face access control system for physical access and healthcare applications	IST-1999-11587	6	0,7 Mio. €	10/00–03/03

* Zu Projektzielen und Namen der Partner s. Text.

Quelle: Behrens/Roth 2001; Platanista 2001a

Die Fördersumme beträgt 550 000 Euro. Prime-Contractor ist PriceWaterhouseCoopers N.V., Amsterdam (NL), die weiteren Teilnehmer sind: ATMEL Grenoble (F), die nationale Technische Universität von Athen (G) sowie Expertnet, Athen (G).

– Projekt „FINGER_CARD – Biometric matching and authentication system on card“ (Ref.-Nr. IST-2000-25168): Das Projekt hat am 1. Januar 2001 begonnen und ist auf 18 Monate angelegt. Es wird mit 1,93 Mio. Euro gefördert. Ziel ist es zu zeigen, dass mit entsprechend verbesserter Technologie ein Fingerbildsensor in eine Smartcard mit Standardabmessungen integriert werden kann. Durch einen leistungsfähigen Prozessor soll auf der Karte die Verifikation durchgeführt werden. Das Projekt wird unter Leitung von Infineon, München (Projektleiterin: Dr. Wirtz), in Zusammenarbeit mit HSB Cards Card Systems B.V, Woerden (NL), der University of Kent at Canterbury (UK), dem Royal Holloway and Bedford New College (UK), den Firmen Microdatec, Erfurt (D), Stralfors Ab, Ljungby (S), Novacard Informationssysteme GmbH, Oldenburg (D), Infineon Technologies Microelectronic Design Centers Austria GmbH, Graz (A), und der Deutschen Bank AG, Frankfurt a. M. (D), durchgeführt.

– Projekt „E-POLL – Electronic polling system for remote voting operations“ (Ref.-Nr. IST-1999-21109): Das Projekt begann am 1. September 2000 und läuft 24 Monate. E-POLL beschäftigt sich mit der Organisation von Wahlprozessen. Ein wichtiger Bestandteil des Abstimmungssystems ist das „Europe Visual Ballot Network“ (EVBN), welches den Informationsfluss zwischen den verschiedenen Verwaltungsstufen koordiniert. Das „Wahlsystem“ basiert auf einer Smartcard mit integriertem Fingerbildleser zur Authentifizierung des Wählers. Die Fördersumme beträgt 1,7 Mio. Euro. Prime-Contractor ist Siemens Informatica S.p.a., Mailand (I), die weiteren Partner sind Aquitaine Europe Communication (F), Société de Production et de Recherches Appliquées SOPRA (F), France Télécom Sa (F), Ancitel Spa (I), Ministero dell'Interno (I) sowie Miedzykomunalna Spolka Akcyjna „Municipium“ Warszawa (PL).

– Projekt „PAIDFAIR - Protecting accumulated intellectual data for accounting in realtime“ (Ref.-Nr. IST-2000-29616) startete im Juni 2001 mit einer Laufzeit von 18 Monaten und einer Fördersumme von 1,3 Mio. Euro. Ziel von PAIDFAIR ist die Entwicklung eines weltweiten Zahlungsstandards zum elektronischen Vertrieb von geistigem Eigentum („IP-Content“) und Software. Hierdurch soll mehr Vertrauen hinsichtlich der Zahlungsvorgänge für Software- und IP-Content-Verkäufer und ihre Kunden geschaffen werden. Die Authentisierung soll durch biometrische Systeme in Verbindung mit Smartcards realisiert werden. Prime-Contractor ist die Wibu-Systems Aktiengesellschaft, Karlsruhe (D), weitere Teilnehmer sind Neol (F), Native Instruments Software Synthesis Gmbh (D),

Hoschar Ag (D), Asknet Ag (D), Compusec N. V. (B) und 2-Tel B.V. (NL).

– Projekt „SABRINA – Secure authentication by a biometric rationale and integration into network applications“ (Ref.-Nr. IST-2000-26273) läuft seit Januar 2001 und endet im Dezember 2002. Das SABRINA-Projekt wird erste Produktbeispiele einer Sensoreinheit, verbunden mit einer generischen Applikationsplattform für verschiedene Testszenarien, entwickeln. Die Hauptaufgabe des Projektes ist die Entwicklung einer sicheren Authentifizierung durch persönliche Merkmale, basierend auf Ultraschallabtastung von Teilen der menschlichen Haut. Der Förderbetrag liegt bei 2,09 Mio. Euro. Prime-Contractor ist die Hitex-Systementwicklung, Gesellschaft für Angewandte Informatik M.b.H – Hitex Automation (D). Partner sind das Forschungszentrum Informatik an der Universität Karlsruhe (D), Non Standard Logics Limited (UK), Avantgarde Products Vollert (D), Infostrada S.p.a. (I), die Universität Karlsruhe (D) sowie Brokat Infosystems 76 (D).

– Projekt „U-FACE – User friendly face access control system for physical access and healthcare applications“ (Ref.-Nr. IST-1999-11587): Ziel des Projektes ist es, Gesichtserkennungsalgorithmen im Zusammenhang mit der Nutzung von Smartcards, insbesondere für physikalische Zugangskontrollen im Finanzbereich und für Patientendateien, zu verbessern sowie Prototypen herzustellen. Das Projekt wurde im April 2000 gestartet und dauert 30 Monate, gefördert mit 700 000 Euro. Prime Contractor ist die Firma Visual Automation Limited, Manchester (UK), weitere Partner sind Netsmart S. A., Athen (G), Biotrast S. A., Thessaloniki (G), Interactive Labs S.r.l., Florenz (I), die Organisation Social Solidarity, Thessaloniki (G), sowie die Victoria University of Manchester (UK).

Ein weiteres aktuelles EU-Projekt im Rahmen des IST-Programms behandelt den Einsatz einer europäischen Bürgerkarte mit biometrischer Komponente (Smartcard mit Fingerbildsensor), die bei Wohnungswechseln in der EU genutzt werden könnte, nicht aber als Passersatz bzw. Ausweis dienen soll. Das Projekt nennt sich FASME („Facilitating Administrative Services für Mobile Europeans“, http://www.fasme.org) und wird von einem Konsortium mehrerer Städte (Grosseto, Köln, Newcastle), Universitäten (Amsterdam, Köln, Rostock, Zürich) und Firmen (ICL, ZUENDEL & Partner) betrieben.

Erkennbar ist somit ein durchaus intensives und umfassendes Engagement der EU bei Erforschung und Förderung der Anwendungen der Biometrie. Eine Überblicksstudie zu den Einsatzmöglichkeiten und den gesellschaftlichen und politischen Implikationen biometrischer Technologien hatte die EU-Kommission bereits im Jahr 1997 erstellen lassen (Polemi 1997).

IV. Biometrische Verfahren in der Praxis

Biometrische Identifikationssysteme eröffnen – wie im Folgenden gezeigt wird – eine Vielfalt von Anwendungsmöglichkeiten. Es gibt eine große und ständig wachsende Zahl von Berichten über konkrete Nutzungen in zahlreichen Einsatzfeldern, insbesondere aus den USA, aber auch aus europäischen und asiatischen Ländern. Quantitative Angaben und Abschätzungen zu Umsatzzahlen und Marktanteilen sowie vor allem zu deren weiterer Entwicklung finden sich schon viel seltener, und wenn, sind sie wegen ihrer Unschärfen in der Regel nur „mit großer Vorsicht zu genießen“. Allerdings ist es methodisch auch schwierig, den eigentlichen „biometrischen“ Anteil einer Gesamttechnologie zu definieren, abzugrenzen und wertmäßig zu beziffern. Auch die Daten der amtlichen Statistiken liefern keine Grundlage, um relevante Kennziffern für biometrische Produkte und Dienstleistungen (Produktionsumfang, Umsätze, Beschäftigte u. Ä.) zu erhalten. Darüber hinaus verfolgen die beteiligten Firmen oft eine eher restriktive Informationspolitik.

1. Anwendungsfelder und -beispiele

Der Einsatz biometrischer Identifikationssysteme erfolgte bis vor einigen Jahren fast ausschließlich zu Sicherheitszwecken, z. B. bei der Zutrittskontrolle in hoch sensiblen Bereichen wie Kernkraftwerken, Gefängnissen oder Rechenzentren. In der Folge wurden nach und nach weitere Anwendungsfelder in Unternehmen und Behörden erschlossen. Der stärkste Antrieb zur intensiveren Nutzung biometrischer Verfahren entstand in jüngster Zeit infolge der Erwartung einer Ausweitung des elektronischen Handels und des damit einhergehenden Bedarfs an einfacheren und sichereren Authentifizierungsmöglichkeiten. Im Rahmen der Diskussion über Maßnahmen zur Erhöhung der inneren Sicherheit nach den terroristischen Anschlägen in den USA im September 2001 hat der Einsatz biometrischer Systeme neue Aufmerksamkeit auch in Europa erfahren.

Bisherige und absehbare Einsatzfelder (Tabelle 9; Kapitel IV.1.5) können grob in fünf Gruppen eingeteilt werden (Behrens/Roth 2001, S. 42 f.):

– Benutzerzugangssicherung,

– Personenidentifikation,

– Gerätezugangskontrolle,

– elektronischer Zugang zu Dienstleistungen (E-Banking und E-Commerce),

– sonstige „Conveniencebereiche“.[2]

[2] Die Beispiele der folgenden Abschnitte entstammen überwiegend (Behrens/Roth 2001) sowie (Albrecht 2001) und gehen häufig auf (Newham et al. 1999), (Lockie 2000) bzw. (Lockie/Deravie 2000) und (Simon 2000) zurück.

1.1 Benutzerzugangssicherung

Diese fast schon „klassisch“ zu nennende Anwendung der Biometrie reicht von der Zugangssicherung zu einem Gelände oder Gebäude bis hin zu Krankenhausapotheken oder Bankschließfächern.

Grundsätzlich genügt eine biometrische Verifikation des Nutzers zur Zugangsautorisierung. Eine niedrige FAR (Rate falscher Akzeptanz) ist notwendig, um ein gewünschtes hohes Sicherheitsniveau zu gewährleisten. Wegen der technischen Unausgereiftheit der Systeme geht eine solche niedrige FAR oft einher mit einer verhältnismäßig hohen FRR (Rate falscher Ablehnung). Diese wiederum ist jedoch meist akzeptabel, da aufgrund der begrenzten Nutzerzahl eine Ersatz-Autorisierung problemlos „manuell“ erfolgen kann. Bei einigen dieser Anwendungen besteht ein fließender Übergang zum nächsten Anwendungstyp, der Personenidentifikation.

Beispiele für biometrisch gesicherte Bereiche in der Literatur (verschiedene Quellen; „genutztes“ Merkmal in […]):

- das US-amerikanische Verteidigungsministerium [Hand],
- alle 75 Bundesgefängnisse der USA sowie Gefängnisse in Großbritannien und den Niederlanden [diverse Systeme],
- Olympisches Dorf in Atlanta 1996 [Hand],
- eine Marinewerft in Indien (gleichzeitig Zeiterfassung) [Gesicht],
- Privatschulen in Japan und Großbritannien (gleichzeitig Anwesenheitskontrolle von Schülern und Mitarbeitern) [Fingerbild],
- Diskotheken und Nachtklubs [v. a. Gesicht, auch Fingerbild],
- Mitarbeiter- und Sicherheitszonen in Flughäfen weltweit [diverse Systeme, z. B. Fingerbild: Frankfurt/Main; Gesicht: London Heathrow],
- Criminal Justice Information Services Center der US-amerikanischen Bundespolizei FBI [Fingerbild],
- Kernbereiche des Trustcenters bei der Regulierungsbehörde für Post- und Telekommunikation (Mainz) [Fingerbild],
- Teilbereiche US-amerikanischer Hochschulen, wie Labore, Computerräume oder Wohnheime [diverse Systeme],
- Räume der Geschäftsführung von Unternehmen (Deutsche Bank, Frankfurt am Main) [Gesicht],
- Krankenhausapotheke (Humana Hospital Aubadon, USA) [Stimme],
- Schließfächer (Zuger Kantonal Bank, Schweiz) [Fingerbild], (Dresdner Bank, Frankfurt am Main) [Gesicht],
- Biathlonmunition (Olympische Winterspiele 1998, Nagano, Japan) [Iris].

1.2 Personenidentifikation

Bei der eindeutigen Identifikation einer Person werden gegenüber der bloßen Verifikation weitaus höhere Anforderungen an ein biometrisches System gestellt. Es fallen weitaus größere Datenmengen an, die an einer zentralen Stelle gespeichert und verarbeitet werden müssen. Die Anwendungskontexte erfordern z. T. eine Verbindung zu hochsensiblen Informationen z. B. polizeilicher Art, sodass Fragen des Datenschutzes hier eine besondere Rolle spielen. Wegen der Größe der Nutzergruppen und der Bedeutung der Zwecke bzw. der Missbrauchspotenziale sind höchste Anforderungen an die technische Ausgereiftheit der biometrischen Systeme (sowohl niedrige FAR als auch FRR!) zu stellen.

Drei zentrale Zwecke der Personenidentifikation sind die – polizeiliche – Überwachung öffentlicher Orte (zu Abschreckungs- wie zu Fahndungszwecken), die Verbesserung des Identitäts- bzw. Legitimationsnachweises (z. B. Führerschein, aber auch Personalausweise o. Ä.) sowie die Kontrolle der Gewährung bzw. die Vermeidung des Missbrauchs von staatlichen (Sozial-)Leistungen oder von Leistungen im Rahmen der Gesundheitsversorgung:

- Der Einsatz von Gesichtserkennungssystemen im Rahmen der Überwachung öffentlicher Straßen und Plätze wird in Europa vor allem aus Großbritannien berichtet. Für Schlagzeilen gesorgt hat das Beispiel des Londoner Stadtteils Newham, in dessen Einkaufszone weit über 100 Kameras aufgestellt worden sind, deren Bilder einem ständigen Abgleich durch ein Gesichtserkennungssystem mit einer Datenbank Verdächtiger oder ehemaliger Krimineller unterzogen werden. Diese datenschutzrechtlich hoch umstrittene Maßnahme soll zumindest anfangs die Kriminalitätsrate in dem überwachten Gebiet um 40 % gesenkt haben. Bekannt geworden ist auch der Einsatz von

Gesichtserkennung zur Überprüfung der Besucher einer Begegnung zwischen den Fußballvereinen West Ham United und Manchester United Ende 1999, um bekannte Hooligans zu identifizieren. Mobile Kameras wurden an strategisch wichtigen Punkten außerhalb des Stadions aufgebaut.

– Ein entsprechender Überwachungsvorgang beim American-Football-Finale in den USA („Superbowl") in Tampa im Februar 2001 hat eine heftige Diskussion in den USA über die Bedrohung von Bürgerrechten durch Biometrie ausgelöst.

– Ebenfalls aus den USA stammen zwei Beispiele für biometriegestützte Führerscheine (Texas und Georgia), die zumindest im Rahmen von Polizeikontrollen auch als Identitätsnachweise dienen. Das Missbrauchspotenzial muss durch die mögliche Verbindung zu anderen staatlichen Informationspools als hoch eingeschätzt werden. Pläne für eine kommerzielle Verwertung (Verkauf der Daten an ein privates Unternehmen, das eine Identitätsprüfung z. B. bei Verkäufen als Dienstleistung anbieten wollte) wurden erst nach öffentlichem Protest eingestellt (Albrecht 2001, S. 70).

– Überlegungen zur biometrischen „Ausrüstung" von Identitätspapieren existieren in vielen Staaten, konkrete Pläne bestehen u. a. in Indonesien, Kolumbien und Südafrika. Auch die deutsche Bundesdruckerei schätzt die Integration biometrischer Komponenten als wichtiges Element zukünftiger Personaldokumente ein und befasst sich seit längerem mit entsprechenden Möglichkeiten (Landvogt 2000, nach Albrecht 2001).

– Zur Identifikation und vereinfachten Abfertigung von Vielfliegern werden Handerkennungssysteme seit Jahren an den Flughäfen von New Jersey, New York, Miami und Washington D. C. sowie in Kanada und Singapur eingesetzt.

– Eine spezielle Anwendung wird anscheinend in den Parlamenten von Kolumbien, Venezuela und der Türkei praktiziert. Hier werden biometrische Identifikationen im Rahmen von Abstimmungsverfahren der Abgeordneten durchgeführt, um die stellvertretende Abgabe von Stimmen zu verhindern. In Jamaika existieren Pläne, Biometrie als Identifikationsverfahren für die Wahlberechtigten einzusetzen.

– Im Falle von Asylbewerberausweisen verbinden sich die Ziele der Kontrolle mit denen der Leistungsbegrenzung bzw. Missbrauchsverhinderung. So erhalten in den Niederlanden Asylbewerber, die in Übergangscamps leben, eine Fingerbild-Smartcard, mit deren Hilfe sie ihren Aufenthalt in dem Camp – das sie nicht eigenmächtig verlassen dürfen – mehrmals am Tag bestätigen müssen. Die deutsche Bundesregierung hat eine Machbarkeitsstudie zu einer multifunktionalen so genannten „AsylCard" durchführen lassen. Sowohl der hessische als auch der schleswig-holsteinische Datenschutzbeauftragte haben sich klar gegen ein solches Projekt ausgesprochen (Albrecht 2001, S. 13). Bereits jetzt werden auf nationaler Ebene automatische Fingerbild-Identifikations-Systeme (AFIS) bei der Asylbewerbung eingesetzt (u. a. in Deutschland, Belgien, Frankreich), die EU plant, ein länderübergreifendes System einzurichten (EURODAC), um doppelte Antragstellung zu vermeiden.

– Die biometrische Ausstattung von Sozialversicherungsausweisen bzw. die Nutzung biometrischer Verfahren bei der Auszahlung von Renten und anderen staatlichen Leistungen wird u. a. in vielen US-Bundesstaaten, in Südafrika und auf den Philippinen bereits praktiziert (meist Fingerbilderkennung).

– Die o. g. europäische Bürgerkarte, die im Projekt FASME erprobt wird (Kapitel III.2), stellt eine Anwendung im Zwischenbereich von Identitätsnachweis, Leistungsgewährung und elektronischem Zugang zu Dienstleistungen (Kapitel IV.1.4) dar.

– Etwas bizarr klingen Berichte über die Verwendung von Fingerbilderkennungsverfahren in Kantinen US-amerikanischer Schulen. Als Vorteile werden die Einsparung von Kosten, der Wegfall diskriminierender Situationen für sozial Schwache (kostenlose Essensausgabe nicht länger erkennbar) und die Kontrolle und gegebenenfalls Steuerung des Essverhaltens der Schüler durch ihre Eltern genannt (Albrecht 2001, S. 14).

– In den Niederlanden werden Handgeometriesysteme in Methadonprogrammen eingesetzt. Die beteiligten drogenabhängigen Patienten können nach erfolgter Authentisierung mehrere Tagesrationen auf einmal erhalten (Albrecht 2001, S. 15 f.).

– Ebenfalls in den Niederlanden wird im so genannten „Parkinson-Projekt" eine Krankenkarte mit Fingerbilderkennung entwickelt, die dem behandelnden Arzt einen Überblick über die Krankengeschichte verschaffen soll. Die Fingerbilderkennung wurde als einziges biometrisches System identifiziert, das von denjenigen Parkinson-Patienten, die durch das Zittern ihrer Hände beeinträchtigt sind, noch ohne fremde Hilfe benutzt werden kann (Albrecht 2001, S. 15).

1.3 Gerätezugangskontrolle

Die biometrische Nutzersicherung von elektronischen und sonstigen Geräten ist gewissermaßen eine Variante der Benutzerzugangssicherung. Eine Verifikation genügt immer, eine Integration in größere Sicherungssysteme ist meist nicht nötig. Verglichen mit o. g. Sicherheitszonen ist die Möglichkeit, durch falsch erteilte Zugangsberechtigung Schaden zu verursachen, in der Regel begrenzt. Deshalb kann eine höhere FAR akzeptiert werden, zugunsten einer niedrigen FRR, die für eine verlässliche und komfortable Nutzung nötig ist. Da also die technischen Anforderungen auf einem mittleren Niveau anzusiedeln sind und auch kaum Schwierigkeiten bei der Datenverwaltung (z. B. datenschutzrechtlich) entstehen, finden sich auf diesem Sektor die ausgereiftesten neuartigen, für den privaten Gebrauch konzipierten Biometrie-Anwendungen, z. B. bei:

- Mobiltelefone & Personal Digital Assistants (PDAs): Sowohl Fingerbildtechnik als auch Gesichts- (v. a. bei zukünftigen UMTS-Telefonen) und Sprechererkennung als PIN-Ersatz sind anwendungsreif, haben aber noch kaum Verbreitung gefunden. Da die bisherige PIN-Sicherung von den meisten Nutzern deaktiviert wird, würde Biometrie bei Handys auf jeden Fall einen Sicherheitszugewinn bedeuten. Für PDAs gibt es mehrere Softwareentwicklungen zur handschriftlichen Authentifizierung: Die Firma Sign-On bietet eine Software für das Palm-OS-Betriebssystem an, während die Platanista GmbH an einer geräteunabhängigen Handschriften-Authentifizierungs-Software arbeitet. Weitere Entwicklungen im PDA-Bereich werden u. a. von der Fa. Mikromatics (http://www.pdalok.com) evaluiert (Platanista 2001a).
- PCs: Bei hochwertigen Laptops werden zunehmend biometrische Systeme als Missbrauchsschutz angeboten (Fingerbild- oder Gesichtserkennung); für Desktop-Systeme existiert eine Vielzahl von Lösungen verschiedener Anbieter, die den Rechner bzw. die Tastatur (Fa. Cherry) oder die Maus (Microsoft) v. a. mittels Fingerbilderfassung sichern.
- Geldausgabeautomaten: Während in Deutschland bislang nur bankeninterne Pilotversuche durchgeführt worden sind (neben dem o. g. BioTrusT-Projekt z. B. bei einer Filiale der Dresdner Bank), finden sich in den USA Beispiele für „echte“ Anwendungen. Die Bank United hat nach eigenen Angaben mit großem Kundenerfolg Iriserkennungssysteme in mehreren Filialen installiert, die Wells Fargo Bank plant in Zusammenarbeit mit „Mr. Payroll“, über 1 000 Scheckeinlösungs-Automaten mit Gesichtserkennung aufzustellen. (Die Inkassonahme von Schecks hat in den USA nach wie vor eine hohe praktische Bedeutung, da laut Schätzungen 37 Mio. US-Amerikaner kein Bankkonto besitzen.)
- Waffen, Kfz, Spielzeug: Ebenfalls aus den USA stammen Beispiele für biometriegestützte Schusswaffensicherung (mittels einer Infrarot-Handerkennung), v. a. von Polizei-Dienstwaffen (seit 1994 gefördert durch die so genannte „Smart Gun Initiative“ des US-Justiz-Ministeriums). Eine ähnliche Funktion erfüllen (meist fingerbildbasierte) biometrische Wegfahrsperren, die in Kfz der Oberklasse in Zukunft als Standardmöglichkeit angeboten werden dürften. Teils skurril, teils banal wirken Hinweise auf biometrisch ausgerüstete elektronische Spielzeuge, wie ein Tagebuch für Kinder (aus den USA) oder ein „Computerhund“ (aus Japan), die bislang allerdings eher spracherkennende Passwortsysteme nutzen.

1.4 Elektronischer Zugang zu Informationen und Dienstleistungen

Anwendungen im Bereich E-Commerce werden zwar häufig als Haupttriebfeder des zukünftigen Einsatzes biometrischer Systeme genannt, real existieren allerdings nur wenige Anwendungsbeispiele. Ein Grund dafür ist, dass die technischen Anforderungen (gleichzeitig niedrige FAR und FRR) eher hoch sind und die Entwicklung daher kostenintensiv ist. Hinzu kommen Daten- und Verbraucherschutzaspekte, die einer schnelle Verbreitung hinderlich sind.

- Electronic Banking: Weltweit werden von vielen Banken biometrische Systeme auf ihre Eignung getestet, bislang meist nur firmenintern (so auch im deutschen BioTrusT-Projekt der S-Finanzgruppe; Kapitel III.1.2). Beispiele sind Versuche zum Einsatz von Fingerbilderkennung beim Online-Banking der kanadischen Tochter der niederländischen Bankgruppe ING oder von Sprechererkennung beim Telefon-Banking der britischen Bank „Nationwide“ (s. auch das EU-Projekt BANCA; Kapitel III.2).
- Electronic Shopping: Beim Einkauf via Telefon wird die Anwendung von Sprechererkennung anscheinend genutzt, von „echten“ Internethändlern sind bislang lediglich konzeptionelle Vorschläge bzw. Überlegungen bekannt (s. auch das EU-Projekt BEE; Kapitel III.2).
- Firmeninterne und -externe Kommunikationssysteme: Sprechererkennung bildet eine Identifizierungs- und Sicherheitsmaßnahme für umfangreiches Außendienstpersonal, z. B. einer Großbäckerei in den USA, oder bei der Abrufung vertraulicher Informationen durch Flugbesatzungen. Auch andere – z. B. über das Internet verteilte – geschlossene Benutzergruppen (Virtual Private Networks, VPN) können biometrisch autorisiert werden.
- Nahe liegend wäre der Einsatz biometrischer Systeme zur Absicherung der so genannten Digitalen Signatur als Voraussetzung für eine Ausweitung der „Elektronischen Verwaltung“ (E-Government), also der Abwicklung von behördlichen Verwaltungsakten zwischen Bürgern und öffentlicher Verwaltung, wie z. B. Abgabe der Steuererklärung, Melde- und Personenstandsangelegenheiten – möglicherweise bis hin zur elektronischen Stimmabgabe bei Wahlen. Bisherige Pilotprojekte, z. B. Medi@Komm (http://www.mediakomm.net), nutzen allerdings noch konventionelle Authentifizierungsverfahren wie Passwörter. Das neue deutsche Signaturgesetz sieht den Einsatz biometrischer Verfahren jedoch bereits explizit als Möglichkeit vor (Kapitel V.2).

1.5 Conveniencebereiche

Viele Experten vermuten das größte Potenzial für biometrische Anwendungen bei der Komforterhöhung in Alltagssituationen. Hierzu gehört eigentlich der gesamte E-Commerce-Bereich – vorausgesetzt, der Zahlungsvorgang wird vereinfacht, z. B. im Rahmen des so genannten Micropayment („Centbeträge“ für einzelne Datenbankauszüge oder Musiktitel). Bereits genutzt werden in US-amerikanischen Selbstbedienungsläden fingerbildbasierte Systeme, mittels derer die Kunden ohne Hilfe des Personals die gewünschte Ware erfassen und bezahlen können. Der Komforterhöhung dienen soll auch die biometrie-

gestützte automatische Erkennung und Zuordnung individueller Einstellungsvarianten von bedienungsintensiven Geräten wie (Behrens/Roth 2001, S. 58):

– Heizungs- und Beleuchtungsanlagen,

– Unterhaltungselektronik,

– Kraftfahrzeugen (Sitz- und Spiegeleinstellungen, Klimaanlage, Radiosender und Autotelefon) oder auch

– einer Kaffeemaschine, die in Abhängigkeit vom identifizierten Nutzer und seinen gespeicherten Vorlieben die Kaffeestärke wählt (Demonstration der Fa. Siemens auf der CeBit).

Noch existieren diese Anwendungsbeispiele zum ganz überwiegenden Teil als Vorschläge, Labormuster oder Messeprototypen.

Tabelle 10 illustriert und charakterisiert in einem Überblick zusammenfassend wichtige Anwendungsbereiche anhand der jeweils vorrangig bestimmenden Optimierungskriterien (FAR oder FRR), nennt die jeweils bevorzugt eingesetzten biometrischen Systeme und deren Verbreitung sowie Beispiele für Einzelanwendungen und Anwender.

1.6 Internetanwendungen und das Problem der Referenzdaten

Bei der Diskussion über die Anwendungsmöglichkeiten biometrischer Verfahren wird regelmäßig auf das Internet, insbesondere auf E-Banking und E-Commerce, verwiesen (Kapitel IV.1.4). Dagegen wird bei Einschätzungen und Stellungnahmen zu Sicherheitsproblemen im Internet und deren Lösungen das Thema Biometrie bislang kaum konkret angesprochen. Deshalb wurde die Platanista GmbH durch das TAB beauftragt, im Rahmen einer Kurzexpertise gezielt der Frage „Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet“ nachzugehen. Die Recherchen bestätigten den Eindruck, dass das Thema bislang noch recht verhalten diskutiert wird, auch wenn gleichzeitig eine Vielzahl von Firmenaktivitäten erkennbar wurde.

Die Rechercheergebnisse der Platanista GmbH (2001b), v. a. in Form von Projekt- und Produktbeschreibungen, werden in Anhang 3 wiedergegeben bzw. zusammengefasst.

Ein recht weit entwickeltes und zunehmend erfolgreiches Produkt ist das Unterschrifterkennungssystem CyberSIGN, das in den USA u. a. im Gesundheitswesen (Patientendokumentierung, Auftrags- und Terminplanung in

Tabelle 10

Biometrische Verfahren in der Praxis

Einsatzbereich	Optimierungs-parameter	vorrangig genutzte Verfahren	Verbreitung	Anwendungen und Anwender
Bankensektor	FRR (+ FAR)	Fingerbild, Iris, Unterschrift	Pilotprojekte	Kreditkarten, Überweisungen, Geldautomat
Computer-Sicherheit	FAR	Fingerbild, Gesicht, Handschrift	gering bis mittel	PC- und Netzwerk-Zugang
E-Commerce/ Internet	FAR (+ FRR)	Fingerbild, Gesicht, Unter- und Handschrift, Stimme	k. A.	Einzelhandel, Vermittlung, Beratungsdienste
Recht, öffentliche Sicherheit	FAR	Fingerbild, Gesicht, Unter- und Handschrift, Iris	Pilotprojekte	Einwanderung, Überwachung, Betrugsvorbeugung, Einreisekontrolle
nationale Sicherheit	FAR	Fingerbild, Gesicht, Iris, Handgeometrie, Stimme	Pilotprojekte	Militär, Spionage- und Terrorismusbekämpfung
Behörden/ Unternehmen	FAR	Fingerbild, Gesicht, Handschrift, Stimme	gering bis mittel	Finanzamt, Versicherungen, Vielflieger, Arbeitsstätte
Gesundheit	FRR	Fingerbild, Gesicht, Handschrift	Pilotprojekte	Krankenkassen, Ärzte, Apotheken
Telekommunikation	FRR	Fingerbild, Stimme	gering	Zugang zu mobilen Endgeräten
privater Raum	FRR	Fingerbild, Gesicht, Handschrift, Stimme	gering	Zugang zu Auto, Haus, PC

Quelle: Platanista 2001a

Krankenhäusern), als Zugriffsschutz für Regierungsdokumente (z. B. bei der Food and Drug Administration, FDA) und bei E-Banking und E-Commerce zur Authentifizierung eingesetzt wird (Platanista 2001b, S. 16).

Speziell im Hinblick auf die Erweiterung der Internetapplikationen haben sich Ende 2000 die drei Firmen Adobe (http://www.adobe.com), Cardiff (http:// www.cardiff.com) und CyberSIGN (http://www.cybersign.com) zusammengeschlossen. Adobe liefert das weit verbreitete Dokumentenformat PDF, Cardiff die elektronische Formularverarbeitung und CyberSIGN das elektronische Signaturverfahren, das den Regeln des amerikanischen Signaturgesetzes entspricht. Die elektronische Signatur wird verbunden mit den elektronischen Formularen von CARDIFF und direkt in PDF-Dokumente eingebunden. Eine Erweiterung der Anwendungsmöglichkeiten bietet ein Grafiktablett der Firma Wacom, das die Handschrift direkt über das Display aufnimmt. Als Anwender kommen insbesondere Ärzte, Architekten und Ingenieure infrage, die durch ihre zusätzlich eingefügte Unterschrift die auf dem Bildschirm bzw. Dokument veränderten oder hinzugefügten Informationen authentifizieren könnten (Platanista 2001b, S. 16 f.).

Bei zukünftigen Internetanwendungen biometrischer Systeme stellen sich Fragen der Referenzdatenaufnahme, -übermittlung und -verwaltung besonders intensiv. Schon in klassischen Filialbetrieben wie Banken und Sparkassen ist noch unklar, ob und wie flächendeckend die erforderlichen technischen und personellen Kapazitäten zum sicheren Enrolment (der Referenzdatenaufnahme, Kapitel II.1) etabliert werden können oder ob den Kunden dabei zusätzliche und weitere Wege als bislang aufgebürdet werden müssen (Platanista 2001b, S. 17 f.).

Nach erfolgreicher Referenzdatenaufnahme schließen sich z. B. im Fall der Erstellung einer Smartcard (als dezentraler Datenspeicher in der Verfügungsgewalt der Nutzer) zwei weitere problematische Phasen an: zuerst der Transfer der Referenzdaten auf die Smartcard (bzw. den Ort der technischen Einrichtung, in der die Smartcards produziert werden), danach die Auslieferung der Smartcards an die Kunden. In Deutschland schließen die Banken derzeit noch einen Direktversand aus, geeignete Lösungsmöglichkeiten werden noch gesucht (Stand Juni 2001; http://www.biotrust.de/WS050601.htm).

Bei Internetanbietern, deren Vorteil ja unter anderem in der Vermeidung der physischen Kontaktaufnahme mit ihren Kunden besteht, wird u. a. wegen fehlender Filialen das Problem des Enrolments noch größer sein. Hinzu kommen Schwierigkeiten, dezentrale Datenspeichervarianten, die von Daten- und Verbraucherschützern präferiert werden, wie die genannten Smartcards, zu nutzen, da hierfür jeder Nutzer ein Kartenlesegerät besitzen müsste. Näher liegend sind daher abgesicherte Online-Server-Systeme, die z. B. bei Unterschriftensystemen wie dem o. g. CyberSIGN eingesetzt werden (wobei auch hier grundsätzlich ein Zusatz-Kundengerät erforderlich ist, das Grafiktablett o. Ä.) (Platanista 2001b, S. 18).

Das Wachstumspotenzial für Internetanwendungen biometrischer Systeme ist zweifellos groß. Will man es tatsächlich ausschöpfen, sind allerdings noch viele technische und ökonomische Probleme zu lösen. Außer Unterschriftsystemen werden zurzeit vor allem der Fingerbilderfassung größere Chancen eingeräumt, sich zu etablieren. Noch erscheinen die anderen Systeme entweder technisch zu anfällig bzw. unsicher (Stimme, Gesicht) oder aber technisch zu aufwendig (Iris, Handgeometrie) (vgl. Kapitel II.3).

2. Markteinschätzung

Der Begriff „Einschätzung“ (im Titel dieses Abschnitts) bezieht sich nicht nur auf die Zukunft, sondern charakterisiert auch die aktuelle Datenlage bei den wirtschaftlichen Kennziffern: Es gibt keine verlässlichen und damit aussagekräftigen amtlichen Statistiken, sondern nur Marktanalysen von verschiedenen Beratungsunternehmen. Weil deren Datengrundlagen, Erhebungsmethoden und Abgrenzungen wenig nachvollziehbar und wenig transparent sind, werden an dieser Stelle lediglich einige knappe Schlussfolgerungen der Auswertung der Ergebnisse von Behrens und Roth (2001)[3] präsentiert (eine ausführlichere Darstellung der Datenlage findet sich in Anhang 4):

– Die Zahl der Firmen, die biometrische Systeme entwickeln/anbieten, betrug im Jahr 2000 ca. 200 (Lockie 2000) und dürfte inzwischen weiter zugenommen haben. Die dominierende Technologie (ca. 40 % der Unternehmen) sind die Fingerbildverfahren, gefolgt von Gesichts- und Sprechererkennung (je ca. 15 %), Unter-/Handschrift und Handgeometrie. Bei Iris- und Retina-Scan gibt es nur wenige Anbieter. Sollte die Biometrie in eine fortgeschrittenere Diffusionsphase eintreten, wird eine Reduktion der Firmenvielfalt durch Fusionen und Übernahmen erwartet.

– Auch bei den Markterlösen – mit von Quelle zu Quelle und Jahr zu Jahr sehr unterschiedlichen Angaben (Anhang 4, Abbildung 10 und 11) – führt die Fingerbilderkennung (bei steigender Tendenz, mit bis zu 50 % des Gesamtumsatzes) vor der Gesichtserfassung (zunehmende Tendenz) und der Handvermessung (abnehmend), es folgen die Merkmale Stimme (abnehmend), Iris/Retina (zunehmend) und Handschrift.

– Die Angaben zur Verteilung der Umsätze auf die verschiedenen Anwendungsfelder (Anhang 4, Abbildung 12 und 13) sind so widersprüchlich und unklar, dass keine Schlüsse aus ihnen gezogen werden können.

– Zur Verteilung der Umsätze auf Weltregionen findet sich – trotz vorhandener Unterschiede der Quellen bei den Einzelwerten – eine gemeinsame Grundeinschätzung (Anhang 4, Abbildung 14 und 15): Der Markt in

[3] Behrens und Roth haben folgende Berichte ausgewertet: Frost & Sullivan 1999 u. 2000a, Lockie 2000, IBG 2000, Morgan Keegan 2000 (Behrens/Roth 2001, S. 64 ff.). Die Gutachter der Platanista GmbH haben Daten aus Biometric Consortium 1999, Frost & Sullivan 2000b, IBG 2001 und IBIA 2001 ergänzt (Platanista 2001a).

Nordamerika dominiert ganz deutlich (60 bis 70 % der weltweiten Umsätze), mit weitem Abstand folgt Europa (10 bis 25 %), danach kommen Asien und Lateinamerika (jeweils 5 bis 10 %).

– Die Unschärfen der „Analysen“ wird besonders augenfällig bei den absoluten Umsatzzahlen bzw. -prognosen: Zum einen verändern bzw. erhöhen die Analysten ihre eigenen Prognosen (z. B. für 2003 in Europa: von 40 Mio. auf 80 Mio. US-$), aber auch ihre Angaben für zurückliegende Zeiträume (für 1997 in Europa: 25 vs. 12 Mio. US-$) von Jahr zu Jahr erheblich (vgl. Daten von Frost & Sullivan 1999 u. 2000a u. b; Anhang 4), zum andern unterscheiden sich die Zahlen zwischen den Quellen (Frost & Sullivan 1999 vs. Morgan Keegan 2000) um bis zu Faktor 10 (z. B. Annahmen für den Umsatz in Nordamerika im Jahr 2002 zwischen 100 Mio. und 1 Mrd. US-$).

– Daten über Umsätze und deren Verteilung auf Technologien oder Anwendungsfelder für Deutschland fehlen völlig. Frost & Sullivan (1999 u. 2000a) verorten die Bundesrepublik als größten Markt innerhalb Europas, prognostizieren allerdings für die kommenden Jahre – bei insgesamt steigenden Werten – einen abnehmenden Umsatzanteil gegenüber anderen europäischen Ländern.

Für die Unterschiede bei den Umsatzzahlen der Vergangenheit dürften – neben der bereits genannten mangelnden Auskunftsbereitschaft von Produzenten und Anwendern – vor allem Abgrenzungsprobleme bzw. -unterschiede verantwortlich sein. Differenzen bis zu einer Zehnerpotenz können leicht entstehen, wenn – wie zu vermuten ist – völlig unterschiedliche Ausschnitte der Wertschöpfungskette als Grundlage für die Berechnungen dienen (z. B. Fingerbildsensor allein vs. Gesamtsystem wie Geldausgabeautomat; Behrens/Roth 2001, S. 75).

Auf der Basis der verfügbaren Zahlen erscheint es daher nicht möglich, das zukünftige Marktgeschehen einigermaßen verlässlich zu beschreiben. Prognosen müssten die höchst schwierige Frage beantworten, in welchen Bereichen sich biometrische Verfahren in welchem Umfang durchsetzen werden. Büllingen und Hillebrand verweisen auf die Delphi-Umfrage im Auftrag des BMBF von 1998, nach der ein Ersatz der PIN durch biometrische Verfahren zwischen 2006 und 2010 erwartet wurde (WIK 2000, S. 10). Es wird vermutlich entscheidend vom weiteren Verlauf der Diskussion um die Aufnahme biometrischer Merkmale in Pässe und Personalausweise und die dabei politisch-rechtlich zu beantwortenden Fragen von Daten- und Verbraucherschutz (Kapitel V.) abhängen, ob sich auch im privatwirtschaftlichen Sektor in absehbarer Zeit eine so genannte „killer application“ (WIK 2000, S. 15) bei einer ausreichend großen Zahl von Nutzern (E-Banking oder E-Commerce, Gerätezugang zu PCs oder Mobiltelefonen) durchsetzen kann.

V. Verbraucherpolitik, Recht, Datenschutz

Die weltweiten Forschungs- und Entwicklungsaktivitäten sowie die zunehmend erkennbare Ausweitung von Einsatzfeldern signalisieren die Möglichkeit, dass biometrische Verfahren schon bald den gesellschaftlichen Alltag durchdringen werden. Deshalb gewinnen Fragen des Verbraucherschutzes, der rechtlichen Rahmenbedingungen sowie insbesondere des Datenschutzes an Bedeutung. In diesem Kapitel wird der Stand der Diskussion bzw. der augenblicklichen Rechtslage in einem ersten Überblick skizziert.

1. Verbraucherpolitische Anforderungen an die Biometrie

Vertreter des Verbraucherschutzes begleiten die Entwicklung der Biometrie in Deutschland bereits seit einiger Zeit. Praktische Erfahrungen mit dem Versuch, den Einsatz biometrischer Verfahren in diversen Anwendungsfeldern sicher, vertrauenswürdig, verbraucherfreundlich und sozialverträglich zu gestalten, werden vor allem im Rahmen und im Kontext des Projekts BioTrusT (Arbeitsgruppe 6 „Biometrische Identifikationssysteme“ von TeleTrust e.V.) gesammelt. Sein Zweck ist es, verschiedene biometrische Verfahren in spezifischen Anwendungsszenarien wie Zutrittskontrolle, PC-Zugangskontrolle, Einsatz an Geldautomaten und im Homebanking zu untersuchen und vergleichend zu bewerten (Kapitel III.1.2).

Im Projekt befasst sich u. a. die Arbeitsgemeinschaft der Verbraucherverbände e.V. (AgV) (seit 2001 Verbraucherzentrale Bundesverband e.V. als Rechtsnachfolgerin) mit Fragen der Akzeptanz und Nutzerfreundlichkeit sowie der rechtlichen Gestaltung des Einsatzes biometrischer Systeme. Auf Vorschlag des TAB wurde Frau Rechtsanwältin Astrid Albrecht mit einem Gutachten zu den verbraucherpolitischen Aspekten beauftragt. Dessen Ergebnisse bilden die Grundlage der folgenden Ausführungen (Albrecht 2001).

Die Ambivalenz von Technologien zeigt sich auch im Fall der Biometrie: Biometrische Verfahren können dank der Verwendung personengebundener Merkmale sicheres Erkennen und Identifizieren ermöglichen. Zugleich aber können sie zur Durchleuchtung und umfassenden Überwachung des Bürgers verwendet werden und zur Diskriminierung von Einzelnen oder Bevölkerungsgruppen führen. Sollen die Chancen der Biometrie genutzt und die Risiken beherrscht werden, so müssen Gestaltung und Anwendung biometrischer Systeme bestimmte Kriterien erfüllen. Dazu zählen vor allem:

– hohe Sicherheit,
– umfassende Vertrauenswürdigkeit,
– ausreichende Nutzerfreundlichkeit sowie
– weitgehende Sozialverträglichkeit.

Im Folgenden werden anhand dieser Kriterien einige der zentralen Forderungen des Verbraucherschutzes an biometrische Verfahren vorgestellt.

Sicherheit

Sollen biometrische Verfahren zur Sicherheit elektronischer Anwendungen beitragen, müssen sie selbst hohen Sicherheitsanforderungen genügen. Ein Missbrauch biometrischer Daten muss weitgehend ausgeschlossen werden können. Um das zu gewährleisten, müssen die unterschiedlichen biometrischen Verfahren je nach Merkmal, Risikopotenzial und Anwendungsfeld differenziert bewertet und vor einer breiten Markteinführung einer umfassenden Risikoanalyse unterzogen werden. Schlüssige Sicherheitskonzepte für einzelne Anwendungsszenarien unter Beachtung verbraucher- und datenschutzrechtlicher Erfordernisse sind aber noch nicht weit entwickelt (Albrecht 2001, S. 42).

Bei der Ausgestaltung der Sicherheit biometrischer Verfahren geht es übergreifend darum, jede Beschädigung der Menschenwürde, des Allgemeinen Persönlichkeitsrechts und speziell des Rechtes auf „informationelle Selbstbestimmung“ zu verhindern. Diese grundsätzliche Perspektive wird weiter unten unter Aspekten des Datenschutzes genauer diskutiert (Kapitel V.3). Im Folgenden geht es zunächst um Sicherheit im engeren Sinn, vor allem um die so genannte „Überwindungssicherheit“.

Wie alle IT-Systeme können auch biometrische Systeme zum Ziel von „Attacken“ werden. Angriffspunkte sind vor allem der Sensor, die Verbindung zwischen Sensor und Verarbeitungseinheit sowie die Verbindung der Verarbeitungseinheit mit weiteren Einheiten, z. B. mit dem Datenbank-Server. Es können übertragene und abgehörte Daten entweder von außen in den Verifikations- oder Identifikationsablauf eingespielt („Replay-Attacken“), oder es kann der Sensor – z. B. mit dem Ausdruck eines Bildes – getäuscht werden. Biometrische Systeme müssen deshalb gegen Manipulationen wie die Verwendung gefälschter biometrischer Merkmale geschützt sein, d. h. die Sensoren dürfen nicht durch Fotografien, Kontaktlinsen mit fremdem Irismuster, Kopf- oder Fingerattrappen, Imitation der Stimme oder Verkleidung überlistet werden können (Angriff „von vorne“ auf die Erfassung des Merkmals selbst). Weiterhin muss das Belauschen und Auslesen biometrischer Daten aus Datenleitungen, Datenbanken und Datenspeichern wie Chipkarten verhindert werden. Bisherige Tests zur Überwindungssicherheit zeigen teilweise noch erhebliche Schwachstellen bei zahlreichen verfügbaren Systemen.

Als praktikable Lösung zur Verhinderung von Täuschungen des Sensors gilt die so genannte Lebenderkennung. Bei der Überprüfung, ob biometrische Daten tatsächlich von der berechtigten Person stammen, erkennt das System gleichzeitig Signale, die nur von einem anwesenden lebenden Menschen stammen können. Bei Fingerbilderkennungsverfahren werden beispielsweise Pulsschlag, Temperatur, Leitfähigkeit der Haut oder Blutsauerstoffgehalt gemessen, bei Gesichtserkennungsverfahren werden Bewegungen des Gesichtes oder der Augen erfasst (Kapitel II.2). Bei vielen der verfügbaren Systeme ist der Leistungsstand der eingebauten Lebenderkennung noch verbesserungswürdig.

Das Risiko des Ausspähens biometrischer Daten lässt sich grundsätzlich dadurch begrenzen, dass keine zentralen Datenbanken geschaffen werden. Die biometrischen Daten wären vielmehr dezentral entweder in autonomen Geräten oder auf einer Chipkarte unter der persönlichen Kontrolle des Nutzers bzw. Betroffenen abzulegen. Allerdings ist die Erkennungsprozedur in autonomen Geräten und auf Karten zurzeit noch nicht für alle Verfahren gleich gut realisierbar, z. B. wegen der erforderlichen Speicherkapazität, und bei keinem verfügbaren System erfolgreich umgesetzt. Bei einer Diskussion um pro und contra müsste – gerade für den Verbraucher – klar herausgearbeitet werden, dass eine zentrale Datenablage zwar komfortabler ist, weil sie eine Chipkarte o. Ä. unnötig macht, dass dies aber zu Sicherheitsrisiken für die persönlichen Daten führen kann (Albrecht 2001, S. 43).

Vertrauenswürdigkeit

Für die breite Akzeptanz biometrischer Verfahren ist entscheidend, dass alle Beteiligten sie als vertrauenswürdig einschätzen (Albrecht 2001, S. 46). Um eine möglichst große Vertrauenswürdigkeit zu erreichen, wird beispielsweise vorgeschlagen, Vertrauensinstanzen einzurichten, die – fachlich kompetent, unabhängig und neutral – ein im Zusammenwirken von Nutzern, Herstellern, Betreibern und Staat vereinbartes Sicherheitsniveau zuverlässig gewährleisten. Derartige Vertrauensinstanzen können etwa Zertifizierungsstellen sein, die bestimmte Dienstleistungen wie das Evaluieren und Zertifizieren biometrischer Systeme und Produkte oder die Generierung und Zertifizierung von Schlüsseln anbieten. Bei der elektronischen Signatur (Kapitel V.2) erfolgt die Zuordnung des Signaturschlüssels zu einer bestimmten Person bereits über das Zertifikat einer solchen Stelle.

Grundsätzlich kommen auch Instanzen infrage, die in der Verantwortung der Anwender stehen – wie bereits bei E-Commerce-Anwendungen. So sind z. B. vier deutsche Großbanken zu gleichen Teilen an dem Hamburger Zertifizierungsunternehmen TC TrusT Center AG beteiligt. Das Eigeninteresse der Akteure ist evident, da für den elektronischen Geschäftsverkehr nicht nur sichere Datenübertragung und Gewissheit bezüglich der Identität der Geschäftspartner essenziell sind, sondern auch, dass Geschäftspartner der gleichen Instanz vertrauen.

Eine Voraussetzung für die Überprüfung und Zertifizierung biometrischer Systeme ist die Entwicklung zuverlässiger Evaluierungskriterien, anhand derer unterschiedliche Verfahren objektiv verglichen werden können, und zwar sowohl unter technischen als auch unter anwendungsbezogenen und rechtlichen Aspekten (Kapitel III.1). Mit einem geeigneten und allgemein akzeptierten Kriterienkatalog würden Prüfung und Zertifizierung auf eine solide Basis gestellt; Anwender und Nutzer bekämen einen Leitfaden für die Auswahl eines sicheren Produktes an die

Hand; zugleich würde ein Richtschnur für die Entwicklung sicherer, vertrauenswürdiger Systeme geboten. Damit solche Evaluierungskriterien breite Akzeptanz finden, sollten sie von anbieterunabhängigen Stellen entwickelt werden (Albrecht 2001, S. 48).

Nutzerfreundlichkeit

Ausreichende Nutzerfreundlichkeit biometrischer Verfahren setzt voraus, dass diese robust und alltagstauglich sind, d. h. im massenhaften Gebrauch über lange Zeit zuverlässig funktionieren. Um ausreichende Nutzerfreundlichkeit zu erzielen, müssen – so lässt sich aus Pilotprojekten und Befragungen schließen – folgende Kriterien berücksichtigt werden: Wichtig ist bereits die Art und Weise, wie der Benutzer beim ersten Kontakt mit dem Verfahren, dem so genannten Enrolment bzw. der Personalisierung, betreut wird. Ferner spielt die ergonomische Gestaltung der Anwenderplätze eine ganz erhebliche Rolle. Die Systeme sollten individuell auf den Nutzer einzustellen sein und so auch körperliche Einschränkungen (wie Kleinwüchsigkeit, Rollstuhlgebundenheit, Blindheit etc.) berücksichtigen. Auch sollte das Erkennungsverfahren selbst möglichst einfach und bequem vonstatten gehen, natürlicher Körperhaltung und selbstverständlichen Handgriffen angepasst sein und nicht mehr Zeit in Anspruch nehmen als herkömmliche Erkennungsverfahren. Nicht zuletzt sind klare Bedienungsanleitungen und zuverlässige Betreuung, persönlich und mittels telefonischer Hotline, wichtig (Albrecht 2001, S. 58).

Sozialverträglichkeit

Die Sozialverträglichkeit biometrischer Verfahren wird sich zum einen daran erweisen müssen, dass ihre breite Implementierung nicht zur weiteren „digitalen Spaltung“ der Gesellschaft beiträgt, also Nutznießer und Ausgeschlossene trennt, zum andern daran, dass kein „Zwang zur Biometrie“ entsteht. Nicht alle Menschen verfügen über ein bestimmtes, für biometrische Verfahren geeignetes Merkmal. Hinzu kommen körperliche Einschränkungen und Behinderungen, die die Nutzung biometrischer Systeme erschweren oder unmöglich machen. Aus verbraucherpolitischer Sicht müssten also Vorkehrungen getroffen werden, die gewährleisten, dass kein Nutzer aus den genannten Gründen von biometrischen Anwendungen ausgeschlossen wird. Für diejenigen, die ein bestimmtes biometrisches Verfahren nicht nutzen können oder wollen, wären Ausweichverfahren bereitzustellen. Dies können andere biometrische Verfahren oder aber herkömmliche sein. Prinzipiell sollte für den Nutzer immer die Möglichkeit bestehen, sich auf herkömmliche Art auszuweisen. Dies gilt vor allem für die öffentliche Verwaltung, aber auch für den privaten Bereich (Albrecht 2001, S. 52).

Es liegt auf der Hand, dass die Umsetzung solcher Forderungen sich hart mit den Bedingungen des Marktes stößt. Für die Betreiber würde dies erheblichen organisatorischen Mehraufwand und finanzielle Mehrbelastung bedeuten.

Häufig wird argumentiert, dass es im Sinne der Sozialverträglichkeit und des Datenschutzes wäre, wenn möglichst viele unterschiedliche biometrische Systeme betrieben würden. Eine „Biometric Balkanization“ könnte die Kompatibilität der Systeme behindern und den Austausch biometrischer Datensätze zumindest erschweren. Dies würde den als sicherheitsrelevant erachteten Standardisierungsbemühungen entgegen stehen, zugleich aber dem Datenschutz dienen (Albrecht 2001, S. 53). Eine Entwicklung in dieser Richtung dürfte allerdings eher unwahrscheinlich sein. Wahrscheinlicher ist und geeigneter für diese Zwecke wäre die Nutzung multimodaler Systeme, die auch in Bezug auf Nutzerfreundlichkeit Vorzüge aufweisen.

2. Elektronische Signaturen und Biometrie – rechtliche Aspekte

Während die technische Entwicklung der Biometrie voranschreitet, sind die rechtlichen Folgen ihres breiteren Einsatzes weitgehend ungeklärt. Wenig entwickelt ist auch noch die Diskussion der Frage, ob und wie das Recht durch Setzung geeigneter Rahmenbedingungen eine sichere und sozialverträgliche Entwicklung und Nutzung dieser Technik befördern könnte. Regelungen, die sich ausdrücklich mit dem Einsatz biometrischer Verfahren befassen, lagen in Deutschland bis vor kurzem nur hinsichtlich ihrer Verwendung im Rahmen elektronischer Signaturen vor. (Auf neuere Entwicklungen im Zusammenhang mit dem „Terrorismusbekämpfungsgesetz“ wird in Kapitel V.4 eingegangen.)

Europäische Signaturrichtlinie

Die Europäische Signaturrichtlinie („Richtlinie 1999/93 EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“) trat im Januar 2000 in Kraft.

Nach Artikel 5 Abs. 1 der Richtlinie, der die Rechtswirkungen der elektronischen Signatur regelt, muss durch die Mitgliedsstaaten gewährleistet werden, dass eine „fortgeschrittene elektronische Signatur“, die auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit produziert wurde, zum einen – wie eine handschriftliche Unterschrift – als formgebundene Erklärung anerkannt und zum anderen in Gerichtsverfahren als Beweismittel zugelassen wird. Der erstgenannten Anforderung wurde 2001 durch das „Formgesetz“ (s. u.) entsprochen. Eine Umsetzung der zweiten Anforderung war in Deutschland nicht erforderlich, da die elektronische Signatur bereits nach geltendem deutschen Beweisrecht im Rahmen der freien Beweiswürdigung (§ 286 ZPO), des Augenscheinbeweises (§§ 371 ff. ZPO) sowie durch Sachverständigen- (§§ 402 ff. ZPO) oder Zeugenbeweis (§§ 373 ff. ZPO) zugelassen ist (Albrecht 2001, S. 19).

Eine fortgeschrittene elektronische Signatur liegt nach Artikel 1 Ziff. 2 der Richtlinie vor, wenn folgende Anforderungen erfüllt sind: Sie

- ist ausschließlich dem Unterzeichner zugeordnet,
- ermöglicht eine eindeutige, zweifelsfreie Identifizierung,
- wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann,
- ist so mit Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Welche Techniken und Verfahren zwecks Erfüllung dieser Kriterien einzusetzen sind, wird in der Richtlinie bewusst offen gelassen. In Erwägungsgrund (8) der Richtlinie heißt es dazu: „Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offen steht.“ Durch diese technologieneutrale Regelung können neben herkömmlichen auch biometrische Verfahren oder andere, künftig noch zu entwickelnde Technologien zur Sicherung der elektronischen Signatur eingesetzt werden.

Signaturgesetz

Seit Mai 2001 ist in der Bundesrepublik ein neues Signaturgesetz („Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“) (SigG) in Kraft, das an die Stelle des Signaturgesetzes von 1997 trat. Das Gesetz trägt zum einen den Vorgaben der Europäischen Signaturrichtlinie Rechnung, zum anderen geht es auf eine von der Bundesregierung veranlasste Evaluierung des alten Gesetzes zurück (Bundesregierung 1997).

Verglichen mit dem alten, enthält das neue Gesetz Änderungen insbesondere hinsichtlich des Betriebes von Zertifizierungsstellen sowie der Anforderungen an die elektronische Signatur. Bei beiden Aspekten bezieht sich nicht das (bewusst technologieoffen gehaltene) Gesetz selbst, wohl aber die Begründung zum Gesetzesentwurf auf die mögliche Nutzung biometrischer Verfahren mit dem Ziel der Erhöhung der (Rechts-)Sicherheit im elektronischen Geschäftsverkehr.

Den Anforderungen und Rechtswirkungen, welche die Europäische Signaturrichtlinie mit der „fortgeschrittenen elektronischen Signatur“ verbindet, kommt das Signaturgesetz mit den Regelungen zur „qualifizierten elektronischen Signatur“ nach. Diese Regelungen implizieren ein bestimmtes Sicherheitsniveau. Um eine „Steigerung des Sicherheitsniveaus“ zu ermöglichen und damit „das erforderliche Maß an Sicherheit, Qualität und Vertrauen zu erreichen“ (Bundesregierung 2000a, S. 27), eröffnet das Gesetz die Option der „qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung“ (§ 15 Abs. 1 Satz 4 SigG). Danach können Anbieter von Zertifizierungsdiensten sich bei der zuständigen Behörde „akkreditieren“, d. h. in Bezug auf die technische und administrative Sicherheit ihrer Arbeit und ihrer Produkte umfassend prüfen und bestätigen lassen. Ein Gütezeichen bringt den „Nachweis“ der Sicherheit zum Ausdruck.

Dementsprechend wird in § 15 Abs. 1 Satz 5 SigG den akkreditierten Zertifizierungsstellen erlaubt, „sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit“ ihrer Produkte zu berufen. In der Begründung zum Gesetzentwurf heißt es dazu, mit der Feststellung des erbrachten „Nachweises“ trete „eine objektive Beschreibung der Sicherheit“ an die Stelle der Sicherheitsvermutung in § 1 Abs. 1 SigG 1997. Damit sei zu erwarten, dass der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung vor Gericht ein besonders hoher Beweiswert zukommen werde, der „im Ergebnis als eine Art ‚Sicherheitsvermutung‘ gewertet werden“ könne. An der bisherigen Rechtslage ändere sich somit nichts (Bundesregierung 2000a, S. 28).

Im Fortgang der Begründung kommt u. a. die Frage der sicheren Autorisierung der Signatur zur Sprache. Aufgrund der in Signaturgesetz und -verordnung vorgesehenen Vorkehrungen sei zu vermuten, „dass der im qualifizierten Zertifikat benannte Signaturschlüssel-Inhaber die Signatur erzeugt oder die Erzeugung autorisiert hat, soweit im Einzelfall nicht andere Fakten entgegenstehen“. In diesem Zusammenhang wird auf den Einsatz biometrischer Systeme zur Erhöhung der Sicherheit Bezug genommen: „Die mögliche Autorisierung einer anderen Person (z. B. durch Weitergabe der sicheren Signaturerstellungseinheit und PIN) kann ausgeschlossen werden, indem die Signaturerstellungseinheit über die Nutzung biometrischer Merkmale ausschließlich an eine Person gebunden wird“ (Bundesregierung 2000a, S. 28).

In § 17 befasst sich das Signaturgesetz mit Produkten für „qualifizierte elektronische Signaturen“, speziell mit dem Schutz des Schlüssel-Mechanismus. Vorgeschrieben wird, „sichere Signaturerstellungseinheiten“ einzusetzen, die „gegen unberechtigte Nutzung der Signaturschlüssel schützen“ (Abs. 1). Technische Komponenten für die Produktion sicherer Signaturerstellungseinheiten müssen so beschaffen sein, dass sie bei der Erzeugung und Übertragung von Signaturschlüsseln deren „Einmaligkeit und Geheimhaltung“ gewährleisten und eine Speicherung außerhalb der Signaturerstellungseinheit ausschließen (Abs. 3 Nr. 1). In der Begründung zu § 17 Abs. 1 wird darauf hingewiesen, dass biometrische Merkmale verwendet werden können, um „einer Nutzung von sicheren Signaturerstellungseinheiten durch Unbefugte wirksam vorzubeugen“. Deshalb sei die Vorschrift „für die Nutzung biometrischer Merkmale entwicklungsoffen“ (Bundesregierung 2000a, S. 30).

Die damit eröffnete Möglichkeit wird in der Verordnung zum Signaturgesetz aufgegriffen und genauer umrissen.

Verordnung zur elektronischen Signatur

In der Neufassung der „Verordnung zur elektronischen Signatur“ (SigV) vom November 2001 werden u. a. die Anforderungen an die technischen Komponenten zur Erzeugung und Prüfung von Signaturschlüsseln näher ausgeführt. § 15 SigV regelt die Erzeugung und Prüfung „qualifizierter elektronischer Signaturen“. Er zielt darauf ab, durch technische Anforderungen einen sicheren Nachweis

der Integrität elektronisch signierter Dateien sowie der Identität und Berechtigung des Signierenden zu gewährleisten. Hierzu können biometrische Verfahren eingesetzt werden. Dazu heißt es in § 15 Abs. 1 Satz 1 SigV: „Sichere Signaturerstellungseinheiten […] müssen gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann." Damit wird die Identifikation anhand biometrischer Merkmale alternativ zur Identifikation aufgrund von Wissen ermöglicht. In der Begründung zum Entwurf hieß es hierzu, dies schaffe einen „Anreiz für entsprechende innovative Lösungen" („Begründung zur Verordnung zur elektronischen Signatur [Entwurf]" vom 16. August 2001).

In § 15 Abs. 1 Satz 1 und 2 der SigV wird speziell für die Nutzung biometrischer Merkmale ein bestimmtes Sicherheitsniveau vorgegeben: Es müsse hierbei „hinreichend sichergestellt sein, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen ist, und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben sein".

Aus Verbraucherschutzsicht ist diese vergleichende Bezugnahme auf Verfahren nach dem Prinzip von „Besitz und Wissen" schon seit längerem kritisch kommentiert worden (Albrecht 2001, S. 22). Dabei wird vor allem auf den Umstand hingewiesen, dass die Sicherheit solcher Verfahren heute weithin umstritten ist und dass viele deutsche Gerichte inzwischen davon ausgehen, dass sie nicht in dem Maße sicher sind, wie die Anbieter behaupten. Dem Vorschlag, von biometrischen Verfahren „hinreichenden" oder, an die europäische Signaturrichtlinie angelehnt, „verlässlichen" Schutz des Signaturschlüssels entsprechend dem Stand von Wissenschaft und Technik zu verlangen, wurde in der SigV nicht gefolgt. Es wird sich zeigen, ob damit – wie befürchtet – einem Absenken des allgemeinen Sicherheitsniveaus Vorschub geleistet wird.

Formgesetz

Das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" (Formgesetz) trat im Juli 2001 in Kraft. Mit diesem Gesetz wird – der europäischen Signaturrichtlinie Rechnung tragend – die „qualifizierte elektronische Signatur" wie eine handschriftliche Signatur als formgebundene Erklärung anerkannt (§ 126a BGB). Dadurch ist es möglich, rechtsverbindliche, zuvor an die herkömmliche Schriftform gebundene Erklärungen grundsätzlich auch in elektronischer Form abzugeben.

Mit § 292a des Gesetzes wird in die Zivilprozessordnung (ZPO) eine Beweisregel eingeführt, die an die „qualifizierte elektronische Signatur" anknüpft: „Der Anschein der Echtheit einer in elektronischer Form (§ 126a des Bürgerlichen Gesetzbuches) vorliegenden Willenserklärung, der sich aufgrund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist."

Diese Regelung des Anscheinsbeweises dient der Begründung des Gesetzentwurfs zufolge dem Anliegen, dem Empfänger einer elektronisch signierten Willenserklärung eine Beweiserleichterung zu schaffen (Bundesregierung 2000b, S. 24). Im Gesetzgebungsverfahren wurde kritisch kommentiert, dass dieses Anliegen zwar nachvollziehbar sei. Der einfache Einwand des Signaturschlüssel-Inhabers, er habe die mit seiner Signatur versehene Erklärung nicht abgegeben, könne nicht grundsätzlich zur vollen Beweislast für die Herkunft der Signatur aufseiten des Empfängers führen. Doch gehe die vorgesehene Regelung des Anscheinsbeweises von falschen Voraussetzungen aus: Der Standard der „qualifizierten elektronischen Signatur", wie das Signaturgesetz ihn festlege, biete keineswegs zuverlässige Sicherheit. Denn nach dem Signaturgesetz würden „qualifizierte elektronische Signaturen" von Zertifizierungsstellen angeboten, die zwar bei der übergeordneten Behörde angemeldet seien und dieser ihre Qualifikation und die Qualität ihrer Produkte nachweisen müssten. Es fehle aber die Überprüfung und Bestätigung einer unabhängigen, vertrauenswürdigen dritten Instanz. Der für einen vollen Beweis erforderliche Nachweis der Integrität der abgegebenen Erklärung (keine nachträglichen Veränderungen), der Authentizität (Urheberschaft) und der Autorisierung (Zurechenbarkeit) könne deshalb gerade nicht erbracht werden (Albrecht 2001, S. 23). Hinsichtlich der beiden letztgenannten Eigenschaften könne aber auch eine Zertifizierung keine Gewähr bieten, da diese auf der konkreten Verwendung der Signatur „vor Ort" beruhen, die von einer Zertifizierung nicht mit umfasst werden kann. Dies gelte jedenfalls so lange, wie bloß auf die Person bezogene und daher von jedem unberechtigten Dritten verwendbare Nachweise einer Zugangsberechtigung wie Persönliche Identifikationsnummern zum Einsatz kommen.

Zudem trage die der Regelung zugrunde liegende Annahme nicht, dass beim Vorliegen einer „qualifizierten elektronischen Signatur" nach der Lebenserfahrung regelmäßig von der Echtheit der vorliegenden Willenserklärung auszugehen sei. Gerade Erfahrung fehle in diesem Bereich noch und werde sich erst mit der fortschreitenden Technik ergeben (Albrecht 2001, S. 23).

Hohe, „nachgewiesene Sicherheit" – so die Kritik (am damaligen Entwurf) – gewährleiste nur die „qualifizierte elektronische Signatur mit Anbieter-Akkreditierung", wie sie von bei der übergeordneten Behörde „akkreditierten" und mit „Gütezeichen" versehenen Zertifizierungsstellen angeboten werde. Allenfalls an diese Signatur könne der Anscheinsbeweis anknüpfen, den § 292a des Formgesetzes an die „qualifizierte elektronische Signatur" anschließt.

Mit den genannten Regelwerken gibt es in Deutschland einen gesetzlichen Rahmen für den Einsatz biometrischer Verfahren im Zusammenhang mit der elektronischen Signatur und dem elektronischen Rechts- und Geschäftsverkehr. Das Recht eröffnet dabei ausdrücklich der Biometrie ein Anwendungsfeld von zukünftig wahrscheinlich wachsender Bedeutung.

Die Praxis wird zeigen, ob dieser Rechtsrahmen ausreicht oder ob vorgetragene Bedenken sich als gerechtfertigt erweisen.

3. Datenschutz

Biometrische Verfahren sind in vielen technischen Ausprägungen und unterschiedlichen Formen der Nutzung zu finden bzw. denkbar. Dementsprechend tangieren sie zahlreiche gesellschaftliche Teilbereiche und Aktivitäten sowie die darauf bezogenen Rechtsmaterien. Im besonderen Maße sind dabei datenschutzrechtliche Fragen einschlägig. Das TAB hat deshalb beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD-SH 2001) ein Gutachten zu diesem Themenkreis eingeholt. Dieses dient als wesentliche Grundlage der folgenden Ausführungen.

Um biometrische Verfahren datenschutzrechtlich beurteilen zu können, ist zum einen eine Betrachtung des Gesamtsystems notwendig, die sowohl technische Aspekte der einzelnen biometrischen Verfahren als auch die konkreten Rahmenbedingungen von Anwendungen in verschiedenen Einsatzszenarien umfasst. Zum anderen sind die daran geknüpften rechtlichen Regelungen und die davon berührten Rechtsgüter mit einzubeziehen (ULD-SH 2001, S. 7).

– Zur Betrachtung und Beurteilung des Gesamtsystems gehört ein Blick auf die Art der verwendeten Daten, die Weise ihrer Erhebung, die Spezifika ihrer Verarbeitung sowie die technische Sicherheit und Zuverlässigkeit des Verfahrens insgesamt. Diese umfassende Perspektive ist notwendig, weil sich auf jeder Stufe eines biometrischen Verfahrens Sicherheitsrisiken und Gefährdungen von Rechten ergeben, denen aber auch mit entsprechenden technischen und organisatorischen Maßnahmen begegnet werden kann.

– Wichtigste rechtliche Grundlage für die Bewertung von biometrischen Verfahren unter Aspekten des Datenschutzes ist das neu gefasste Bundesdatenschutzgesetz („Gesetz zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze“, in Kraft getreten im Mai 2001), das die Vorgaben der EG-Datenschutzrichtlinie von 1995 („Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“) aufnimmt und umsetzt. Zweck des Gesetzes ist es, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 Abs. 1 BDSG).

  Insofern biometrische Verfahren auf persönliche körperliche Merkmale zurückgreifen, sind bei ihrer Verwendung Grundrechte in ganz besonderer Weise berührt. Fragen des Datenschutzes stellen sich speziell und verschärft. Über das Datenschutzrecht hinaus kommen als Maßgaben für die Beurteilung biometrischer Verfahren das Allgemeine Persönlichkeitsrecht und die verfassungsrechtlich besonders geschützte Menschenwürde in Betracht. Ergänzend sollte zur Orientierung die EG-Datenschutzrichtlinie herangezogen werden.

3.1 Biometrische Daten als personenbezogene Daten

Das Bundesdatenschutzgesetz sieht den Schutz „personenbezogener Daten“ vor. Solche Daten sind im Sinne des Gesetzes dann gegeben, wenn sich „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ zuordnen lassen (§ 3 Abs. 1 BDSG). Ob das der Fall ist, ergibt sich aus dem jeweiligen Kontext: vor allem daraus, ob die Daten verarbeitende Stelle über das für die Zuordnung notwendige Zusatzwissen verfügt (ULD-SH 2001, S. 14).

Das gilt auch für biometrische Daten. Zu personenbezogenen Daten werden sie dann, wenn sie sich zuordnen lassen. Ob biometrische Verfahren zu personenbezogenen Daten führen bzw. Personenbezug erleichtern oder erschweren, hängt u. a. von der Art des Verfahrens und den dabei verwendeten Merkmalen ab.

Grundsätzlich generieren Verfahren, die für den Abgleich biometrische Rohdaten verwenden, eher personenbezogene Daten als solche, die mit Templates oder gar templatefrei arbeiten (ULD-SH 2001, S. 15 ff.). Vorgesehen ist der Rückgriff auf Rohdaten häufig bei Gesichtserkennungsverfahren. Da diese an ein im Prinzip für jedermann offen liegendes Merkmal anknüpfen, ist nicht auszuschließen, dass die Daten sich einer bestimmten Person unmittelbar zuordnen lassen. Damit dürften sie in aller Regel als personenbezogene Daten gelten. Bei Rohdaten, die an weniger offen liegende Merkmale, wie z. B. Fingerabdrücke, anknüpfen, wird es im Allgemeinen nicht möglich sein, sie einer bestimmten Person unmittelbar zuzuordnen. Um diese Daten zu personenbezogenen zu machen, müssten sie erst mit anderen Informationen, wie z. B. Name oder Adresse, verbunden werden.

Die aus Rohdaten erzeugten Templatedaten ergeben erst recht nur dann personenbezogene Daten, wenn sie mit geeigneten zusätzlichen Informationen verknüpft werden. Das können zum einen herkömmliche Informationen wie Name oder Adresse sein, zum anderen weitere, aus anderen Rohdaten errechnete Templates. Die Möglichkeiten, Templates unterschiedlicher Provenienz zusammenzuführen, sind zurzeit noch erheblich eingeschränkt. Datenformate und Algorithmen sind zumeist privates Eigentum, weder offen gelegt noch kompatibel. Auf der Ebene der Algorithmen allerdings lassen sich Standardisierungen, die Templates vergleichbar machen, absehen.

Nicht unwichtig für mögliche datenschutzrechtliche Probleme ist die Frage der Vielfalt und Kompatibilität der Systeme. In manchen Bereichen ist damit zu rechnen, dass ein bestimmtes Verfahren sich marktbeherrschend durchsetzt. Sollte beispielsweise ein einheitliches System im Bereich der Geldautomaten installiert werden, so wäre ein großer Teil der bundesdeutschen Bevölkerung davon betroffen. In Fällen wie diesen dürfte es nicht allzu schwierig sein, Templates (oder Templates und Rohdaten)

so zusammenzuführen, dass sich ein Personenbezug ergibt.

Solche Gefährdungen lassen sich mit templatefreien Verfahren, wie sie zur anonymen und pseudonymen Authentifizierung verwendet werden, vermeiden. In beiden Verwendungen dienen biometrische Daten der sicheren Verschlüsselung, ohne dass auf sie zurückgerechnet und Personenbezug aus ihnen abgeleitet werden könnte (ULD-SH 2001, S. 17).

Sensitive Daten

Im Zusammenhang mit Daten in biometrischen Verfahren ist speziell § 3 Abs. 9 BDSG von Interesse, der in Anlehnung an Artikel 8 der EG-Datenschutzrichtlinie „besondere Arten personenbezogener Daten“ benennt. Unter diesen Begriff fallen „Angaben über rassische und ethnische Herkunft, über politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“. Solche „besonderen“ oder sensitiven Daten dürfen nur ausnahmsweise erhoben werden und stehen damit unter erhöhtem Schutz.

Bestimmte Daten in biometrischen Verfahren können einen Informationsgehalt haben, der in diesen besonderen Schutzbereich fällt. So kann sich z. B. bei der Gesichtserkennung ein Hinweis auf die ethnische Herkunft ergeben. Andere Merkmale (Augenhintergrund, Fingerabdruck) könnten Hinweise auf den gesundheitlichen Zustand enthalten. Einen solchen „überschießenden“ Informationsgehalt haben zunächst aber nur die biometrischen Rohdaten. Die Templatedaten für sich alleine stellen keine sensitiven Daten dar, da aus ihnen nicht unmittelbar auf die vollständige biometrische Eingangsinformation (z. B. ein Abbild des Gesichtes) zurückgeschlossen werden kann (ULD-SH 2001, S. 19).

Nun ist offensichtlich, dass zahlreiche Allerweltsdaten zu den besonders geschützten Daten gehören. Das Porträtfoto eines Betroffenen enthält Informationen über seine rassische Herkunft; oft kann schon der Name Aufschluss über die ethnische Herkunft geben. Um die Geltung des erhöhten Schutzniveaus sinnvoll zu begrenzen, nennt § 13 Abs. 2 Nr. 1 bis 9 BDSG für den öffentlichen Bereich eine Reihe von Bedingungen und Zwecken, unter bzw. zu denen sensitive Daten eben doch erhoben und verarbeitet werden dürfen. Beispielsweise ist die Datenerhebung zulässig, soweit dies „zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung […] erforderlich ist“ und die Verarbeitung der Daten durch Personen erfolgt, „die einer entsprechenden Geheimhaltungspflicht unterliegen“ (§ 13 Abs. 2 Nr. 7 BDSG). Als zulässig gilt die Datenerhebung auch, soweit dies „zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist“ (§ 13 Abs. 2 Nr. 6 BDSG).

Für den nicht öffentlichen Bereich sind die Ausnahmen von der prinzipiellen Unterschutzstellung sensitiver Daten in § 28 Abs. 6 Nr. 1 bis 4 BDSG geregelt.

3.2 Grundrechtsbezug biometrischer Daten und Verfahren

Datenverarbeitung mittels biometrischer Verfahren greift in einen speziellen Aspekt des Allgemeinen Persönlichkeitsrechts ein: das Recht auf informationelle Selbstbestimmung. Darüber hinaus betrifft sie u. U. weitere Aspekte des Allgemeinen Persönlichkeitsrechts, wie es in Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG umrissen ist. Auch die Menschenwürde als herausragendes Schutzgut kann betroffen sein.

Menschenwürde

Im so genannten Volkszählungsurteil von 1983 stellte das Bundesverfassungsgericht fest, dass die geplante Datenerhebung, da sie nicht zu einer „mit der Würde des Menschen unvereinbaren gänzlichen oder teilweisen Registrierung und Katalogisierung der Persönlichkeit“ (BVerfGE 65, 1, 52, zit. n. ULD-SH 2001, S. 26) führe, keinen Verstoß gegen die Menschenwürde darstelle. Dazu erklärte das Gericht: „Etwas anderes würde nur gelten, soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre; denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig“ (BVerfGE 60, 1, 53, zit. n. ULD-SH 2001, S. 26). Aus diesen Ausführungen lässt sich schließen, dass die Erhebung und Verarbeitung eines einzelnen, isolierten biometrischen Merkmals keinen Verstoß gegen die Menschenwürde darstellt. Die Grenzen zu einem Würdeverstoß wären aber dann berührt oder überschritten, wenn durch den Staat die Erfassung und Speicherung eines relevanten Teils oder gar sämtlicher in Betracht kommender biometrischer Merkmale verlangt würde und damit die Möglichkeit eröffnet wäre, eine Person in zahlreichen Lebenssituationen zu observieren. In die Nähe eines solchen Würdeverstoßes könnte es auch schon führen, wenn der Einzelne verpflichtet würde, an verschiedenen staatlichen Verfahren teilzunehmen und dabei immer wieder ein bestimmtes oder einige wenige Merkmale zu verwenden (ULD-SH 2001, S. 26 f.).

Zurzeit dürfte es nicht oder doch nur unter ganz erheblichem Aufwand möglich sein, Informationen aus verschiedenen Verfahren zusammenzuführen. Es ist aber nicht auszuschließen, dass Verfahren dahin gehend standardisiert werden, dass sämtliche Anwendungen mit einheitlichen, austauschbaren Merkmalen arbeiten. Eine „Registrierung“ und „Katalogisierung der Persönlichkeit“ wäre damit als Möglichkeit eröffnet. Deshalb könnte es geboten sein, in verschiedenen staatlichen Verfahren unterschiedliche Merkmale einzusetzen oder durch technische Vorkehrungen der Gefahr übergreifender Profilbildung zu begegnen (ULD-SH 2001, S. 27).

Allgemeines Persönlichkeitsrecht

Im Volkszählungsurteil hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung umrissen. Es hat festgestellt, dass das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen garantiert, prinzipiell selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Zugleich hat das Gericht begrenzte staatliche Eingriffe in dieses Recht zugelassen. Staatlich angeordneter Einsatz biometrischer Verfahren greift aber nicht nur in diesen speziellen Schutzbereich des Allgemeinen Persönlichkeitsrechtes ein. Indem er auf körperliche Merkmale und Verhaltensweisen rekurriert, Körperfunktionen erfasst und als Informationsquelle nutzt – und dies womöglich gegen den Willen des betroffenen Einzelnen –, dürfte er einen weiteren, bislang rechtlich nicht klar definierten Bereich des Allgemeinen Persönlichkeitsrechtes betreffen oder zumindest tangieren.

Folgt man dieser Einschätzung, so sind rechtliche Konsequenzen zu ziehen. Die vorhandenen Befugnisse zur Datenverarbeitung decken lediglich den Eingriff in das informationelle Selbstbestimmungsrecht, nicht aber den darüber hinausgehenden Zugriff auf den Körper. Dieser müsste vom Gesetzgeber grundsätzlich (durch Gesetz) gerechtfertigt und sozialverträglich ausgestaltet werden (ULD-SH 2001, S. 28 f.).

3.3 Folgerungen für rechtliche Regelungen und die Praxis biometrischer Verfahren

Soweit mithilfe biometrischer Verfahren personenbezogene Daten erzeugt werden, unterliegen diese Verfahren den Regelungen des allgemeinen Datenschutzes. Das gilt sowohl für den öffentlichen als auch für den nicht öffentlichen Bereich. Für den öffentlichen Bereich sind darüber hinaus spezielle, bereichsspezifische (auf den jeweiligen Anwendungsbereich bezogene) Regelungen erforderlich.

(Gesetzliche) Grundlagen

Es ist allgemein anerkannt, dass, als Konsequenz des Rechtes auf informationelle Selbstbestimmung, jede staatliche Erhebung und Verarbeitung personenbezogener Daten einer gesetzlichen Grundlage bedarf. Dementsprechend hat der Gesetzgeber in fast alle einschlägigen Gesetze entsprechende Regelungen zur Datenverarbeitung eingefügt. Dies erfolgt zumeist derart, dass die Verarbeitung personenbezogener Daten für die im Gesetz festgelegten Zwecke für zulässig erklärt wird (ULD-SH 2001, S. 28). Staatliche Verarbeitung sensitiver Daten ist nur dann zulässig, wenn eine eigene, bereichsspezifische Rechtsgrundlage gegeben ist bzw. geschaffen wird.

Für die Erhebung und Verarbeitung personenbezogener Daten durch nicht öffentliche Stellen ist das Grundrecht auf informationelle Selbstbestimmung nicht unmittelbar relevant. Allerdings ergeben sich aus zivilrechtlichen Rechtspositionen, namentlich aus dem Allgemeinen Persönlichkeitsrecht, inhaltlich vergleichbare Abwehrmöglichkeiten. Im Falle erheblicher Rechtsgefährdungen durch andere Subjekte des Privatrechts könnte der Staat verpflichtet sein, zum Schutz des Betroffenen tätig zu werden (ULD-SH 2001, S. 18).

Als Rechtfertigung für die Erhebung, Speicherung, Veränderung und Nutzung von Daten kommt im öffentlichen wie im nicht öffentlichen Bereich grundsätzlich auch die Einwilligung des Betroffenen in Betracht (§ 4 Abs. 1 BDSG). Als alleinige Rechtsgrundlage für die Datenverarbeitung in staatlichen Verfahren scheidet die Einwilligung allerdings aus, „da die Befugnisse der öffentlichen Stellen nicht durch individuelle Absprachen mit den Betroffenen erweitert werden können“ (ULD-SH 2001, S. 35). Als alleinige Rechtsgrundlage im nicht öffentlichen Bereich kann sie zweifelhaft sein. Zum Beispiel dann, wenn eine biometrische Anwendung – etwa in Zahlungsverfahren im alltäglichen Geschäftsverkehr – eine große Anzahl von Benutzern betrifft und der Einzelne, will er an diesen Verfahren teilnehmen, kaum die Freiheit hat, seine Einwilligung zu verweigern (ULD-SH 2001, S. 49).

Teilt man die Einschätzung, dass biometrische Verfahren u. U. über den Bereich des Rechtes auf informationelle Selbstbestimmung hinaus in einen weiteren Bereich des Allgemeinen Persönlichkeitsrechts eingreifen, so folgt daraus, dass die bestehenden gesetzlichen Erlaubnisse zur Datenverarbeitung diesen weiter gehenden Eingriff nicht abdecken. Das heißt in der Konsequenz, dass für die Implementierung biometrischer Komponenten in staatliche Verfahren eine eigenständige Entscheidung des Gesetzgebers erforderlich ist, die beide Aspekte des Eingriffs – den spezifischen biometrischen ebenso wie den in das Recht auf informationelle Selbstbestimmung – legitimiert (ULD-SH 2001, S. 28 f.).

Eingriffsintensität und Systemdatenschutz

Ob und wieweit eine bestimmte Praxis des Einsatzes biometrischer Verfahren datenschutzrechtlichen Vorgaben genügt, hängt grundlegend ab von der Intensität, mit der das verwendete Verfahren den geschützten Bereich des Persönlichkeitsrechts berührt oder in ihn eingreift (ULD-SH 2001, S. 35). Dies wird im Wesentlichen von drei Momenten bestimmt: Entscheidend ist erstens, in welchem Umfang personenbezogene Daten erhoben und verarbeitet werden, zum Zweiten, wie aufwendig es ist, einen Bezug zwischen erhobenen Daten und betroffener Person herzustellen, und zum Dritten, welcher Grad der Mitwirkung am Geschehen vom Betroffenen verlangt bzw. ihm zugestanden wird. In allen drei Punkten macht das Datenschutzgesetz Vorgaben, die als Richtschnur für möglichst eingriffsarme Verfahren gelten können:

– Grundsätzlich sind Daten offen zu erheben, unmittelbar beim Betroffenen, unter seiner Mitwirkung und mit seiner Unterrichtung bzw. seiner Kenntnis u. a. bezüglich der Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung (§ 4 Abs. 2 und 3 BDSG). Unter diesem Gesichtspunkt sind Verfahren, die einen hohen Grad der Mitwirkung bezüglich der Erfassung der Rohdaten verlangen, solchen, die weniger beteiligen oder gar unbemerkt arbeiten, vorzuziehen.

– Gefordert ist unter dem Stichwort „Datenvermeidung und Datensparsamkeit“, schon bei der Auswahl und Gestaltung eines Datenverarbeitungssystems darauf zu achten, dass keine bzw. möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden (§ 3a BDSG).

– Anzustreben ist ferner – zwecks hoher Datensicherheit –, von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, „soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht“ (§ 3a BDSG).

Aktive Mitwirkung des Betroffenen, sparsame Erhebung und Verwendung von Daten sowie technikbedingt hohe Sicherheit in der Vermeidung von Personenbezug: Damit sind wichtige Komponenten eines Systemdatenschutzes als (materielle) Grundlage effektiven Datenschutzes benannt. Entscheidend dazu beitragen können templatefreie Verfahren. Sie ermöglichen „Anonymisierung“ und „Pseudonymisierung“ von Daten und sorgen dafür, dass die Möglichkeit, Personenbezug herzustellen, praktisch ausgeschlossen ist (ULD-SH 2001, S. 17). Einen weiteren Beitrag leistet die dezentrale Ablage der Daten entweder in autonomen Geräten oder auf einer Chipkarte unter persönlicher Kontrolle der Betroffenen.

Bei konsequenter Umsetzung von Maßgaben des Systemdatenschutzes sind im Ergebnis Verfahren denkbar, die wegen ihrer geringen Eingriffsintensität weder in Hinblick auf das Recht auf informationelle Selbstbestimmung noch in Bezug auf weitere Bereiche des Allgemeinen Persönlichkeitsrechts oder die Menschenwürde problematisch wären. Damit hätte die Realisierung des Systemdatenschutzes zur Folge, „dass der Einsatz des Verfahrens an keinen weiteren datenschutzrechtlichen Vorgaben gemessen werden“ müsste (ULD-SH 2001, S. 36).

4. Das Terrorismusbekämpfungsgesetz

Im Zuge der intensiven Diskussionen um Maßnahmen zur Verbesserung der Sicherheitslage nach dem 11. September 2001 wurde auch der Einsatz biometrischer Verfahren erörtert. Mit dem kürzlich verabschiedeten „Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)“ ist der Gesetzgeber entsprechend tätig geworden. Insbesondere im Pass- und Personalausweisrecht wird die Möglichkeit computerunterstützter Identifizierung von Personen durch biometrische Daten in Ausweisdokumenten eröffnet. Mithilfe der Biometrie soll deren Fälschung erschwert bzw. unterbunden und es soll verhindert werden, „dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen können“. Entsprechend werden zweifelsfreie Feststellung der Echtheit von Dokumenten und der Identität von Personen erwartet (Begründung zum Terrorismusbekämpfungsgesetz; SPD/BÜNDNIS 90/DIE GRÜNEN 2001, S. 47). Hierzu nimmt das Gesetz Änderungen des Passgesetzes (PassG) und des Gesetzes über Personalausweise (PersAuswG) dergestalt vor, dass – neben Lichtbild und Unterschrift – weitere biometrische Merkmale in Pass und Personalausweis aufgenommen werden dürfen. Alternativ werden genannt: Merkmale von Fingern, Händen oder Gesicht.

Ein zukünftiges „besonderes Bundesgesetz“ wird diese Vorgaben konkretisieren: Zu regeln sind die „Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form […] sowie die Art der Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung“ (§ 4 Abs. 4 PassG neu, § 1 Abs. 5 PersAuswG neu).

Den Anforderungen des Datenschutzes entsprechen die Neuregelungen in Pass- und Personalausweisgesetz durch die Benennung der Zweckbindung der entstehenden Daten sowie die Normierung der Auskunftsrechte der Betroffenen (§ 16 Abs. 6 PassG neu, § 3 Abs. 5 PersAuswG neu).

Im Ausländergesetz (AuslG) wird die Nutzung biometrischer Merkmale in der oben genannten Art und Weise ebenfalls als Möglichkeit eröffnet. Vor allem die Aufenthaltsgenehmigung, aber auch der Ausweisersatz, die Bescheinigung über die Duldung und die „Bescheinigung über die Wirkung [...] [der] Antragsstellung (Fiktionsbescheinigung)“ können künftig biometrische Merkmale von Fingern oder Händen oder Gesicht enthalten (§ 5 Abs. 4, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu). Damit sollen Fälschung und Missbrauch von Dokumenten effektiv verhindert und insgesamt die „Möglichkeiten der Identitätssicherung“ erweitert und verbessert werden (Begründung zum Terrorismusbekämpfungsgesetz; SPD/BÜNDNIS 90/DIE GRÜNEN 2001, S. 53 und 36).

Die konkrete Ausgestaltung der so eröffneten Möglichkeiten liegt beim Bundesministerium des Innern und erfolgt durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf (§ 5 Abs. 6, § 39 Abs. 1, § 56a, § 69 Abs. 2 AuslG neu).

Mit dem „Terrorismusbekämpfungsgesetz“ hat der Gesetzgeber eine eigene Entscheidung hinsichtlich der Erforderlichkeit und Angemessenheit der Nutzung biometrischer Daten in bestimmten staatlichen Verfahren getroffen. Entsprechend der Rechtsprechung des BVerfG zum informationellen Selbstbestimmungsrecht ist eine parlamentsgesetzliche Grundlage geschaffen worden, aus der (auch für den Bürger) Voraussetzungen, Ziel und Umfang des Eingriffes in dieses Recht klar hervorgehen:

– Die zu nutzenden biometrischen Merkmale werden alternativ explizit genannt.

– Der Zweck der gespeicherten Daten ist ausdrücklich bestimmt.

– Für die Einführung von mit biometrischen Merkmalen versehenen Ausweisdokumenten für deutsche Staatsbürger ist ein Gesetzesvorbehalt vorgesehen. Anders bei den Ausweispapieren für Ausländer: Hier soll eine Rechtsverordnung die rechtliche Grundlage bilden.

Gesetzliche Regelung der Nutzung der Biometrie im Passgesetz, im Gesetz über Personalausweise und im Ausländergesetz

Das PassG wurde durch die Aufnahme folgender Bestimmungen in §§ 4 und 16 (das PersAuswG durch Aufnahme der §§ 1 und 3 gleich lautend) wie folgt geändert:

„Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. […]

Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form […] sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet."

[...] „Im Pass enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen und verwendet werden. Auf Verlangen hat die Passbehörde dem Passinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen."

Das Ausländergesetz wurde u. a. durch Einfügungen in § 5 wie folgt geändert:

„Die Aufenthaltsgenehmigung kann neben dem Lichtbild und der eigenhändigen Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Inhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in die Aufenthaltsgenehmigung eingebracht werden."

[…] „Vordruckmuster und Ausstellungsmodalitäten, ihre Einzelheiten sowie ihre Aufnahme und die Einbringung von Merkmalen in verschlüsselter Form bestimmt das Bundesministerium des Innern nach Maßgabe der gemeinschaftsrechtlichen Regelungen durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf."

Den Anliegen des BDSG wurde vor allem dadurch entsprochen, dass dem Pass- oder Ausweisinhaber auf Verlangen von den zuständigen Behörden Auskunft über den Inhalt der – verschlüsselten – Daten zu erteilen ist. Es ist ferner ausdrücklich vorgesehen, dass keine „bundesweite Datei" eingerichtet werden soll. Bei den Beratungen im Innenausschuss wurde ausdrücklich festgehalten, dass dies auch für eine länderübergreifende Vernetzung etwaiger lokaler Register gilt (Innenausschuss 2001, S. 5).

VI. Perspektiven der weiteren Entwicklung – Forschungs- und Handlungsbedarf

Es war die Aufgabe des TAB, im Rahmen einer „Vorbereitenden Untersuchung" das Feld der biometrischen Verfahren und Systeme einer ersten Sichtung zu unterziehen und den Versuch einer Bestandsaufnahme sowie einer vorläufigen Beurteilung der FuE-Aktivitäten, der Marktentwicklung und der augenblicklichen und zukünftigen Anwendungsfelder (und -potenziale) zu unternehmen. Aus rechtlicher, insbesondere datenschutzrechtlicher, und verbraucherpolitischer Sicht sollte eine erste Einschätzung biometrischer Verfahren und Systeme erfolgen.

Dem explorativen Charakter der „Vorbereitenden Untersuchung" entsprechend, können die Ergebnisse nur vorläufige sein, zumal sich im Verlauf des Vorhabens gezeigt hat, wie dynamisch sich nicht nur die technologischen, sondern auch die gesellschaftlichen Rahmenbedingungen ändern.

Einige Thesen zu den Perspektiven der Biometrie

– Trotz vieler Unsicherheiten, insbesondere bei den Rahmenbedingungen, ist zu vermuten, dass sich biometrische Systeme und Verfahren weltweit in einer entscheidenden Phase der Diffusion befinden. Nachdem sie lange Zeit vor allem als Zugangssicherung in sicherheitskritischen Bereichen wie Gefängnissen, Kraftwerken oder Rechenzentren zum Einsatz kamen, lassen nun zahlreiche Hinweise ihre Expansion in weitere öffentliche und private Anwendungsfelder erwarten.

– Die technologischen Fortschritte sind unübersehbar. Zwar ist Biometrie noch eine relativ junge Technologie – zunehmend aber werden Kinderkrankheiten auskuriert. Die technischen Funktionalitäten einzelner Systeme werden ausgereifter und weisen eine verbesserte Leistungsfähigkeit auf.

– Die Preisentwicklung bei vielen Systemen dürfte ihre weitere Verbreitung befördern. Einzelne Basiskomponenten wie Sensoren oder Chips sind preisgünstig am Markt verfügbar, ein erhöhter Produktionsausstoß ermöglicht darüber hinaus weitere Preissenkungen. Damit dürfte die Innovationsschwelle Preis in Zukunft stetig abgesenkt werden.

- Das Nachfragepotenzial ist seit jeher als immens eingeschätzt worden. Sinnvolle (oder als sinnvoll wahrgenommene) Applikationen sind aber über lange Zeit nicht in genügend großer Zahl vorhanden gewesen. Zudem waren biometrische Systeme technisch anfällig und hochpreisig, sodass sie an der Schwelle der Märkte verblieben. Mittlerweile stellt sich das Angebot preisgünstiger und qualitativ verbessert dar, sodass die Nachfrage besser stimuliert und befriedigt werden kann.
- Die Entwicklungen der letzten Zeit haben gezeigt, wie schnell sich die Innovationsbedingungen ändern können. Nachdem in der frühen Diffusionsphase eher Sicherheitsaspekte dominierten und die Entwickler ihre Anstrengungen vor allem hieran ausrichteten, schien es zunächst zu einem Wechsel zu kommen. Zunehmend wurde das Komfortkriterium bei den Anwendungen als Marketingaspekt thematisiert – eine Entwicklung, die letztlich zu einer weit gehenden Veralltäglichung biometrischer Systeme hätte führen können. Diese Entwicklungsperspektive scheint zunächst eher blockiert zu sein, nachdem – seit den Anschlägen vom 11. September 2001 – Sicherheit in allen Lebensbereichen neu bewertet worden ist. Der eigentliche Massenmarkt könnte sich jetzt durch (weltweite) staatliche Sicherheitsanstrengungen (v. a. bei Pässen, Ausweisen, Visa, beim Reiseverkehr, aber auch bei der Strafverfolgung und der Vorbeugung von Straftaten sowie bei der Missbrauchsbekämpfung im Sozial- und Gesundheitssektor) ergeben.
- Die geltenden rechtlichen Rahmenbedingungen (insbesondere SigG und SigV) eröffnen der Biometrie im Bereich elektronisch getätigter Transaktionen und Rechtsgeschäfte einen riesigen Markt. Durch das „Terrorismusbekämpfungsgesetz“ ist die Tür zum Markt der Sicherheitstechnologien weiter geöffnet worden. Sollte in Deutschland (und Europa) durch staatliche Verfahren ein Masseneinsatz von biometrischen Systemen angestoßen werden, so würde dies – allen Regeln technologischer Innovationen zufolge – Signalwirkungen für und Auswirkung auf andere Anwendungsfelder in der Wirtschaft und im privaten Bereich haben.
- Die gesellschaftlichen Rahmenbedingungen sind seit jeher nicht ungünstig gewesen. Die gesellschaftliche Akzeptanz dürfte nicht geringer (aber auch nicht höher) sein als bei anderen Neulandtechnologien mit zunächst noch unklaren Einsatzperspektiven und diffusem Risikoprofil. Von Verbraucherverbänden und Datenschützern ist die Biometrie zwar stets kritisch, zugleich aber auch positiv bewertet worden. Insbesondere wird das Potenzial der Biometrie als verbraucher- und datenschutzfreundliche Technologie herausgestrichen – allerdings verbunden mit der Aufforderung an Entwickler und Anwender, für technische und organisatorische Lösungen zu sorgen, die den Kriterien eines fortgeschrittenen Daten- und Verbraucherschutzes genügen.

Handlungs- und Forschungsbedarf

Biometrische Verfahren im öffentlichen wie im nicht öffentlichen Bereich sollten durch gemeinsame Anstrengungen aller Beteiligten so gestaltet werden, dass sie als sicher, vertrauenswürdig, nutzerfreundlich und sozialverträglich gelten können. Handlungsbedarf zeichnet sich hierbei auf verschiedenen Ebenen ab.

Beurteilung der Leistungsfähigkeit biometrischer Systeme und Verfahren

Die Leistungsfähigkeit verfügbarer biometrischer Systeme ist auf der Basis der – oftmals äußerst widersprüchlichen – Informationen, die für den vorliegenden Bericht erhoben werden konnten, nicht seriös einzuschätzen. Für Verwirrung sorgt häufig die unscharfe Trennung zwischen möglichem Potenzial und augenblicklicher tatsächlicher Kapazität.

Grundsätzlich erscheint die Datenlage für einen differenzierten Leistungsvergleich bei weitem noch nicht ausreichend. Zwar sind weltweit verschiedene Gremien von Anbieter-, Betreiber- und Regulierungsseite bemüht, Standards zur Evaluierung und Zertifizierung zuverlässiger biometrischer Systeme zu entwickeln, doch erzielen sie nur langsam Fortschritte. Was ihre Arbeit so schwierig macht, ist der Umstand, dass die realisierbaren Leistungen eines biometrischen Verfahrens, z. B. in Bezug auf das erreichbare Sicherheitsniveau, nach Ansicht der Mehrzahl unabhängiger Fachleute äußerst anwendungsspezifisch sind (Platanista 2001a). Daher können (standardisierte) Evaluationsprozeduren, ob im Labor oder im begrenzten Feldversuch, lediglich Anhaltspunkte liefern, nicht aber verlässliche und für die Praxis aussagekräftige Werte. Ganz entscheidenden Einfluss auf die Leistungsfähigkeit hat z. B. die Zahl der Nutzer, vor allem im „Identifikationsmodus“ biometrischer Verfahren (Kapitel II.1) bei zentraler Verwaltung der Referenzdatensätze: Auch bei einer sehr niedrigen FAR können – eine ausreichend große Zahl von Nutzern angenommen – unautorisierte Personen akzeptiert werden.

Trotz erkennbarer Verbesserungen und sicherlich weiter zunehmender technischer Fortschritte ist daher Berichten und Einschätzungen über mittlerweile erreichte hohe Standards bei Genauigkeit und Zuverlässigkeit biometrischer Systeme nach wie vor mit Skepsis zu begegnen.

Insbesondere dann, wenn es um einen weit reichenden-den, große Nutzergruppen – ob freiwillig oder verpflichtend – einbeziehenden Einsatz biometrischer Systeme geht, z. B. im Rahmen der Ausrüstung von Ausweispapieren, müssen höchste Ansprüche an eine substanziierte Evaluation der infrage kommenden Systeme gestellt werden. Eine regelmäßige Berichterstattung zum Stand der laufenden Pilotprojekte und der (internationalen) Standardisierungsbemühungen wäre als Basis für die weitere politische Behandlung des gesamten Themenkomplexes sicherlich nützlich. Eine sinnvolle Ergänzung zu laufenden Aktivitäten könnten Projekte und Verfahren der Technikfolgenabschätzung bieten (s. u.).

Beobachtung und Erhebung des Marktgeschehens

Vorliegende Daten und Berichte zum Einsatz biometrischer Systeme wirken häufig sehr punktuell und zufällig. In der Regel sind sie wenig transparent, auf keinen Fall geben sie ein vollständiges Bild. Der Stand der Diffusion, der Umsätze und der Marktanteile (national wie international) bleibt äußerst unscharf.

Festgestellt werden können allenfalls tendenziell steigende Umsätze in den vergangenen Jahren. Die USA stellen dabei den dominierenden Markt dar (auf dem ca. zwei Drittel der Umsätze erzielt werden), gefolgt von Europa, Asien und Lateinamerika. Wie so oft, gilt Asien als bedeutender Zukunftsmarkt, doch auch in Europa wird eine zunehmende Nachfrage vermutet. Derzeit anscheinend führende Technologie, sowohl umsatzbezogen als auch hinsichtlich der Zahl der Anbieter und Systeme, sind die Fingerbildverfahren (Größenordnung des Anteils: 40 bis 50 %); besonders der Gesichtserkennung wird zunehmendes Potenzial eingeräumt. Angenommen wird eine Konsolidierung des Marktes, sobald einzelne Systeme und Anbieter größere Marktanteile erlangen können.

Im Hinblick auf eine mögliche gezieltere Förderung im Bereich Biometrie wären genauere Daten mit Sicherheit vonnöten. Voraussetzung hierfür wäre allerdings die Entwicklung von Konzepten und Methoden zur besseren Erfassung relevanter wirtschaftlicher Kennziffern, differenziert nach eigentlichem biometrischen System, peripheren Geräten und der Art und des Umfangs der Anwendung.

Expertendiskurs Biometrie

Eine substanzielle Verbesserung der Informationslage, die gerade angesichts anstehender politischer Entscheidungen zum Einsatz biometrischer Systeme als Folge des „Terrorismusbekämpfungsgesetzes“ erforderlich wäre, wird nicht leicht zu erreichen sein. Prägend für die Debatte zur Biometrie ist die geringe Zahl an Experten, die fast immer auch Entwickler sind und sich verständlicherweise in diesem jungen, dynamischen Technologiebereich positionieren möchten.

In Ergänzung zu Formen der Sachstandserhebung durch Gutachten oder in Anhörungen könnte die Möglichkeit moderierter Expertenrunden (Stakeholder Workshops) ins Auge gefasst werden, zunächst zu grundsätzlichen Fragen:

– Wie praxistauglich sind die einzelnen biometrischen Systeme?

– Was können sie in den verschiedenen Kontexten und hinsichtlich der gewünschten Funktion leisten?

Aufgabe wäre die Erarbeitung gemeinsamer Stellungnahmen, auf die sich Entwickler, Anbieter, regulierende Instanzen, Daten- und Verbraucherschützer einigen sollten, um so die jeweiligen partikulären Perspektiven zu überwinden. Eine enge Anbindung an die Fragestellungen und Entscheidungsnotwendigkeiten der Politik sollte darüber hinaus gewährleistet werden. Hierdurch könnte zum einen deren Informationsbedürfnis klarer herausgearbeitet und direkt in die Expertenrunde hineintransportiert werden, zum andern hätten die Entwickler die Möglichkeit, ihre Erwartungen an die Politik zu verdeutlichen sowie Problemlösungen proaktiv anzubieten.

Aus Sicht der Politik könnte der Expertendiskurs Fingerzeige für Handlungs- und Gestaltungsbedarf liefern, beispielsweise, ob eine stärkere und zielorientiertere Förderung von Forschung, Entwicklung und Pilotprojekten durch BMBF und BMWi erfolgen sollte oder ob Impulse für die Standardisierung der biometrischen Systeme sowie die Vereinheitlichung der Evaluationsverfahren gegeben werden sollten.

Technikfolgenabschätzung Biometrie

Zur weiteren Abklärung der zukünftigen Entwicklung biometrischer Systeme sollte eine umfassende Technikfolgenabschätzung (TA) durchgeführt werden. Erforderlich wäre eine systematische, zukunftsorientierte Analyse und Beurteilung der gesellschaftlichen, ökonomischen und rechtlichen Voraussetzungen und Folgen einer weiter zunehmenden Verbreitung biometrischer Verfahren, die einen Zeithorizont bis 2010 aufspannen sollte. Die Analyse hätte darüber hinaus politischen Gestaltungsbedarf zu identifizieren. Die zuvor genannten Expertenworkshops könnten in Zusammenhang mit einer TA Biometrie durchgeführt werden.

Verbraucherschutz

Wünschenswert wäre eine umfassende Risikoanalyse biometrischer Systeme, wie sie auch von den Verbraucherschutzverbänden gefordert wird – eine Analyse, welche die diversen angebotenen Systeme vor einer breiten Markteinführung differenziert vergleicht und bewertet. Für einzelne Anwendungsszenarien sind schlüssige Sicherheitskonzepte zu entwickeln – unter Beachtung sowohl verbraucher- als auch datenschutzrechtlicher Vorgaben. Fortschritte sind noch erforderlich bei der Entwicklung von Evaluierungs- und Prüfkriterien. Diese sollten von unabhängigen Gremien erarbeitet werden und keinesfalls nur auf Labortests, sondern auf aussagekräftigen Feldtests mit hoher Praxisrelevanz aufbauen.

Vor dem breiten Einsatz biometrischer Verfahren sollte erwogen werden, gewisse technische Mindestanforderungen festzulegen. Auch wäre an Standards bei der Verschlüsselung biometrischer Daten zu denken. Die Einhaltung solcher Mindestanforderungen sollte – staatlich organisiert – durch unabhängige Stellen überprüft und bestätigt werden. Zertifizierung und Gütesiegel sollten für qualifizierte Produkte möglich sein. Hierbei ist neben rechtlichen Regelungen an Vereinbarungen auf der Basis der Selbstregulierung der Entwickler und Anwender biometrischer Verfahren zu denken.

Datenschutz

Der Einsatz biometrischer Verfahren bietet grundsätzlich neue Möglichkeiten für ein Erhöhung der Datensicherheit. Insofern können sie potenziell als so genannte

Privacy Enhancing Technology eingestuft werden. Auch erhofft man sich, dass sie – durch einen Einsatz bei der Zugangskontrolle, der Personenidentifikation, der Strafverfolgung etc. – dazu beitragen, die Sicherheit in diversen Lebensbereichen zu verbessern. Zugleich aber bringt der Einsatz der Biometrie vor allem in solchen Verfahren, in die eine große Zahl von Betroffenen einbezogen ist, besondere Herausforderungen für den Schutz personenbezogener Daten sowie möglicherweise Gefährdungen für grundrechtliche Positionen mit sich (informationelles Selbstbestimmungsrecht, Allgemeines Persönlichkeitsrecht, Menschenwürde).

Eine Konsequenz daraus sollte sein, dass Biometrie in verpflichtend vorgeschriebenen staatlichen Verfahren so zurückhaltend wie möglich angewandt wird. Wird ihr Einsatz als erforderlich und angemessen angesehen, sollte durch entsprechende Technik- und Verfahrensgestaltung sichergestellt werden, dass Gefährdungen für die Rechte der Betroffenen ausgeschlossen sind oder doch zumindest begrenzt werden (ULD-SH 2001, S. 60). Entsprechendes gilt für den Einsatz biometrischer Verfahren im nicht öffentlichen Bereich.

Bezüglich sicherer Technik- und Verfahrensgestaltung hätte man sich an den Anforderungen des Systemdatenschutzes zu orientieren, der als unabdingbare Grundlage zuverlässigen Datenschutzes anzusehen ist. Ergänzt werden sollte dies durch effektive Datenschutzkontrollen. Voraussetzung dafür wäre die personelle und finanzielle Stärkung der zuständigen Datenschutzkontrollinstanzen (ULD-SH 2001, S. 61).

Neben adäquater Technikgestaltung und Kontrolle sind angemessene rechtliche Grundlagen erforderlich. Dabei ist der Einsatz der Biometrie in staatlichen Verfahren durch besondere Rechtsgrundlagen zu gestalten. Private Verfahrensbetreiber arbeiten auf der Grundlage geltenden Rechts. Sollte dieses, verbunden mit den vorgesehenen staatlichen Kontrollen, zum Schutz der Belange der Betroffenen nicht ausreichen, so sind fallweise regulative Maßnahmen ins Auge zu fassen.

Biometrische Daten bei der Strafverfolgung

Mit dem fortschreitenden Einsatz biometrischer Verfahren wird künftig eine wachsende Zahl von Daten – bei öffentlichen wie privaten Stellen – unter den Anwendungsbereich von § 98a StPO (Rasterfahndung im Bereich der Strafverfolgung) fallen. Dazu kommt, dass mit biometrischen Daten – besser als mit bisherigen Datenbeständen – nicht nur eine Gruppe von Tatverdächtigen eingegrenzt werden kann. Vielmehr lassen sich gezielt einzelne Personen identifizieren. Sollte sich deshalb für die Zukunft ein Anstieg der auf § 98a StPO gestützten Maßnahmen ergeben, bei denen auf solche Datenbanken – insbesondere umfangreiche „private“ biometrische Datenbestände (etwa bei großen Konzernen, Banken, Ausgabestellen elektronischer Signaturen etc.) – zugegriffen wird, so könnte dies Anlass sein zu prüfen, ob die Vorschrift noch im Rahmen der Verhältnismäßigkeit bleibt (ULD-SH 2001, S. 63). Hier wäre ggf. der Gesetzgeber gefordert. Der Verzicht auf eine zentrale Datenspeicherung dürfte in vielen Fällen eine unkomplizierte Lösung dieser Problematik darstellen.

Rechtliche Perspektiven der Technikgestaltung

Mit dem „Terrorismusbekämpfungsgesetz“ als gesetzliche Grundlage ist auf breiter Basis die Möglichkeit der Nutzung biometrischer Verfahren eröffnet worden. Die begonnene Diskussion sollte verstärkt weitergeführt werden. Drei Aspekte seien hierzu genannt:

– Nicht ganz zu überzeugen vermag der Umstand, dass der Gesetzgeber bei den jüngst erfolgten Änderungen im Ausländergesetz andere rechtliche Maßstäbe als im Pass- bzw. Personalausweisgesetz in Bezug auf deutsche Staatsbürger angelegt hat. Hier ist weiterer Diskussions- und Forschungsbedarf nicht zu übersehen, der sich über diese Frage hinaus auch auf die Anforderungen an ein zukünftiges Bundesgesetz zur Biometrie erstreckt.

– Weiterer Bedarf an Klärung ist bei der Frage der internationalen Einbettung der jetzt ins Auge gefassten Maßnahmen offensichtlich. Dazu gehört die Prüfung der Frage, inwieweit die Bundesrepublik durch internationale Verträge in ihrer Aktionsfreiheit hinsichtlich der Nutzung biometrischer Merkmale in Ausweispapieren eingeschränkt ist, beispielsweise durch europarechtliche Bindungen oder Verträge über die internationale zivile Luftfahrt. Hier ist an die Rolle der International Civil Aviation Organization (ICAO) zu denken, die z. B. die Normen für die Maschinenlesezone auf Reisedokumenten entwickelt hat. Daneben sind bilaterale Abkommen (Stichworte „Visafreiheit“ und „Advanced Passenger Information System“ [APIS] und dessen Ergänzung um biometrische Merkmale im Reiseverkehr mit den USA) von Interesse. Schließlich wäre auch – angesichts der augenblicklich aktiven Rolle der USA bei der Prüfung der Nutzung biometrischer Merkmale bei der Einreise – darüber nachzudenken, welche Folgen eine einseitige Festlegung der USA für andere Staaten hätte.

– In nächster Zeit besonders diskussionswürdig erscheint die mögliche Kopplung von Videoüberwachung und biometrischen Erkennungssystemen. Neben der Tauglichkeit solcher Systeme wären hier auch Rechtsfragen zu prüfen, u. a. deshalb, weil z. B. bei einer Anwendung auf einem Flughafengelände im Passagierbereich die Grenzen zwischen staatlicher Nutzung (Sicherheitsbehörden) und privater Nutzung (Flughafenbetriebsgesellschaft, Stichwort „Passagierlenkung“) nicht ganz einfach zu ziehen sind.

Spezifische Rechtsfragen

Die rechtlichen Implikationen der Biometrie sind heute noch weitgehend unklar, eine entsprechende Literatur ist nicht oder kaum vorhanden. Über die genannten rechtlichen Fragen hinaus dürften zahlreiche Einzelaspekte aus juristischer Sicht von hoher Relevanz sein. An dieser Stelle soll exemplarisch nur das Thema „Rechtsfragen der Biometrie am Arbeitsplatz“ genannt werden.

Literatur

1. Vergebene Gutachten

ALBRECHT, A. (2001): Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren unter Berücksichtigung der Situation in den USA. Arbeitsgemeinschaft der Verbraucherverbände (AgV e.V.), Bonn

BEHRENS, M., ROTH, R. (2001): Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt. Eine Bestandsaufnahme – unter Berücksichtigung der USA. TransMIT-Zentrum, Institut für biometrische Identifikationssysteme, Gießen

PLATANISTA GmbH (2001a): Biometrische Systeme – FuE, Diffusionstendenzen und Anwendung. Kommentar- und Ergänzungsgutachten, im Auftrag des Deutschen Bundestages (Autoren: Dittmann, J., Mayerhöfer, A., Vielhauer, C.). Darmstadt

PLATANISTA GmbH (2001b): Kurzexpertise „Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet“. Im Auftrag des Deutschen Bundestages (Autoren: Dittmann, J., Mayerhöfer, A., Vielhauer, C.). Darmstadt

ULD-SH (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) (2001): Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen (Autoren: Bäumler, H., Gundermann, L., Probst, Th.). Kiel

2. Weitere Literatur

BEHRENS, M., ROTH, R. (2000): Sind wir zu vermessen, die PIN zu vergessen? In: Datenschutz und Datensicherheit 24(6), S. 327–331

BIOMETRIC CONSORTIUM (1999): http://www. itl. nist. gov/div895/isis/bioapi/BioAPIpresentations/b_dunn1.pdf

BMBF (Hg.) (1998): Delphi’98 – Studie zur globalen Entwicklung von Wissenschaft und Technik. Methoden- und Datenband. Karlsruhe

BREITENSTEIN, M. (2002): Überblick über biometrische Verfahren. In: Nolde, V., Leger, L.: Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation. Köln

BSI (Bundesamt für Sicherheit in der Informationstechnik) (2000): Technische Evaluierungskriterien zur Bewertung und Klassifizierung biometrischer Systeme. Entwurf Version 0.6, 14. Sepember 2000 (http://www.bsi.de)

BUNDESREGIERUNG (1997): Bericht über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des Informations- und Kommunikationsdienste-Gesetz. IuKDG-Bericht gemäß Beschluss des Deutschen Bundestages vom 11. Juni 1997, Deutscher Bundestag, Bundestagsdrucksache 13/7935, Bonn

BUNDESREGIERUNG (1999): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Angela Marquardt, Dr. Heinrich Fink und der Fraktion der PDS – Bundestagsdrucksache 14/1226 – Förderung biometrischer Verfahren und ihrer datenschutzrechtlichen Begleitung durch die Bundesregierung. Deutscher Bundestag, Bundestagsdrucksache 14/1405, Bonn

BUNDESREGIERUNG (2000a): Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften. Deutscher Bundestag, Bundestagsdrucksache 14/4662, Berlin

BUNDESREGIERUNG (2000b): Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr. Deutscher Bundestag, Bundestagsdrucksache 14/4987, Berlin

FIRSTSURF (1999): „Schau mir in die Augen, Kleines!“ – Passwörter der Zukunft. http://www.firstsurf.com/biometrie_t.htm (33/99, 16. August; Stand: 07.06.2000)

FROST & SULLIVAN (Hg.) (1999): World Emerging Biometric Markets. Report 5806–11

FROST & SULLIVAN (Hg.) (2000a): Der europäische Markt für biometrische Identifikationssysteme. Presseinformation 11/2000

FROST & SULLIVAN (2000b): Report 3584 (11/00)

IBG (International Biometric Group) (2000): Sample Chart from the Biometric Market Report 2000. http://www.biometricgroup.com/a_shared/market_size.htm

IBG (International Biometric Group) (2001): Charts from the Biometric Market Report 2001. http://www.biometricgroup.com

IBIA (International Biometric Industrial Association) (2001): http://ibia.org/newsletter04201.htm

IGD (Fraunhofer-Institut für grafische Datenverarbeitung) (2000): Studie BioIS – Vergleichende Untersuchung biometrischer Identifikationssysteme – Technische Untersuchung. Offener Abschlussbericht, 15. Mai 2000 (http://www.bsi.de)

INNENAUSSCHUSS (2001): Bericht des Innenausschusses (4. Ausschuss) 1. zu dem Gesetzentwurf der Bundesregierung – Bundestagsdrucksachen 14/7727,

14/7754 – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), 2. Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN – Bundestagsdrucksache 14/7386 (neu) – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz), 3. Antrag der Abgeordneten Wolfgang Bosbach, Volker Rühe, Eckart von Klaeden, weiterer Abgeordneter und der Fraktion der CDU/CSU – Bundestagsdrucksache 14/7065 (neu) – Sicherheit 21 – Was zur Bekämpfung des internationalen Terrorismus jetzt zu tun ist. Deutscher Bundestag, Bundestagsdrucksache 14/7864, Berlin

JAIN, A., BOLLE, R., PANKANTI, S. (1999): Introduction to Biometrics. In: Jain, A., Bolle, R., Pankanti, S.: Biometrics: Personal Identification in Networked Society. New York, S. 1–42

LANDVOGT, W. (2000): Perspektiven zum Einsatz biometrischer Technologien im Bereich von Personaldokumenten. Statement auf dem BioIS-Symposium am 9. Februar 2000 in Darmstadt, S. 1–3

LASSMANN, G. (2001): Erfahrungen mit biometrischen Systemen. Vortrag, Tagung „Arbeitskreis Kryptosysteme“, T-Systems Nova GmbH, 25. Oktober 2001, Darmstadt

LOCKIE, M. (2000): Biometric Technology Today – Market Developments and application examples of biometric systems. Vortrag auf dem BioIS-Symposium am 9. Februar 2000 in Darmstadt, S. 1–10

LOCKIE, M., DERAVI, F. (2000): The Biometric Industry Report – Market and Technology Forecasts to 2003. Oxford

MORGAN KEEGAN (Hg.) (2000): Equity Research 08/2000

NEWHAM et al. (1999): The Biometrics Report 1999. SJB Services, Somerset

NOLDE, V., LEGER, L. (2002): Einleitung. In: Nolde, V., Leger, L.: Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation. Köln

POLEMI, D. (1997): Final Report – Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentification, Including an Appraisal of the Areas Where They Are Most Applicable. Institute of Communication and Computer Systems, National Technical University of Athens, Greece (ftp://ftp.cordis.lu/pub/infosec/docs/biomet.doc)

SCHEUERMANN, D., SCHWIDERSKI-GROSCHE, SC., STRUIF, B. (2000): Usability of Biometrics in Relation to Electronic Signatures. GMD-Report 118

SIMON, G. (2000): Biometrie im Unternehmen – Erfahrung und Anforderungen aus Betreibersicht. In: Standortbestimmung Biometrie. Tagungsband zum SECURITY-Kongress 2000 in Essen, S. 23 ff.

SPD, BÜNDNIS 90/DIE GRÜNEN (2001): Gesetzentwurf der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN – Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz). Deutscher Bundestag, Bundestagsdrucksache 14/7386 (neu), Berlin

TELETRUST (Deutschland e.V.) (1998): Kriterienkatalog – Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Arbeitsgruppe 6: Biometrische Identifikationsverfahren, Stand 28. August 1998, Erfurt (http://www.teletrust.de)

VIELHAUER, C. (2000): Handschriftliche Authentifikation für digitale Wasserzeichenverfahren. In: Sicherheit in Netzen und Medienströmen. Tagungsband des GI-Workshops „Sicherheit in Mediendaten“, Berlin, S. 134–148

WIK (Wissenschaftliches Institut für Kommunikationsdienste GmbH) (2000): Vergleichende Untersuchung biometrischer Identifikationssysteme (BioIS) – Teiluntersuchung Technikfolgenabschätzung – Endbericht (Autoren: Büllingen, F., Hillebrand, A.). Bad Honnef

WIRTZ, B. (1999): Biometrische Verfahren – Überblick, Evaluierung und aktuelle Themen. In: Datenschutz und Datensicherheit 23(3), S. 129–134

Anhang

Seite

1. Tabellenverzeichnis

Tabelle 1: Derzeit vorrangig genutzte „biometrische Merkmale“ des Menschen 10

Tabelle 2: Technische Angaben zu biometrischen Systemen/Verfahren 20

Tabelle 3: Vorzüge und Nachteile biometrischer Verfahren/Systeme 21

Tabelle 4: Bewertung biometrischer Verfahren nach Jain et al. 1999 22

Tabelle 5: Bewertung biometrischer Verfahren nach Scheuermann et al. 2000 22

Tabelle 6: Öffentliche Forschungsaktivitäten zur Biometrie in Deutschland . . . 28

Tabelle 7: Industrielle FuE/Beratung zum Thema Biometrie in Deutschland . . . 29

Tabelle 8: Exemplarische internationale Forschungsstandorte und -themen . . . 31

Tabelle 9: Laufende Biometrie-Projekte im Rahmen des IST-Programms der EU 32

Tabelle 10: Biometrische Verfahren in der Praxis 37

2. Abbildungsverzeichnis

Abbildung 1: Gewinnung des Minuzienbildes bei der Fingerbilderkennung . . 13

Abbildung 2: Erfassen der Handgeometrie 14

Abbildung 3: Iris-Muster 15

Abbildung 4: Iris mit Iris-Code 16

Abbildung 5: Infrarot-belichtete Retina 17

Abbildung 6: Einzelbilder der Eigengesichtstechnik 18

Abbildung 7: Thermogramm eines Gesichts 18

Abbildung 8: Online-Handschriften („Haus von Nikolaus“ und vorgegebener Schriftzug) 19

Abbildung 9: Zahl der Firmen nach biometrischen Erkennungssystemen . . . 56

Abbildung 10: Marktverteilung biometrischer Systeme (1999) weltweit, nach IBG 57

Abbildung 11: Marktverteilung biometrischer Systeme weltweit, nach Lockie 57

Abbildung 12: Umsatzverteilung biometrischer Systeme nach Anwendungsfeldern 58

Abbildung 13: Umsatzentwicklung biometrischer Systeme 1997 bis 2002 . . . 59

Abbildung 14: Regionale Umsatzverteilung biometrischer Systeme, nach Lockie 59

Abbildung 15: Regionale Umsatzverteilung biometrischer Systeme, nach Frost & Sullivan 60

3. Biometrie und Internet – Projekte und Produkte

Die folgenden Angaben entstammen der Kurzexpertise der Platanista GmbH zum Einsatz biometrischer Systeme zur Erhöhung der Sicherheit im Internet (Platanista 2001b). Exemplarisch werden einige Hersteller, Entwickler und Anwender, ihre Produkte und die von ihnen anvisierten Anwendungsfelder aufgeführt. Es zeigt sich, dass die meisten Verfahren auf der Fingerbilderkennung basieren. Hand- bzw. unterschriftenbasierte Systeme gewinnen jedoch offensichtlich an Bedeutung, was vermutlich an der impliziten Willenserklärung liegt.

– CAD/CAM-Beratung Kühl und SIEMENS – Benutzerwechsel bei Betriebsdatenerfassung und Dateneingabe (Weiterentwicklung: Browser Plug-In) mit Fingerbilderkennung: Die Fingerprint ID Mouse, entwickelt von SIEMENS, wird für Betriebsdatenerfassungsvorgänge und Dateneingaben eingesetzt. Die ID Mouse bietet die Möglichkeit, mehrere Benutzer ohne erneutes Login-Verfahren zu koordinieren. Dies bedeutet eine Arbeitserleichterung sowie schnelleren und sichereren Zugang. Auf dieses System aufgebaut wird derzeit ein Browser Plug-In, um damit Business-to-Business-Bereiche biometrisch absichern zu können. (http:// www.kuehl-edv.de; http:// www.siemens.de)

– NASA – Netzzugriffsschutz durch Gesichts- und Fingerbilderkennung: Die NASA startete 2001 einen Feldversuch, um Fernnetzzugriffe nur mit biometrischen Merkmalen zuzulassen. Mitarbeiter von entfernten Arbeitsstationen konnten sich anhand ihrer biometrischen Merkmalen für den Zugriff auf das Netzwerk authentifizieren. Alle Techniker und Wissenschaftler sollten biometrisch erfasst werden. (http://www.fcw.com/fvw/articles/2001/0101/web-nasa-01-04-01.asp)

– Giesecke & Devrient – „Star Account"/Internetbanking und E-Commerce mit Fingerbild-Smartcard: Giesecke & Devrient entwickelt weltweit Internetbanking-Karten. Die „StarAccount" Chipkarten-Lösung bietet neben dem PIN-basierten Internetbanking als zusätzliche Sicherheit den biometrischen Fingerabdruck. Die Identitätsprüfung via Fingerabdruck wird mittels Public Key Infrastructure (PKI) abgesichert. Zu den Anwendungen zählen weiterhin Datenbank- und Netzwerkzugangskontrolle, Internetzahlungen und E-Business-Lösungen. (http://www.gdm.de)

– E-Contract und Triton Secure – Zeiterfassung durch Fingerbilderkennung: Die Firma E-Contract nutzt das Fingerbildsystem SAFESITE der Firma Triton Secure zur Arbeitszeiterfassung ihrer Vertragsarbeiter. E-Contract „Vertragsfirmen" können auf das Online-Timesheet zugreifen und dieses verwalten. (http:// www.tritonsecure.com)

– Biometrics Solution Group (BSG) – „IBAS (Internet Based Authentifications Service)"/Netzzugriffssicherheit durch Fingerbilderkennung: IBAS bietet Scanmodule für internet- und intranetbasierte Anwendungen, die zu den gängigsten Computern kompatibel sind, um biometrische Daten aufnehmen zu können. IBAS soll Angriffe und unrechtmäßige Zugriffe auf Internet- und Intranetnetzwerke verhindern. Spoofing und Replay-Attacken werden durch die „one-time-template"-Technologie ausgeschlossen. Die Daten werden mit einer sicheren Verbindung zu dem IBAS-Server transferiert, der laut BSG mit den meisten Internet- und Intranetservern kompatibel ist. (http://www.bioace.net)

– Fraunhofer-Institut für Sichere Telekooperation (SIT) – „FipSec"/Biometrisch ausgerüstete Smartcards (Fingerbild, Unterschrift) z. B. für E-Banking: Ziel ist es, durch On-Card-Matching der biometrischen Daten Lösungen für Internet-Applikationen wie E-Banking zu entwickeln. Das Projekt FipSec (Schutz von Smartcard-Funktionen mit Fingerprint Security) demonstriert biometrische Authentifizierung in Verbindung mit wissensbasierter Authentifizierung zur Freischaltung der digitalen Signatur (unter Beachtung von Signaturgesetz und -verordnung) in den Anwendungsumgebungen „Arztpraxis mit Signieren von elektronischen Rezepten", „Anwaltspraxis mit Signieren von elektronischen Mahnbescheiden" und „Büro- und Internetumgebung mit Signieren von E-Mails". (http://sit.fraunhofer.de)

– Keyware Technologies: Zugangskontrolle, Webseitenabsicherung mit Fingerabdruck, Spracherkennung, Iriserkennung (http://www. keyware. com)

– SecuGen: Onlinebanking mit Fingerabdruck (http://www.secugen.com)

– Iridian: Onlinebanking, E-Commerce mit IrisScan. (http://www.iriscan.com)

– SAFLINK Corporation: Onlinebanking, E-Commerce mit multimodalen Systemen (http:// www.saflink.com)

– Alpha Net Online GmbH: E-Commerce mit Fingerabdruck (http://www.alphanet.de)

– Identification Systems Dermalog: E-Commerce mit Fingerabdruck (http://www.dermalog.de)

– DCS – BioID: Onlinebanking, Videokonferenz mit multimodalem System (http://www.bioid.com)

– Identix – BioLogon: Netzzugriffsschutz, Fingerabdruck (http://www.identix.com)

– Visionics Corporation: Onlinebanking, E-Commerce mit Gesichtserkennung (http://www.visionics.com)

– NUANCE Communications: Telefonbanking mit Stimmerkennung (http://www.nuance.com)

– Miros: Onlinebanking, Netzzugriffsschutz (z. B. im Gesundheitswesen) mit Fingerabdruck und Gesichtserkennung (http://www.miros.com)

– LCI Smartpen: E-Commerce mit Unterschriftenerkennung (http://www.smartpen.net)

– Viisage Technology Inc.: E-Commerce mit Gesichtserkennung (http://www.viisage.com)

4. Marktabschätzungen zur Biometrie

Im Rahmen ihrer Bestandsaufnahme zum Einsatz biometrischer Identifikationssysteme haben die Gutachter Behrens und Roth auch den Versuch unternommen, das (weltweite) Marktvolumen abzuschätzen. Zu diesem Zweck haben sie folgende Quellen ausgewertet: Frost & Sullivan 1999 u. 2000, Lockie 2000, IBG 2000, Morgan Keegan 2000 (Behrens/Roth 2001, S. 64 ff.). Dabei ergab sich folgendes Bild:[4]

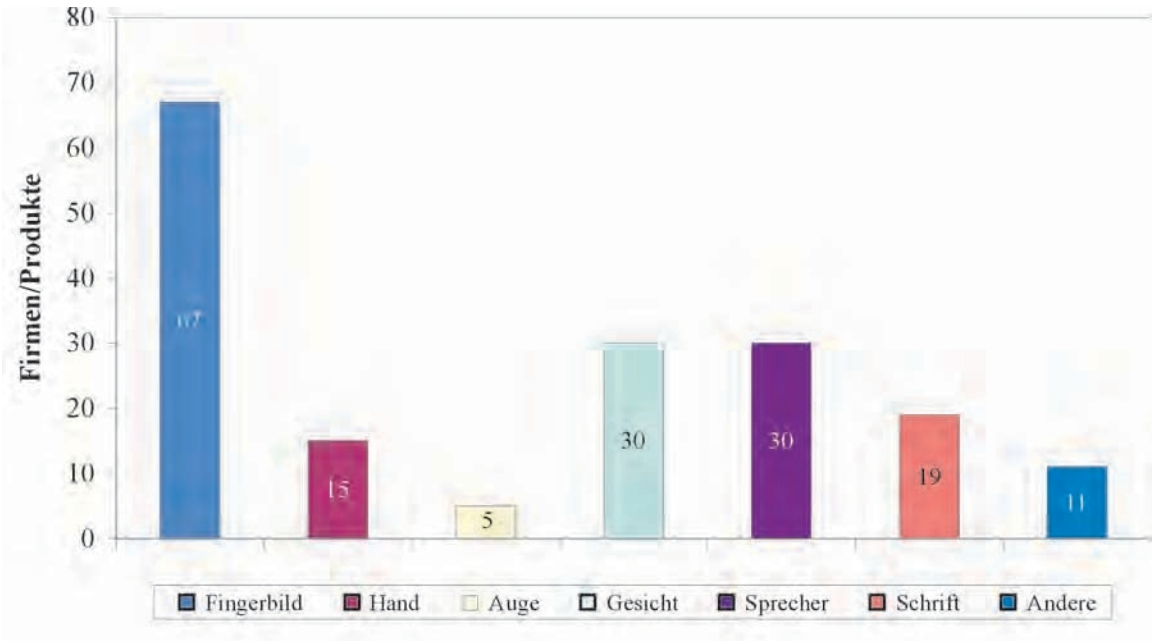
– Die Zahl der Firmen, die biometrische Systeme entwickeln/anbieten, beträgt ca. 200 (Lockie 2000); ihre Aufteilung nach einzelnen Systemtypen (Fingerbild, Gesicht, Hand, Schrift, Stimme, Auge und übrige) zeigt Abbildung 9 (Frost & Sullivan 1999; damals ausgehend von 177 Firmen). Es dominieren klar die Fingerbildverfahren (fast 40 Prozent), quantitativ das Schlusslicht bilden mit weniger als 3 Prozent (fünf Firmen) die „Augenverfahren" Iris- bzw. Retina-Scan, was vermutlich auf die Komplexität der Technologie zurückzuführen ist. Sollte die Biometrie in eine fortgeschrittenere Diffusionsphase eintreten, wird eine „Marktbereinigung" der Firmenvielfalt durch Fusionen und Übernahmen erwartet.

– Zum Anteil der verschiedenen Systeme am Gesamtumsatz weltweit existieren Angaben für 1999 von IBG (2000) (Abbildung 10) und vergleichend für März 1998 und Dezember 1999 nach Lockie (2000) (Abbildung 11). Zwar sind die Unterschiede zwischen den Zahlen teilweise beträchtlich (z. B. beim Anteil der Sprecher- oder der Gesichtserkennung), sie belegen aber die gleichen Tendenzen (für 1999): Es „führt" die Fingerbilderkennung mit ca. ⅓ des Umsatzes (für 2001 wird durch die IBG ein Marktanteil von fast 50 Prozent angegeben) vor der Handvermessung (abnehmende Tendenz), danach folgen die Gesichtserkennung (zunehmend) und die Sprecheridentifikation (abnehmend) vor „Augenverfahren" (zunehmend) und Unterschrift.

– Abbildung 12, Seite 58, zeigt die Umsatzverteilung – wieder im Vergleich März 1998 und Dezember 1999 – nach Anwendungsfeldern (Lockie 2000): physischer Zugang, innere Sicherheit, Finanzen, Gesundheit, Einwanderung, soziale Sicherung, Computersicherheit und Telekommunikation. Die verhältnismäßig große, wenn auch abnehmende Bedeutung im Gesundheitsbereich überrascht angesichts der in der Literatur eher selten angeführten Anwendungsbeispiele. Die auffälligsten Verschiebungen zeigen die drei Anwendungen physischer Zugang, innere Sicherheit und Finanzen, mit einem starken Rückgang bei der Zugangskontrolle und Zuwächsen bei Sicherheit und v. a. Finanzen.

Abbildung 9

Zahl der Firmen nach biometrischen Erkennungssystemen

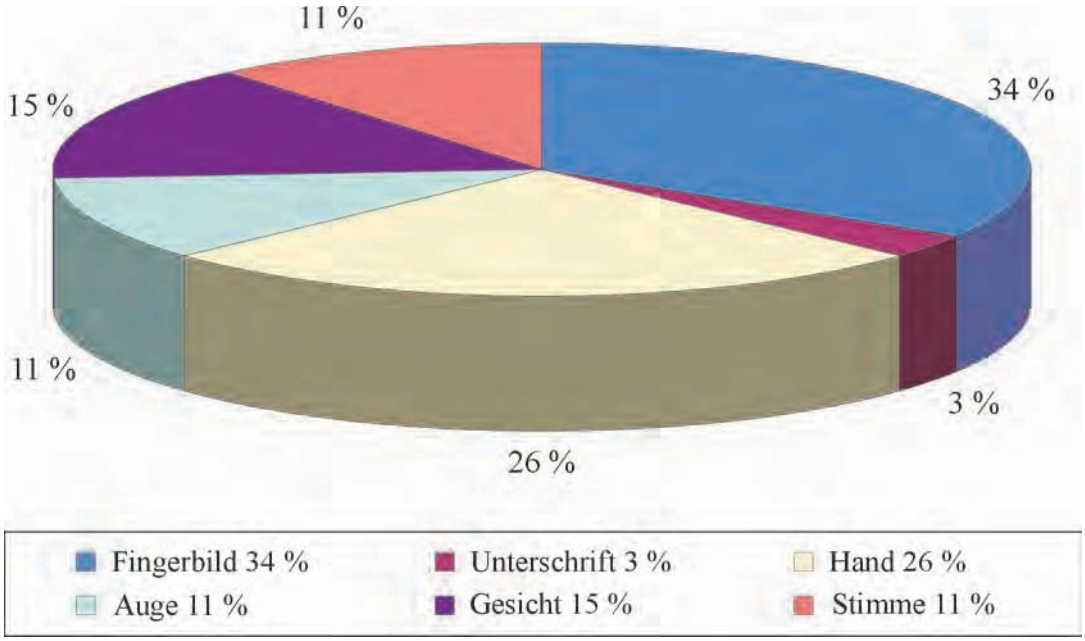


Quelle: Behrens/Roth 2001, S. 64, nach Frost & Sullivan 1999

[4] Daten aus weiteren Studien, die von Platanista zusammengestellt wurden (biometric Consortium 1999; Frost & Sullivan 2000b; IBA 2001), ergaben keine zusätzlichen Aufschlüsse.

Abbildung 10

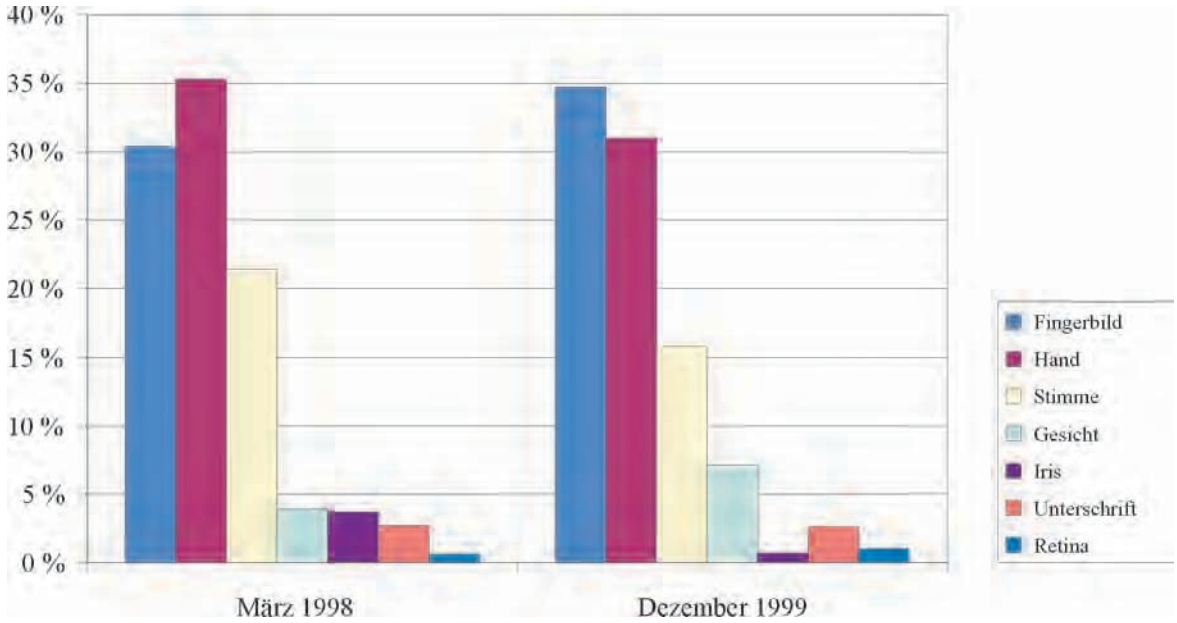
Marktverteilung biometrischer Systeme (1999) weltweit, nach OBG



Quelle: Behrens/Roth 2001, S. 67, nach IBG 2000

Abbildung 11

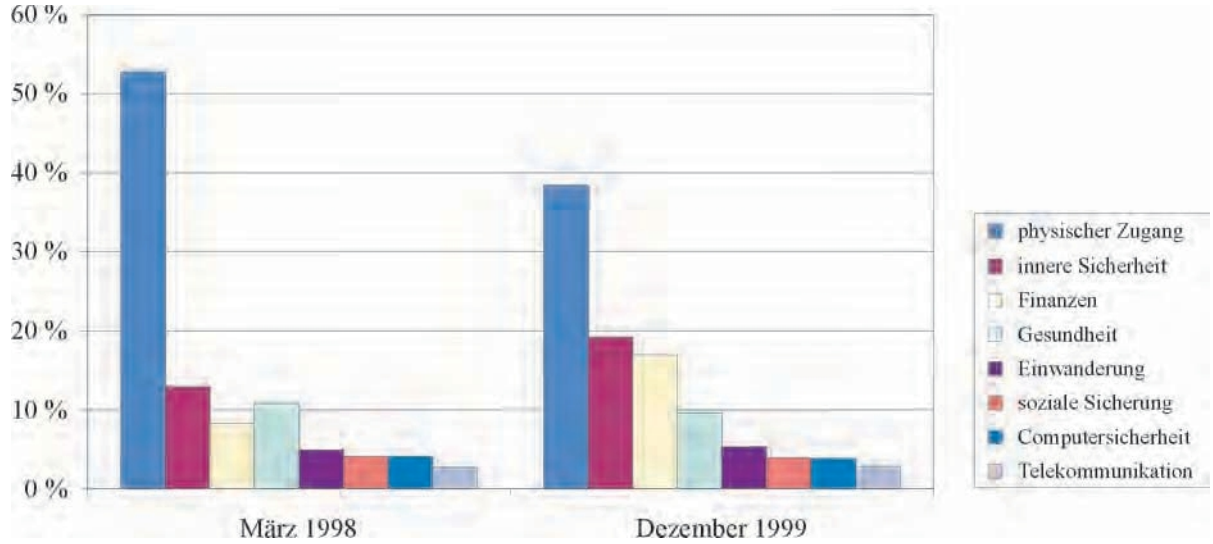
Marktverteilung biometrischer Systeme weltweit, nach Lokie



Quelle: Behrens/Roth 2001, S. 65, nach Lockie 2000

Abbildung 12

Umsatzverteilung biometrischer Systeme nach Anwendungsfeldern



Quelle: Behrens/Roth 2001, S. 65, nach Lockie 2000

– Eine Illustration der Unschärfe der Biometrie-Marktzahlen liefert Abbildung 13, welche die Entwicklung der Umsatzzahlen von 1997 bis 2002 in vier Anwendungsfeldern nach Frost & Sullivan 1999 wiedergibt: Die vier verwendeten Kategorien – zivile/staatliche Nutzung, Zugangskontrolle/Zeiterfassung, Computer-/Netzwerksicherheit und Finanzsektor – bilden ein nicht nachvollziehbares Durcheinander von (unvollständigen) Anwendungszwecken und Anwendern. Daher verwundert es auch nicht, dass diese Daten in keiner Weise zu denen aus Abbildung 12 passen (vgl. Bedeutung von Zugangskontrolle und Finanzen).

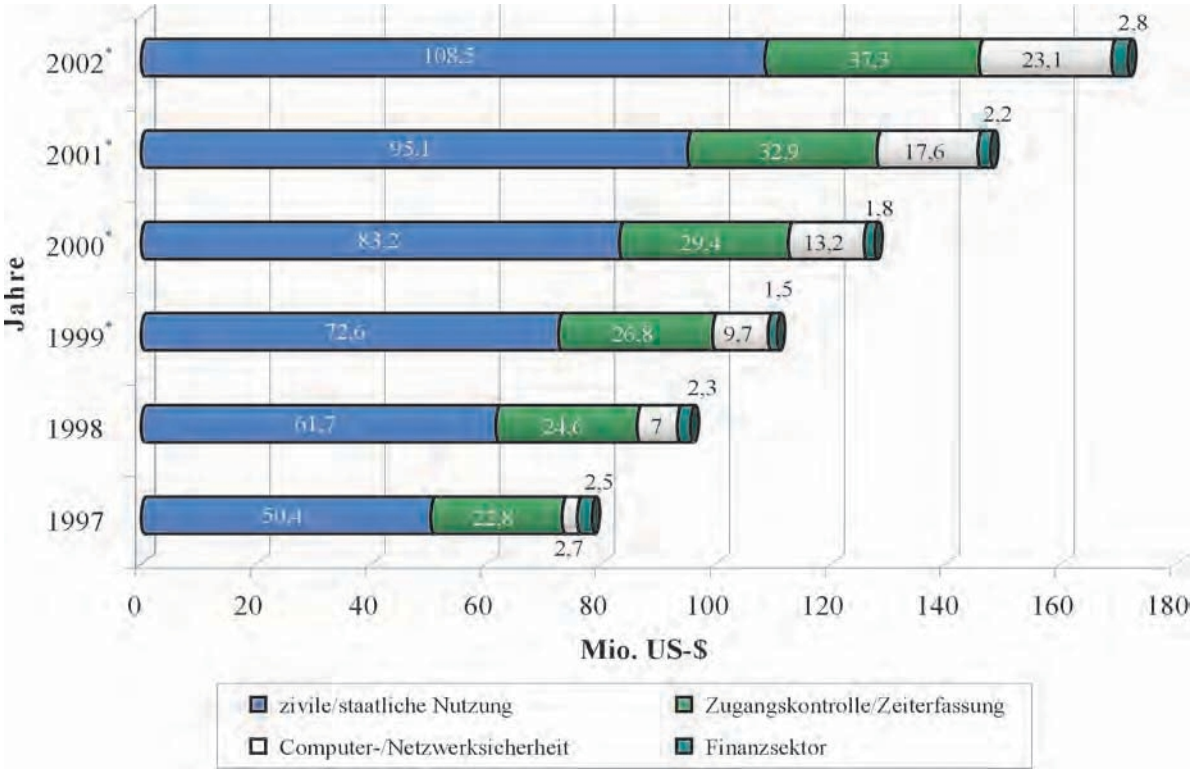
– Auch die Verteilung der Umsätze auf Weltregionen weist erhebliche Diskrepanzen zwischen den Quellen – Lockie 2000 und Frost & Sullivan 1999 auf (Abbildung 14 und 15): Gleichartig ist lediglich die Grundeinschätzung – Nordamerika als ganz dominierender und Europa als klar zweitwichtigster Markt. Die einzelnen Zahlen jedoch unterscheiden sich massiv: Frost & Sullivan beziffern den Anteil des US-Marktes für das Jahr 1999 mit 71 Prozent, Lockie gibt 57 Prozent an; der Anteil der Asien-Pazifik-Region soll entweder 4 Prozent oder aber 9,5 Prozent betragen. Für Europa lautet der Wert für 1998 von Frost & Sullivan 23,5 Prozent, Lockie nennt 12 Prozent.

– Endgültig unklar wird die Datenlage bei den absoluten Umsatzzahlen bzw. -prognosen. So haben Frost & Sullivan ihre Prognose für den Umsatz in Europa für das Jahr 2001 innerhalb eines Jahres von 33 auf 53 Mio. US-Dollar, für das Jahr 2003 von 39 auf 78 Mio. US-Dollar erhöht (Frost & Sullivan 1999 u. 2000a, nach Behrens/Roth 2001, S. 69). Während in Abbildung 15 (nach Frost & Sullivan 1999) für Nordamerika im Jahr 2002 ein Umsatz von gut 100 Mio. US-Dollar prognostiziert wird, zitieren Behrens/Roth (2001, S. 68) eine Abschätzung von Morgan Keegan (2000, S. 13), die einen zehnfach höheren Wert nennt, also ca. 1 Mrd. US-Dollar! Hier muss vermutet werden, dass die beiden Quellen völlig unterschiedliche Ausschnitte der Wertschöpfungskette als Grundlage für ihre Berechnungen genommen haben, ohne dass dies jedoch expliziert worden wäre (Behrens/Roth 2001, S. 68).

Für Deutschland können – wenig überraschend – ebenfalls keine seriösen Zahlen präsentiert werden. Frost & Sullivan (1999 u. 2000a) verorten die Bundesrepublik als größten Markt innerhalb Europas, prognostizieren allerdings für die kommenden Jahre einen abnehmenden Umsatzanteil gegenüber anderen europäischen Ländern – bei insgesamt steigenden Werten. Eine telefonische Umfrage der Gutachter Behrens und Roth bei neun deutschen Herstellern biometrischer Systeme ergab Umsatzvermutungen für 2003 zwischen 7 Mio. und 900 Mio. DM (Behrens/Roth 2001, S. 70) – und müssen somit als nicht verwertbar bezeichnet werden. Deshalb können auch keine sinnvollen Angaben über eine Verteilung der Umsätze mit biometrischen Systemen auf verschiedene Anwendungsfelder oder Anwender gemacht werden.

Abbildung 13

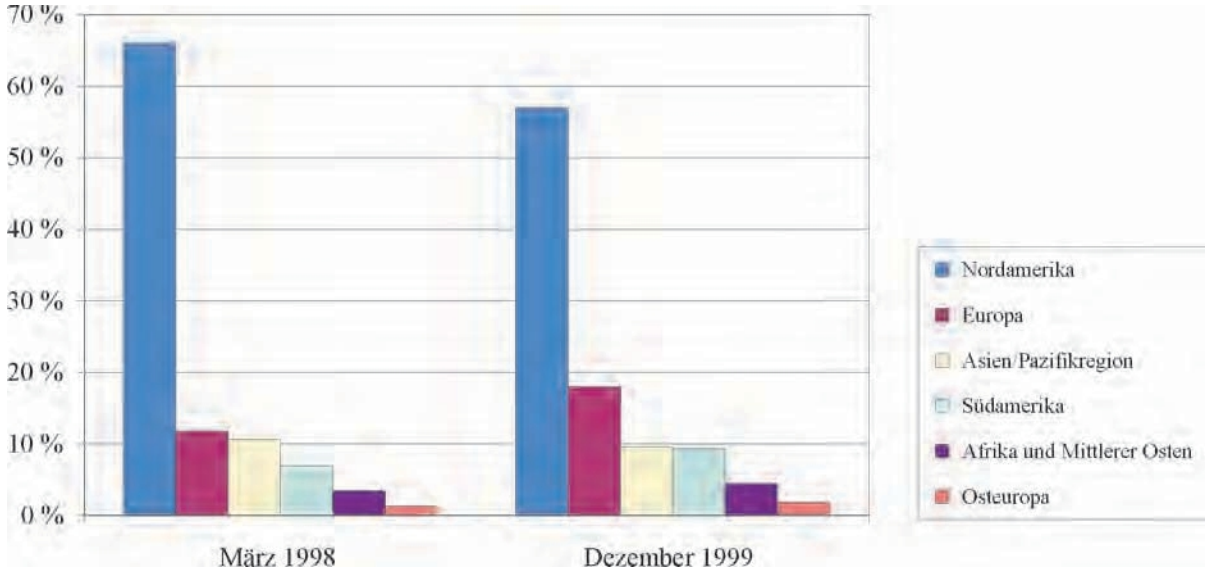
Umsatzentwicklung biometrischer Systeme 1997 bis 2002



* prognostizierte Werte
Quelle: Behrens/Roth 2001, S. 66, nach Frost & Sullivan 1999

Abbildung 14

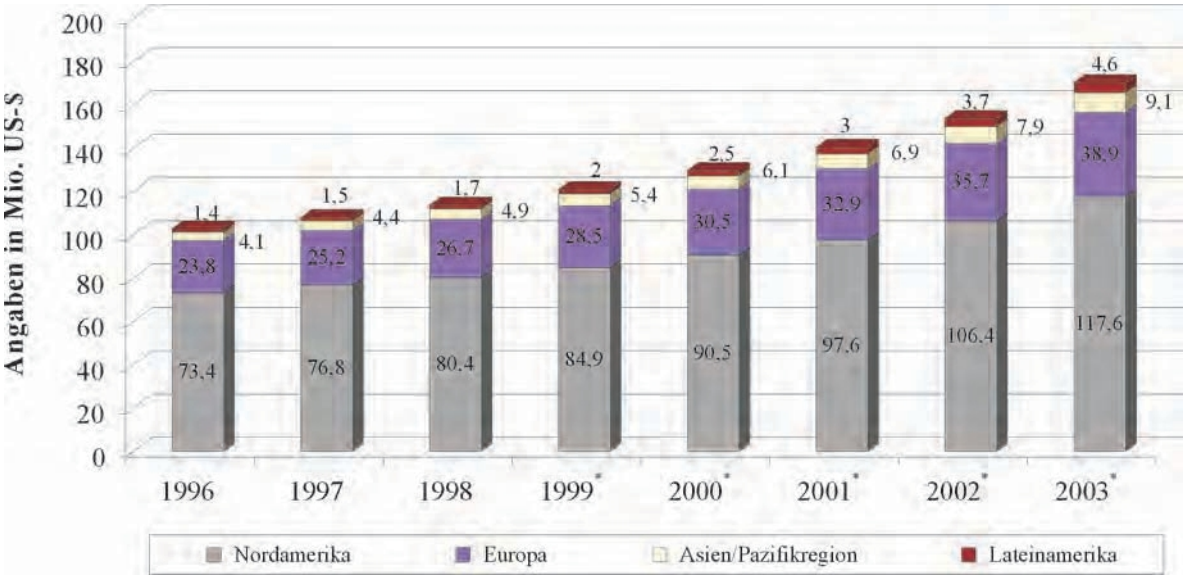
Regionale Umsatzverteilung biometrischer Systeme, nach Lockie



Quelle: Behrens/Roth 2001, S. 67, nach Lockie 2000

Abbildung 15

Regionale Umsatzverteilung biometrischer Systeme, nach Frost & Sullivan



Quelle: Behrens/Roth 2001, S. 67, nach Frost & Sullivan 1999

Druck: MuK. Medien- und Kommunikations GmbH, Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28 / 3 82 08 40, Telefax: 02 28 / 3 82 08 44
ISSN 0722-8333