Deutsches Forum für Kriminalprävention

Deutsches Forum für Kriminalprävention (Hrsg.):

Arbeitskreis Kriminalprävention und Biometrie

- Workshop-Dokumentation vom 30. September 2002 in Bonn -

Inhaltsverzeichnis

Zentralverband
Elektrotechnik- und
Elektronikindustrie e.V.

ZVEI

Das DFK bedankt sich beim ZVEI für die Unterstützung bei den Druckkosten.

Vorwort

Deutsches Forum für Kriminalprävention

Arbeitskreis Kriminalprävention und Biometrie

Das Thema Biometrische Verfahren ist nach den Anschlägen vom 11. September 2001 ein Thema der Sicherheitspolitik in Deutschland geworden. Die Auffassungen über den Nutzen und Mehrwert derartiger Verfahren im Hinblick auf kriminalpräventive Aspekte sind allerdings sehr unterschiedlich. Eine in Teilen kritische gesellschaftspolitische Diskussion wird bereits geführt.

Das Deutsche Forum für Kriminalprävention möchte die gesellschaftspolitische Bedeutung biometrischer Verfahren im Rahmen der Kriminalprävention analysieren und einer kriminalpolitischen Bewertung unterziehen. Wir streben dazu die Mitarbeit staatlicher und nichtstaatlicher Institutionen an. Aufklärung, kritische Sensibilisierung und, wenn es vertretbar erscheint, ein Beitrag zur öffentlichen Akzeptanz verlässlicher Verfahren sind die angestrebten Ziele.

Warum engagiert sich das Deutsche Forum für Kriminalprävention?

Für das Deutsche Forum für Kriminalprävention ist der Bereich der technischen Prävention eine wichtige Komponente der gesamtgesellschaftlichen Debatte über die Verhütung von Straftaten. Damit wird deutlich, dass nicht nur die besonders wichtige primäre und ursachenorientierte Kriminalprävention auf breiter Ebene angepackt werden muss, sondern dass auch die sekundäre Kriminalprävention, und hier die technische Prävention, eine wesentliche Hilfe zur Verhinderung von Kriminalität und Bedrohungen in einer offenen Gesellschaft sein kann. Dabei muss die Technik immer in ein präventives Gesamtkonzept eingebettet werden, wobei der Faktor Mensch nicht zugunsten einer Technikgläubigkeit bei den Präventionsbemühungen unterbewertet werden darf.

Technische Errungenschaften der modernen Dienstleistungsgesellschaft wie Mobilfunk, E-Commerce und Internet bieten für unser Alltagsleben eine Fülle von Erleichterungen, aber eben auch eine Fülle von Gefährdungen, insbesondere wenn Kriminelle die Spielregeln nicht einhalten. Deshalb sind neue Präventionsansätze und Präventionskonzepte erforderlich, um dem Missbrauch zu begegnen. Auch die Industrie muss noch stärker bedenken, dass Aspekte der technischen Prävention in die Produktentwicklung einfließen müssen.

Das Spektrum der technischen Kriminalprävention umfasst daher nicht nur biometrische Verfahren, sondern auf der Agenda stehen u.a. auch die Produktsicherung, die digitale Signatur, die elektronischen Zahlungsmittel, die Videoüberwachung öffentlicher Räume , Kraftfahrzeugsicherungstechnik bis hin zum Geld- und Werttransport und der Bankenschutz. Selbstverständlich haben alle diese Themen in einem kriminalgeografischen Raum Europa durch die fortschreitende globale wirtschaftliche Vernetzung eine bedeutende internationale Perspektive.

Einrichtung des Arbeitskreises als Forum

Durch die Einrichtung eines Arbeitskreises zum Thema Kriminalprävention und Biometrie innerhalb der Stiftung Deutsches Forum für Kriminalprävention (DFK) wollen wir im o.a. Sinne im Spannungsfeld zwischen Sicherheitsbedürfnis und Schutz der Privatsphäre des Einzelnen einen kriminalpolitischen Beitrag leisten.

Das DFK möchte daher u. a. mit Vertretern des Datenschutzes, der Wissenschaft, der Behörden, der Fachverbände und anderer interessierter Vereinigungen ein auf Dauer angelegtes Arbeitskonzept vereinbaren, das die bereits vorhandenen vielfältigen Aktivitäten zu diesem Thema einbezieht und für einen Arbeitskreis eine breite Ausgangsbasis darstellt.

Der Arbeitskreis hat sich am 30. September 2002 konstituiert. In kurzen Statements ist der aktuelle Sachstand zur Biometrie-Diskussion in Deutschland aus unterschiedlicher fachlicher Perspektive beleuchtet worden. Die Dokumentation dieser Vorträge findet der interessierte Leser in dieser Broschüre des Deutschen Forums für Kriminalprävention.

Der Vorsitzende des Arbeitskreises
Jörg Ziercke
Ministerialdirigent und Mitglied des DFK-Vorstandes

DFK-Arbeitskreis Kriminalprävention und Biometrie

Jörg Ziercke, Vorsitzender des Arbeitskreises, Ministerialdirigent und Mitglied des DFK-Vorstandes

Arbeitskreis Kriminalprävention und Biometrie

Programmablauf 30. September 2002

- Begrüßung und Vorstellung
- Erörterung der Ziele
- Organisation und Arbeitsweise
- Kurzvorträge
- Arbeitsplanung des Arbeitskreises

Kriminalpolitische Ziele des Arbeitskreises Kriminalprävention und Biometrie

- Analyse und Bewertung biometrischer Verfahren für die Kriminalprävention
- Reflektion der kritischen gesellschaftspolitischen Diskussion zur Biometrie
- Aufklärung und Sensibilisierung für Zwecke der Kriminalprävention
- Beitrag zur öffentlichen Akzeptanz verlässlicher biometrischer Verfahren

Engagement des Deutschen Forums für Kriminalprävention

- Technische Prävention als wichtige Komponente der Kriminalprävention
- Technikeinsatz nur als Teil eines präventiven Gesamtkonzeptes
- Gefährdungen durch Technik mit Konsequenzen für die industrielle Produktentwicklung

Agenda Technische Kriminalprävention

- Produktsicherung
- Digitale Signatur
- Elektronische Zahlungsmittel
- Videoüberwachung
- Biometrische Verfahren
- Kfz-Sicherungstechnik
- Geld- und Werttransportschutz
- Bankenschutz
- klass. technische Gebäude- und Wohnungssicherung

Vorschlag zur Organisation und Arbeitsweise des Arbeitskreises

Thematischer Schwerpunkt:
Kriminalpolitische Analyse, Bewertung und Empfehlungen zur Biometrie-Diskussion

- Vorsitz DFK einschl. Geschäftsstelle
- ständige Mitglieder als Kernarbeitskreis
- zwei ordentliche Sitzungen pro Jahr

Weitere Vorschläge zur Arbeitsweise

- Meinungsbildung im AK mit ausgewogener Darstellung
- keine Abstimmungen oder Mehrheitsentscheidungen
- Veröffentlichte Bewertungen nach Beteiligung der AK-Mitglieder
- Grundsätzliche Abstimmung mit dem Vorstand DFK
- jeweils aktuelle Expertenstatements im AK
- Informationssammlung beim DFK
- Dokumentation aller Aktivitäten

Vorschläge für Projekte des Arbeitskreises

- Veranstaltung von Workshops
- Begleitung der evtl. gesetzlichen Normierung
- Begleitung der aktuellen technischen Entwicklung
- Begleitung von Forschungsprojekten
- Begleitung von Pilotprojekten

Kurzvorträge 30. Sept. 2002

- Innere Sicherheit und Biometrie
- Erkenntnisstand BioTrust-Analysen einschl. ausländischer Erfahrungen
- Biometrische Verfahren in der Anwendung aus Sicht der Industrie
- Biometrie aus der Sicht des Bundesamtes für Sicherheit der Informationstechnologie

Weitere Kurzvorträge 30. Sept. 2002

- Sachstand: Öffentliche Ausschreibung des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages „Biometrische Identifikationssysteme – Leistungsfähigkeit und rechtliche Rahmensetzung“
- Stand der gesellschaftspolitischen Diskussion zur Biometrie insbesondere unter den Aspekten Rechtsstaat, Datenschutz und Verbraucherschutz

Arbeitsplanung des Arbeitskreises

- Dokumentation der Kurzvorträge und Diskussion durch Geschäftsstelle DFK / Vorsitz AK
- Druck und Veröffentlichung der Dokumentation
- Zusammenfassung der Ergebnisse der 1. AK-Sitzung durch Chefredakteur der Zeitschrift „forum kriminalprävention“ und Veröffentlichung
- Darstellung der Tätigkeit des AK in der Kuratoriumssitzung des DFK im November 2002

Weitere Arbeitsplanung des Arbeitskreises

- Präsentation des Themenfeldes Kriminalprävention und Biometrie auf dem 8. Deutschen Präventionstag April 2003
- Vorbereitung der 2. Sitzung des Arbeitskreises im April 2003
- ggfl. Vorbereitung einer öffentlichen Veranstaltung zum Themenfeld Kriminalprävention und Biometrie im Herbst 2003

Biometrie und innere Sicherheit

Prof. Dr. Jürgen Stock, Leiter des Kriminalistischen Instituts Im Bundeskriminalamt

Biometrie und Innere Sicherheit sind ein Begriffspaar, das mit Ende des 19. Jahrhunderts in der wissenschaftlichen Kriminalistik auftaucht – also die Wissenschaft von den Methoden und Mitteln der Verhütung, Aufdeckung und Aufklärung von Straftaten einschließlich der Fahndung nach Personen und Sachen ergänzen sollte.

Die frühesten Wurzeln der Biometrie gehen auf das Jahr 1879 zurück, als bei der Pariser Polizei unter Alphonse Bertillon mit der Vermessung des Körperbaus von Straftätern mit dem Ziel begonnen wurde, diese anhand der erhobenen Daten zweifelsfrei zu einem späteren Zeitpunkt wieder identifizieren zu können und somit die objektive Personenidentifizierung zu erleichtern.

Spätestens 1903, als in den USA anhand dieses noch ungenauen Systems zwei Personen mit beinahe gleichem Körperbau festgestellt wurden, setzte sich das biometrische Verfahren der Identifizierung anhand von Fingerabdrücken (bereits 1896 in Argentinien und 1898 in England eingeführt) endgültig durch, das als das erste verläßliche manuelle biometrische Identifizierungssystem angesehen werden kann.

Seither, und insbesondere in den letzten zwanzig Jahren, haben sich die Möglichkeiten der Verbrechensbekämpfung durch den Einsatz von Technik rasant entwickelt. Das Bundeskriminalamt hat darauf schon vor längerer Zeit durch die Einrichtung einer Gruppe Neue Technologien reagiert, deren Mitarbeiter den Markt nach für den Kriminalisten Verwertbarem sondieren und eigene Entwicklungen durchführen, aber auch prüfen sollen, inwieweit sich Straftäter neue Technologien zu Nutze machen können.

Die Bundesregierung misst der Kriminalprävention durch Technik auf nationaler und internationaler Ebene einen hohen Stellenwert zu. Dies war schon vor dem 11. September so, hat aber nach den Terrorakten in den USA nochmals eine besondere Bedeutung erfahren. Neben der Aufgabe der Ermittlung der Terroristen und ihrer Unterstützer und Hintermänner trat nämlich die Gefahrenabwehr besonders in den Blickwinkel mit der zentralen Frage, wie sich derartige menschenverachtende und verbrecherische Akte künftig wirksamer verhindern lassen? Damit verbunden ist die Überprüfung, an welchen Stellen unsere moderne postindustrielle Gesellschaft besonders verwundbar ist, Stichwort etwa die sog. kritischen Infrastrukturen.

Biometrische Verfahren, also das Erkennen von Personen mit Hilfe ihrer individuellen Körpermerkmale wie z.B. dem Fingerabdruck, dem Gesicht, dem Auge oder der Hand erschienen schnell als ein geeigneter Weg, auch in der Bekämpfung des islamistischen Terrorismus wesentliche Impulse setzen zu können.

Der Bedeutung dieses Themas entsprechend werden durch das Bundeskriminalamt in Zusammenarbeit mit anderen Behörden wie dem Bundesamt für die Sicherheit in der Informationstechnik Projekte und Studien initiiert, um die Eignung der verschiedenen Systeme für einen Einsatz in sicherheits- und polizeirelevanten Bereichen zu prüfen und verlässliche Aussagen über deren Praxistauglichkeit machen zu können.

Grundsätzlich gibt es **zwei verschiedenartige Anwendungen** biometrischer Verfahren, auf deren unterschiedliche Zielsetzung im Rahmen der aktuellen Diskussion um die Biometrie deutlich hinzuweisen ist:

Identifikation (1:n-Vergleich)

Eine zu überprüfende Person soll aus einer vorgegebenen Menge, z.B. einer Datenbank gesuchter Straftäter, erkannt werden. Hier wird also die Identifikationsfrage „wer bin ich?“ gestellt. Diese Anwendung setzt allerdings sehr leistungsstarke Rechnersysteme und Datenbanken voraus. Auch sind nicht alle biometrischen Verfahren technisch dazu geeignet. Wenn ein Verfahren nicht genügend Merkmale erfasst und auswertet (z.B. einfachere Verfahren der Fingerabdruckerkennung, die nur wenige Merkmale aufnehmen), kommt es bei großen Datenbanken sehr schnell zu einer Überforderung des Systems.

Verifikation (1:1-Vergleich)

Hier wird vom System eine Identitätsüberprüfung gefordert, um die Frage zu beantworten: „Bin ich der, für den ich mich ausgebe?“. Es soll also die Identitätsgleichheit einer aktuell anwesenden Person mit der Person, deren Referenzdaten vorliegen, bestätigt oder ausgeschlossen werden. In der Praxis könnte im Verifikationsverfahren z.B. geklärt werden, ob die zu überprüfende Person mit der im Ausweisdokument abgebildeten Person identisch ist; eine kriminalistisch zentrale Fragestellung angesichts häufig auftretender Schwierigkeiten bei der sicheren Identitätsfeststellung. Gerade bei international agierenden Tätern, die mit falschen Papieren und zigfachen Aliasnamen operieren, muss es zentrales Ziel der Strafverfolgung sein, hier größtmögliche Sicherheit bei der Feststellung der Person zu bekommen.

Eine solche Anwendung stellt geringere Anforderungen an die Leistungsfähigkeit der IT-Infrastruktur und wird von den heute auf dem Markt befindlichen Produkten in akzeptabler Zeit, allerdings mit unterschiedlicher Zuverlässigkeit, erfüllt.

In einer seriösen Diskussion um potenzielle künftige Einsatzbereiche biometrischer Produkte für Zwecke der Inneren Sicherheit muss in jedem Falle berücksichtigt werden, dass aufgrund von Messfehlern und natürlichen Alterungseffekten bei bestimmten biometrischen Merkmalen sowohl beim Identifikationsmodus als auch bei der Verifikation nicht die Gleichheit der Daten, sondern nur eine im Rahmen festgelegter Toleranzen hinreichende Ähnlichkeit geprüft wird.

Zwei zu verschiedenen Zeitpunkten aufgenommene digitale Abbildungen eines biometrischen Merkmals sind daher niemals identisch. Vielmehr ergeben sich mehr oder weniger deutliche Differenzen zwischen den aktuell gelesenen und den gespeicherten Daten, die bei Codewort- oder PIN-gestützten herkömmlichen Verfahren unbekannt sind.

Aus diesen systemimmanenten Abweichungen sind biometrische Verfahren u.a. durch Fehlerquoten in Form von Falschakzeptanzraten und Fehlzurückkweisungsraten gekennzeichnet.

Außerdem ist evident, dass gerade wegen der Öffentlichkeit der biometrischen Merkmale von Menschen und deren Zuordnungsmöglichkeit zu konkreten Personen sowohl besondere sicherheitstechnische Anforderungen als auch die Berücksichtigung potenzieller sozialer und gesellschaftlicher Folgen verlangt werden müssen. Im Gegensatz zu den schon lange gebräuchlichen Authentisierungsmethoden, bei denen das Wissen um ein Geheimnis (z.B. Passwort oder PIN) oder der Besitz eines materiellen Berechtigungsnachweises (z.B. Chipkarte, Ausweis) notwendig ist, können die öffentlichen biometrischen Merkmale einer Person etwa bei missbräuchlicher Verwendung durch Unbefugte nicht einfach „ersetzt" werden.

Aus polizeilicher Sicht erscheint zunächst eine Befassung mit folgenden ausgewählten Biometrieverfahren angezeigt:

Finger(abdruck)erkennung.

Von den meisten biometrischen Systemen wird der Fingerabdruck für eine Benutzererkennung verwendet. Auf Grund der Einzigartigkeit der Papillarlinien wird für die Identitätsgleichheit beim Einsatz von Fingerabdrucklesern zur biometrischen Verifikation meist eine Größenordnung von 1:1.000.000 angegeben. Grundsätzlich ist zwischen polizeilichen Fingerabdruckerkennungssystemen und Produkten für den zivilen Einsatz zu unterscheiden. Die polizeilichen Systeme wie das Automatische Fingerabdruck-Informationssystem AFIS sind für Identifizierungen von Fingerabdrücken aus einem großen Datenbestand ausgelegt. Während der Enrolmentprozess aller 10 Finger hier sehr aufwändig ist, erfassen kommerzielle Sensoren lediglich aufgelegte Fingerteilflächen. Neben noch unzureichenden Fehlerkennungsraten ist auch die Lebenderkennung ein noch weitgehend ungelöstes Problem.

Gesichtserkennung

Aufnahmen des Gesichts zur Verifikation oder Identifikation erfolgen entweder mittels Digital- oder Analogkamera. Die Qualität der Vergleichsergebnisse, die Gesichtserkennungssysteme in der Praxis liefern können, hängt maßgeblich von der Anzahl und Qualität der Vergleichsbilder bzw. Referenztemplates ab. Entsprechend dem Einsatzbereich des Systems reicht entweder ein zweidimensionales Bild (z.B. ein Passbild) für die Verifikation oder es sind mehrere Aufnahmen aus unterschiedlichen Perspektiven erforderlich, um ein „dreidimensionales" Bild in das entsprechende Template umzuwandeln.

Die Vorteile der Gesichtserkennung liegen in der Benutzerfreundlichkeit, da es sich um ein berührungsloses System handelt und die zu überprüfende Person normalerweise nicht aktiv werden muss. Außerdem steht der Mensch als zusätzliche Kontrollinstanz im Hintergrund zur Verfügung, Lichtbilder in Ausweisen können bei Bedarf auch visuell kontrolliert werden.

Handgeometrie

Die Hand ist ein leicht zugängliches biometrisches Merkmal, bei dem sich zur Identifizierung unter anderem die Fingerlänge, die Breite und Krümmung der Finger, die Stärke und Position der Fingergelenke oder auch die gesamte Handbreite anbieten. Da jedoch die Einzigartigkeit der Hand als biometrisches Merkmal nicht gegeben ist (Häufigkeit etwa 1:10.000), eignen sich Handgeometriescanner nur zur Verifikation, nicht aber zur Identifikation.

Iriserkennung

Das Iris-Muster ist einzigartig und konstant, die Wahrscheinlichkeit, dass zweimal das gleiche Template errechnet wird, liegt bei 1:10 hoch 78. Zur Aufnahme werden Monochromkameras (schwarz-weiß) genutzt. Aus dem anschließend digitalisierten Bild der Iris wird das Template errechnet. Bei Einbindung einer Lebenderkennung ist die Iris in hohem Maße fälschungssicher. Sie eignet sich grundsätzlich sowohl für die Verifikation als auch für die Identifikation. Nachteilig sind die hohen Kosten für das aufwändige Kamerasystem, die erforderlichen konstanten Lichtverhältnisse sowie eine bisher geringe Benutzerakzeptanz.

Unterschriftenerkennung

Die automatische Unterschriftenprüfung ist ein noch sehr junges Forschungsgebiet. Grundsätzlich wird zwischen der Erfassung des statischen Schriftbildes mittels Kamera und des dynamischen Schriftbildes mittels sog. Grafiktablett (online) unterschieden. Bei modernen Handschriftenerkennungssystemen zur Verifikation oder Identifikation wird die geleistete Unterschrift mehrdimensional digital erfasst (z.B. Druckstärke, Stiftposition, Länge, Breite und Zeitverlauf).

Nach den Terroranschläge in den USA ist ein gesteigerter Bedarf an biometrischen Identifikationssystemen zu Zwecken der Zugangs- und Zutrittskontrolle artikuliert worden.

Die Innen- und Justizminister der Europäischen Union haben am 20. September 2001 in einer von Deutschland initiierten Sondersitzung des Rates Justiz und Inneres einen umfangreichen **Maßnahmenkatalog zur Terrorismusbekämpfung** beschlossen. Dieser Katalog sieht unter anderem Maßnahmen bei der Visaerteilung, der Grenzkontrolle sowie Maßnahmen im Inland vor, die sich in weiten Bereichen mit dem nationalen Sicherheitspaket decken.

Mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 hat die Bundesrepublik Deutschland zahlreiche Sicherheitsgesetze der neuen Bedrohungslage angepasst.

Unter anderem wurden das *Passgesetz* und das *Gesetz über Personalausweise* sowie das *Ausländergesetz* und das *Asylverfahrensgesetz* geändert, um die Identifizierung von Personen zu verbessern. Mit der Änderung dieser Gesetze wurde nun erstmals auch die Ermächtigungsgrundlage für die Nutzung biometrischer Merkmale in deutschen Pässen und Personalausweisen sowie Aufenthaltsgenehmigungen und anderen ausländerrechtlichen Personaldokumenten gegeben.

Neben dem Lichtbild und der Unterschrift dürfen die **Personaldokumente** seit Anfang dieses Jahres weitere **biometrische Merkmale** von Fingern, Händen oder Gesicht des Inhabers enthalten. Die bei bestimmten biometrischen Verfahren genutzte Iris ist zwar nicht explizit aufgeführt, dürfte aber nach Meinung der Fachleute als Bestandteil des Gesichts ebenfalls in Betracht kommen.

Dabei dürfen all diese biometrischen Merkmale sowie die sonstigen Angaben zur Person mit Sicherheitsverfahren verschlüsselt in das Ausweisdokument eingebracht werden. Die Zweckbindung bestimmt, dass die verschlüsselten Merkmale und Angaben nur zur Echtheitsprüfung des Dokuments und zur Identitätsprüfung des Inhabers verwendet werden dürfen. Eine bundesweite Datei soll nicht eingerichtet werden.

Die Ausstellung von **Visa** bis 3 Monaten Aufenthaltsdauer ist durch EU-Recht geregelt (EU-Visaverordnung, Schengener Durchführungsübereinkommen), wo die Aufnahme biometrischer Merkmale in die Visadokumente bisher nicht vorgesehen ist. Die aus anderem Grund (Vorbeugung illegaler Lichtbildauswechslungen in ausländischen Personaldokumenten mit Sichtvermerken) erfolgte Anpassung der EU-Visa-Verordnung durch den Rat ermöglicht jedoch seit Anfang dieses Jahres die Aufnahme von Lichtbildern in das Visadokument selbst. Die Aufnahme weiterer biometrischer Merkmale hingegen würde eine erneute Änderung des Gemeinschaftsrechts auf dem Wege einer EU-Verordnung erfordern.

Im Ergebnis wird mit der Aufnahme von biometrischen Merkmalen in Pässe, Personalausweise und andere Personaldokumente das Ziel verfolgt, die Identitätsprüfung im Rahmen bestimmter Kontrollmaßnahmen (z.B. bei der Grenzkontrolle) durch **Automatisierung** zu verbessern. In diesem Zusammenhang geht es immer um den Abgleich zwischen der aktuell zu kontrollierenden Person und dem zur Legitimation vorgelegten Ausweisdokument und den darin enthaltenen Identitätsdaten (sog. Verifikationsmodus, 1:1-Vergleich).

Um die politischen Entscheidungsträger zu der Frage kompetent beraten zu können, welche biometrischen Merkmale künftig für welche spezifischen Zwecke genutzt werden sollten, müssen die derzeit auf dem Markt verfügbaren Biometrieverfahren einer qualifizierten Analyse unterzogen werden. Aber auch die Rahmenbedingungen und Konsequenzen im gesamten geplanten Anwendungsbereich sind zu berücksichtigen und in die Kosten-Nutzen-Abwägung vorausschauend einzubeziehen. Im Falle des Einsatzes biometrischer Verfahren in Personaldokumenten bedeutet dies zum Beispiel, das Anwendungsspektrum in Bezug auf die einzubeziehenden Dokumentensysteme von der Ausstellungsebene über die Dokumententechnik bis hin zur Kontrollebene ganzheitlich zu betrachten.

Selbstverständlich ist in diesen Bereichen auch die internationale Zusammenarbeit eine entscheidende Planungsgröße. Insbesondere die notwendige Standardisierung und Harmonisierung der Konzepte kann nur durch ein gemeinsames Vorgehen auf transnationaler Ebene erreicht werden.

Staatliche Behörden, Forschungs- und Lehrinstitute sowie die Industrie treiben die Entwicklung der biometrischen Identifikation voran. Deshalb ist in naher Zukunft ihr Einsatz in sicherheitsrelevanten Applikationen zu erwarten.

Um beispielhaft weitere Entwicklungen in der Biometrie betr. des Aufgabenfelds „Innere Sicherheit" nennen zu können, ist zunächst zu berücksichtigen, dass nahezu alle denkbaren biometrischen Anwendungen die Aufgabe haben, Personen zu identifizieren. Somit lassen sich die **Aufgabenfelder der Biometrie** grundsätzlich in zwei große Bereiche unterteilen :

a) Zutritts- und Zugangskontrolle
und
b) Fahndung.

Unter **a)** lassen sich beispielhaft subsumieren :

- Integration weiterer biometrischer Merkmale neben dem Lichtbild in Personaldokumente im Rahmen der Terrorismusbekämpfung
- Einsatz biometrischer Identifizierungsverfahren zur Kontrolle des physischen Zutritts zu sicherheitsempfindlichen Bereichen wie die Infrastruktur von Flughäfen (zur Abwehr terroristischer Bedrohungen) oder zu Großveranstaltungen wie etwa Fußballspiele (Kontrolle von Hooligans)
- Kontrolle des Zugangs und Aufenthalts ausschließlich Berechtigter zum Cockpit von Luftfahrzeugen oder sonstiger Verkehrsmittel zur Vorbeugung gegen Entführung oder Diebstahl
- Einsatz der Biometrie für weitere Zwecke der Technischen Prävention, etwa zur Unbrauchbarmachung gestohlener Mobilfunkgeräte, zur Sicherung von Wohnungen und anderem Eigentum
- Einsatz der Biometrie im Rahmen der Digitalen Signatur zur Absicherung rechtsverbindlicher Transaktionen über Datennetze (Stichwort : e-commerce)
- Kontrolle der Zu- und Abgänge bzw. der Aufenthaltsregelungen (zugewiesene Arbeitsbereiche von Inhaftierten) im Justizvollzug
- Aufrüstung des neuen digitalen Dienstausweises mit einem biometrischen Merkmal.

Zu b) gehören der

- Einsatz von Gesichtserkennungsverfahren als Fahndungshilfsmittel an Kriminalitätsbrennpunkten sowie bei der Grenzkontrolle (Videoüberwachung auf öffentlichen Straßen und Plätzen, Bildabgleich mit Fahndungsdatenbanken)

- Mobiler Einsatz von Fingerabdruckscannern zur Personenerkennung vor Ort (Kontrollstellen, Razzien)
- Erweiterte ED-Maßnahmen => Erfassung verschiedener biometrischer Merkmale wie *Fingerabdrücke Schrift, Stimme, Gang, Gesicht und DNA* zur Gewinnung von Referenzdaten für künftige Tat /Tat- und Tat /Tätervergleiche (Beispiel : Phantombild / Referenzdatei)

Ergänzend muß ausgeführt werden, dass die Integration weiterer biometrischer Merkmale neben dem Lichtbild in Personaldokumente gleichzeitig die Grundlage für Zutrittskontrolle und Fahndung im Rahmen einer Identitätsüberprüfung / Personenkontrolle ermöglicht.

Die Sicherheit dieser Identitätsprüfung bezieht sich jedoch nur auf die Übereinstimmung von biometrischen Merkmalen im Personaldokument mit den biometrischen Merkmalen des Ausweisträgers. Die eigentliche Echtheit der Personalien muß bereits bei Erstellung des Ausweisdokumentes geprüft werden.

Letztendlich gewährleisten zusätzliche biometrische Merkmale in Personaldokumenten lediglich den Schutz vor mißbräuchlicher Verwendung fremder Ausweispapiere von Menschen, die sich z.B. sehr ähnlich sehen.

Weiter gewährleisten nur wenige Systeme im oberen Preissegment schon heute technische Sicherheit in ausreichendem Maße.

Neue Konzepte der Lebenderkennung, die biometrische Systeme vor Überwindungsversuchen durch Fälschungen und Kopien schützen soll, müssen sich noch beweisen. Nach zuverlässiger Lösung dieser Probleme kann die Biometrie aber durchaus als Konzept zur Identifikation von Personen in sicherheitsrelevanten Bereichen überzeugen.

Gleichwohl wird immer eine genaue Analyse der Tauglichkeit biometrischer Verfahren in Abhängigkeit vom beabsichtigten Einsatzgebiet anzuraten sein. Denn es ist ein für die Biometrie typisches Problem, die Toleranzschwellen so einzustellen, dass eine zu hohe Fehlzurückweisungsrate berechtigter Personen vermieden und gleichzeitig aber die Fehlakzeptanz unberechtigter Personen ausgeschlossen wird.

Fazit: Biometrische Verfahren können in verschiedenen Kriminalitätsbereichen ein Baustein in Bekämpfungskonzepten sein, indem die ansonsten manuelle Überprüfung durch den Menschen in einem größeren Maßstab computergesteuert automatisiert ermöglicht wird. Der Einsatz kommt also in jedem Kriminalitätsfeld in Frage, bei dem Personen versuchen, unter falscher Identität Zutritt zu bestimmten Objekten oder Zugang zu Leistungen und Informationen zu erhalten. Weiter kann die Biometrie Fahndungshilfsmittel sein, indem künstliche Sensoren ermüdungsfrei die Augen des Menschen ersetzen und Vergleichsalgorithmen den Abgleich großer Datenbanken übernehmen.

Die Frage der Zweck-Mittel-Relation, also der Verhältnismäßigkeit, muss je nach Grundrechtsrelevanz auf der Grundlage eines kriminalpolitischen Diskurses innerhalb der Gesellschaft von der Politik entschieden werden, wie das auch bei zahlreichen anderen Beispielen in der Vergangenheit der Fall war. Unser Rechtssystem kennt keine Strafverfolgung um jeden Preis. Das Schutzbedürfnis der Bevölkerung auf der anderen Seite verpflichtet den Staat zu wirksamen Maßnahmen der Strafverfolgung und Gefahrenabwehr. In diesem Spannungsfeld werden biometrische Verfahren auch in Zukunft weitere Fortschritte vor allem in der vorbeugenden Verbrechensbekämpfung bringen.

BioTrusT: Einige Ergebnisse und Wirkungen

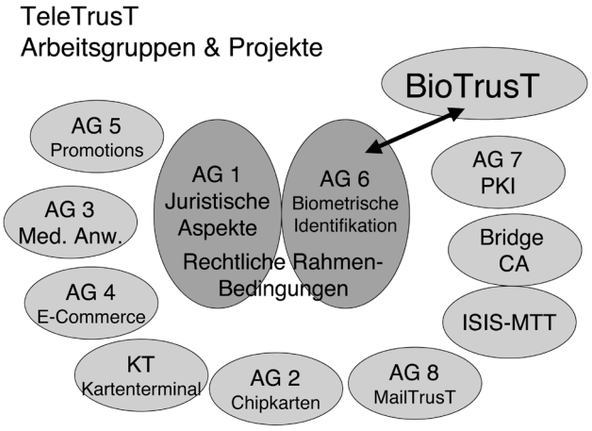
Prof.Helmut Reimer TeleTrusT Deutschland e. V.

TeleTrusT Deutschland e. V.

- Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
- angewandte **Kryptographie** und **Biometrie**
- gegründet 1989
- 110 Mitglieder: Hersteller, Systemintegratoren, Anwendungsbereiche, Prüfinstitute...
- gemeinnützig und unabhängig

TeleTrusT & Biometrie

- 1996 – AG ‚Biometrische Identifikationsverfahren'
- Schwerpunkt: Biometrie & IT-Sicherheit
- 1998 – Kriterienkatalog / Neufassung 2002
- 1999-2002: Projekt BioTrusT
- Biometrie-Promotions: CeBIT, SYSTEMS, RSA, ISSE, IEEE, EU ....



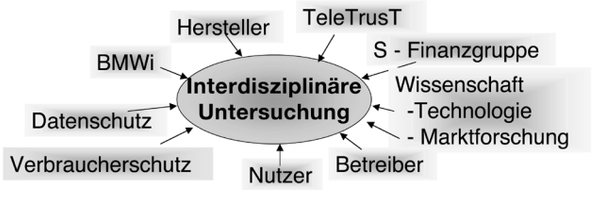
BioTrusT - Ziele

- Verbesserung der Marktchancen für biometrische Systeme:
  - Innovationsförderung
  - Evaluierung
- Authentisierung in elektronischen Geschäftsprozessen:
  - Vertrauenswürdigkeit von Anwendungen
  - Nutzerakzeptanz
- Wissenschaftliche Fragestellungen:
  - Anwendungsverhalten biometr. Systeme
  - Evaluierung von Datenschutz und –Sicherheit
  - Evaluierung von Nutzerakzeptanz und Verbraucherschutz
  - Entwicklung von Schnittstellen und Standards

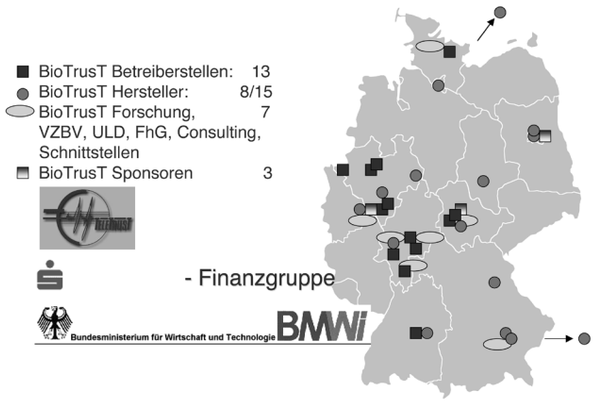
BioTrusT: Interdisziplinär und komplex

Viele Hersteller unterschiedlicher biometrischer Verfahren wollen in den Markt

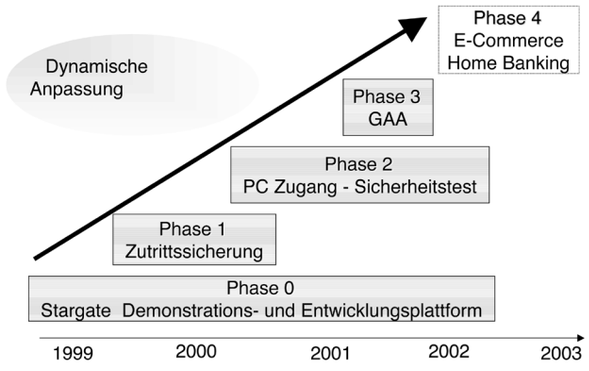
Eine Fülle von offenen Fragen lassen sich nur durch einen Massentest untersuchen



BioTrusT Kooperationspartner



BioTrusT: Test- und Evaluierungspakete



Phase 1 (Voruntersuchung) Zutrittssicherung - Robustheitstest

Gesichtserkennung		
	ZN	Informatik Kooperation
	Plettac	SKW
Fingererkennung		
	Atair	SKW
	Bergdata	Informatik Kooperation
	G&D	DSV
Spracherkennung		
	ABS	FH
Iriserkennung		
	SNI	DSV
Multimodal		
	DCS	FH

Empirische Studie mit wissenschaftlicher Auswertung durch
FH Giessen-Friedberg (Prof. Behrens / Prof. Roth)
Empfehlungen von
– Verbraucherschutz
– Datenschutz

Phase 2 PC-Zugang - Sicherheitstest

Ziele

- Entwicklung / Adaption einer Standardschnittstelle zum IT-System (BioAPI)
- Test von verschiedenen Biometrieverfahren
- Entwicklung eines Verfahrens zur Registrierung und Analyse des Nutzerverhaltens

- Drei Testserien
  - BioAPI 1.0 / Templatespeicherung im PC
  - BioAPI 1.1 / Templatespeicherung im PC
  - BioAPI 1.1 / Templatespeicherung auf SmartCard

BioAPI-Implementierungen für

- Fingerprint
- Signatur
- Iris Recognition
- Multimodale Verfahren
- Anwendungen

Phase 3
Evaluierung – Biometrie und GAA

Ziel

- Evaluierung der Anforderungen an eine biometrische Identifikation als Ersatz für die PIN
  - Bankspezifische Aspekte
  - Verbraucherschutzrechtliche Aspekte
  - Datenschutzrechtliche Aspekte
  - Allgemeine Richtlinien

BioTrusT – Ergebnisse I

- **Verbesserung von Biometrielösungen**
  + Hersteller verbessern ihre Lösungen -> Wettbewerbsvorteil (BioAPI, Benutzerführung, Templates auf Chips, Standardanwendungen)
  + Empfehlungen von Datenschutz, Verbraucherschutz, Benutzeranalysen
  + Positionierung der S-Finanzgruppe (Einführung, Integration, Betrieb)
- **Hervorragendes Biometriewissen**
  + Projektpartner
  + Interdisziplinäre Kompetenz
  + Vorlesung und Labor bei der FH Gießen-Friedberg
- **Enge Kooperation der Biometrienawender und Wissensträger**
  + Projektpartner u. A.: BKA, BSI, Dt. Telekom, Bundesdruckerei

BioTrusT – Ergebnisse II

- Die konkrete Anwendung der Biometrie ist Differenzierungsmerkmal für Anforderungen
- Die tatsächliche IT-Systemssicherheit kann durch die Hinzunahme biometrischer Verfahren verbessert werden
- Die Infrastruktur für den Umgang mit Biometrie (Administration) muss unbedingt berücksichtigt werden und erfordert erhebliche Ressourcen

BioTrusT-Ergebnisse III

- Deutsche Aktivitäten zur Biometrie sind international wirksam geworden – insbesondere auch in Standardisierungsgremien
- TeleTrusT kooperiert zunehmend mit anderen relevanten Organisationen
- Beiträge zur Weiterentwicklung der Sicht auf Biometrie und Anwendungszusammenhänge
- Grundlagen für Pilotanwendungen stehen bereit

Sicherheit durch Biometrie?

- Biometriedaten sind nicht streng digital reproduzierbar
- Automatische Identifikation und Verifikation haben Fehlerraten, die eine Risikoabschätzung erfordern
- Performance und Fehlerraten verhalten sich gegenläufig
- Lebenderkennung ist wichtige Maßnahme zur Vermeidung von (einfachen) Überwindungsangriffen

Faktoren für die Bewertung der Sicherheit

Herkömmliche Verfahren, ihre Risiken und Infrastrukturen komplex betrachten:

- Zutrittskontrolle, Zugangssysteme – Schlüsselsysteme, Teilnehmerverwaltung Sicherheitsrisiko: Verlorene oder weitergegebene Token
- Zugriffskontrolle – PasswortverwaltungSicherheitsrisiko: Menschlicher Umgang mit ‚Geheimnissen'

Biometrie: Körperliche Anwesenheit ‚eines' Teilnehmers

Biometrie bietet mehr als Sicherheit

- Biometrieintegration darf die Sicherheit und Verlässlichkeit von Anwendungen nicht beeinträchtigen!
- Biometrie kann zusätzliches Vertrauen in Anwendungen ermöglichen!

Biometrische Systeme in der Anwendung

Herr Seibt, Zentralverband Elektrotechnik- Elektronikindustrie e.V.

Biometrische Verfahren zur Verifikation oder Identifikation von Personen sind heute „in aller Munde".

Ausgelöst wurde die teilweise hektische Betriebsamkeit u. a. durch die Gesetzgebung in Deutschland, biometrische Merkmale im Personalausweis zu speichern und durch den Druck der USA Pässe und Visum mit eben diesen Merkmalen zu ergänzen. Darüber hinaus diskutieren und testen Fluggesellschaften bzw. Flughafenbetreiber biometrische Systeme, um bei den Fluggästen die „Spreu vom Weizen" zu trennen – um nur eine weitere Anwendungsmöglichkeit zu nennen.

Weltweit haben sich die verschiedensten Unternehmen auf die Entwicklung und Vermarktung biometrische Systeme gestürzt.

Das ohnehin schon schwierige Gebiet menschliche Merkmale zu erfassen und zu vergleichen – der Mensch ist nun einmal nicht standardisiert – wird durch die Vielzahl der Anbieter nicht einfacher.

Umso mehr ist es an dieser Stelle notwendig, auf den sehr positiven Aspekt hinzuweisen, das der DFK namentlich Herr Ziercke, sich dieser Thematik annimmt und so erneut zum Ausdruck bringt, das neben der Wertevermittlung und der Stärkung des Rechtsbewusstseins der Schutz vor Kriminalität durch personelle und technische Maßnahmen eine wichtige Säule der Kriminalprävention bildet.

Doch nun zurück zur Technik:

Die unterschiedlichen Verfahren und das Fehlen von Anwendungs- und Prüfrichtlinien verkomplizieren die Auswahl für den Anwender.

Andererseits ruft der Markt nach Verfahren, die die Identifikation oder Verifikation von Personen im Sinne von Freund-Feind-Erkennung mit hoher Erkennungssicherheit erlauben.

Diese Verfahren kann man sicherlich mit biometrischen Systemen abdecken, sofern die Funktionssicherheit gewährleistet wird; hierin sind sich alle Fachleute einig.

Biometrie in der Kriminalprävention kann also als ein entscheidendes Mittel für die Stärkung der Sicherheit, nicht nur in Europa angesehen werden.

Derzeitig laufen biometrische Systeme allerdings Gefahr in der öffentlichen Diskussion als Wunderwaffe bezeichnet oder Teufelswerkzeug verbannt zu werden.

Ein unbedingt notwendiger Schritt ist daher als Voraussetzung für den breiten Einsatz von Biometrie, für den Anwender Leitlinien über Auswahlverfahren und Einsatzmöglichkeiten zu schaffen und Qualitätsstandards zu definieren.

Darüber hinaus ist aber auch der gesellschaftspolitische Aspekt nicht zuletzt unter datenschutzrechtlichen Bedingungen zu beleuchten und somit ist es nur folgerichtig, dass der DFK sich dieses Themas annimmt.

Der ZVEI-Zentralverband Elektrotechnik und Elektronikindustrie ist der Auffassung, dass beide Bereiche, d.h. die technischen und die gesellschaftspolitischen Aspekte nicht losgelöst betrachtet werden können ohne Gefahr zu laufen, die Rechnung ohne den Wirt gemacht zu haben. Insbesondere unter der Sicht der Wirksamkeit und der Akzeptanz wird es ohne eine genaue Analyse der technischen Möglichkeiten und der Funktionalität nicht gehen.

Die Mitarbeit des ZVEI in einem Arbeitskreis des DFK, der sich zur Aufgabe gemacht hat, die gesellschaftspolitische Bedeutung biometrischer Verfahren im Rahmen der Kriminalprävention zu analysieren und einer kriminalpolitischen Bewertung zu unterziehen, ist daher notwendig. Auf der Basis dieser Überlegungen hat der ZVEI einen Arbeitskreis gegründet, der sich mit der Technik von biometrischen Systemen in der Anwendung befasst.

Zunächst einmal galt es eine Struktur zu finden, die die Anwendungsbereiche solcher Systeme verdeutlicht.

In der Matrix (siehe nächste Seite) sind die biometrischen Systeme in fünf Bereiche wie folgt gegliedert:

1. spielerischer Einsatz
2. Nutzungsberechtigung
3. sicherheitstechnische Anwendungen – kooperativ
4. sicherheitstechnische Anwendungen – nicht kooperativ
5. hoheitliche Anwendungen

Im weiteren Schritt sind beispielhaft die wichtigsten Anwender genannt. Die nächste Ebene zeigt die „Treiber", die die Weiterentwicklung der Systeme wesentlich beeinflussen. Darunter sind einige Einsatzmöglichkeiten definiert sowie die Anwendergruppen. Als Basis für alle Anwendungsbereiche sind die Normen auf nationaler, europäischer und internationaler Ebene zu nennen.

Die Verbindungspfeile zeigen in der Matrix die Abhängigkeiten bzw. die Einflüsse der einzelnen Bereiche untereinander.

Über alle Bereiche hinweg können die Applikationen in vier Kategorien unterteilt werden:

- Nachweis einer Berechtigung (Verifikation)
- Elektronische Personalisierung von Merkmalen der Rückverfolgung (Tracking)
- Berechtigungprüfung als Komfort
- Identifikation

Auf der Basis dieser Strukturen sind z. Zt. zwei Unterarbeitskreise wie folgt tätig:

a) Anwendungsrichtlinien erarbeiten im Sinne der Norm (application guidlines)
b) Standards und Prüfrichtlinien

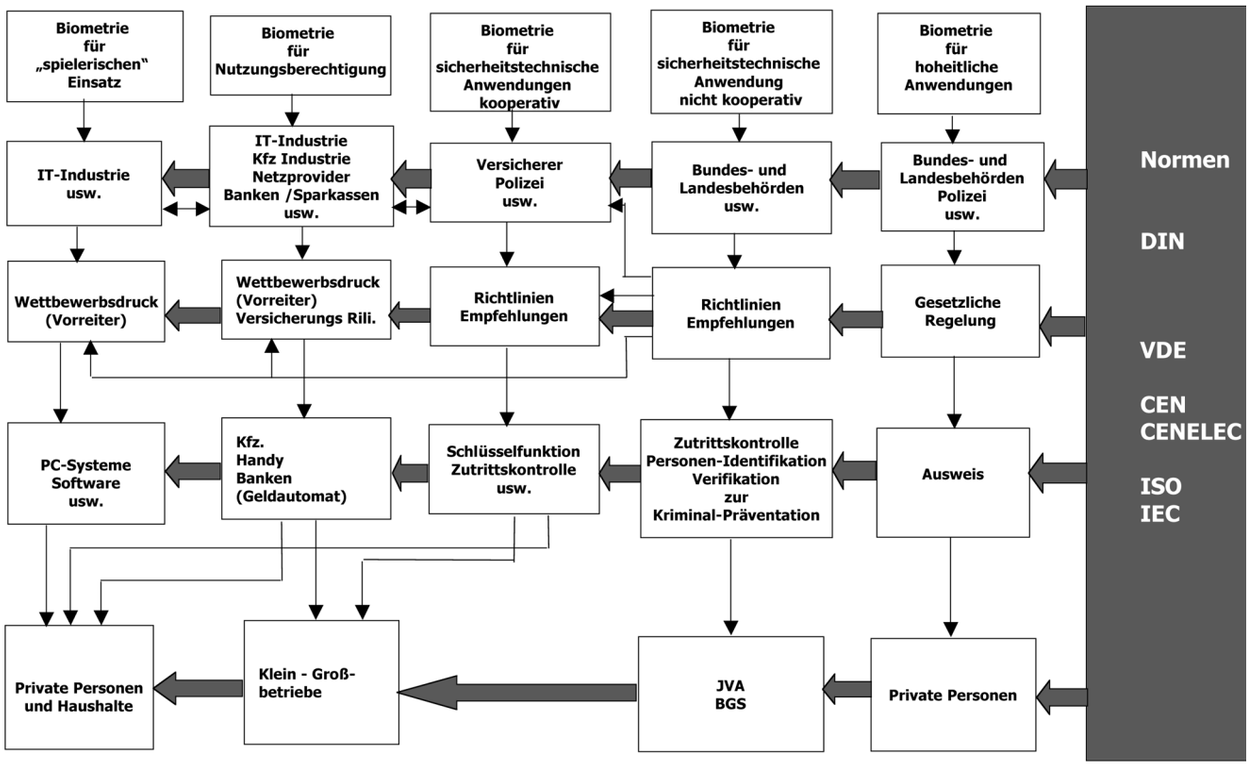
Ist-Situation und Bedarf ermitteln

Bis zur Security sollen bereits erste Ergebnisse vorgestellt werden.

Zur Vermeidung von Doppelarbeit ist eine Abgrenzung innerhalb des Systemaufbaus von biometrischen Systemen notwendig. In Anlage 2 sind die grundsätzlichen Systemkomponenten aufgezeigt:

- Datenerfassung – Aufbereitung

Strategie Biometrie in der Anwendung



- Daten-Übertragung
- Datenspeicherung auf Chip
- Datenbank zentral (abhängig von Anwendung)
- Datenvergleich und Ergebnisanzeige

Der ZVEI befasst sich im wesentlichen mit den Systemen zur Erfassung biometrischer Daten, deren Aufbereitung und deren Verarbeitung zur Verifikation bzw. Identifikation.

Für die Übertragung von Daten und deren Speicherung auf Chips werden lediglich Anforderungen definiert, die mit Arbeitsgruppen anderer Verbände z. B. Bitkom in engem Schulterschluss abzustimmen sind.

Um die Arbeiten der AG abzurunden, sind auch das BKA, BSI, der VdS, der Datenschutz und die Projektorganisation TeleTrust eingebunden und bringen somit ihre eigenen Erfahrungen und Kenntnisse ein, dabei legen wir großen Wert darauf, dass der AK Technik auf schon vorliegende Ausarbeitungen (etwa durch BKA, BSI oder Biotrust) aufbaut und nicht das Rad zum zweiten Mal erfindet.

Alle Beteiligten sind davon überzeugt, dass mit dieser Vorgehensweise sowohl für den Anwender wichtige Entscheidungsgrundlagen in absehbarer Zeit zur Verfügung stehen, als auch die unbedingt notwendigen Normenarbeiten strukturiert vorangetrieben werden.

Dabei ist durch die Einbindung dieser ZVEI-AG in den DFK auch sichergestellt, dass der Kriminalprävention und der bevölkerungspolitischen Akzeptanz Rechnung getragen und deren Einflüsse auf die Systemwelt biometrischer Systeme sinnvoll umgesetzt werden können. Nicht zuletzt wird dies auch zur Versachlichung der politischen Diskussion beitragen.

IT-Sicherheit und Biometrie

Dipl. Math. Klaus J. Keus, Bundesamt für Sicherheit in der IT (BSI) Referatsleiter „Schlüsseltechnologien“

Einführung I:

Was ist *Biometrie*?

- Das Messen („Metrik“) von individuellen Merkmalen des menschlichen Körpers zum Zwecke der Identifikation
- Identität „Klaus Keus“

Einführung II:

Warum *Biometrie* und nicht ...?

↳ z.B.: Identifikation / Authentisierung durch:

- *Wissen:* Passwort, PIN, andere Geheimnisse
- *Besitz:* Chipkarte, Schlüssel, Token,...
- *Merkmal:* biometrische Eigenschaft

Einführung III:

Klassifizierung *biometrischer Merkmale*:

↳

- *Geno typisch:* biometrische Eigenschaften auf der Grundlage von Genen ⇩ partiell per Abstammung/Vererbung
- *zufällig typisch:* Entstehung in der embryonalen Phase durch Zufall ⇩ lebenslange Dauer
- konditioniert: biometrische Merkmale infolge Verhalten, Erziehung, Training etc. ⇩ änderbar im Lebenszyklus

Einführung IV:

Klassifikation von *biometrischen Verfahren*:

↳

- *Identifikation:*
  Erkennung der Identität ohne Vorwissen
  (1 : n - Vergleich)
- *Verifikation:*
  Überprüfung einer Vorgabe
  (1 : 1 - Vergleich)

Biometrie-Anwendungen:

↳ *Ziele:*

Identifikation / Authentisierung: von Sicherheit bis Convenience

- *typische Verfahren (einzelne, Kombinationen etc.):*
  - Finger Recognition
  - Gesicht Recognition
  - Sprache Recognition
  - Signatur
  - Retina
  - Iris
  - Handgeometrie
  - Tastaturanschlag (Geschwindigkeit, Druck)
  - Bewegung (Lippen, Gehen etc.)
  - DNA
  - Venen
  - Körpergeruch

Ziel:

- 1) Jeder authentische Nutzer wird akzeptiert
- 2) Jeder nicht authentische Nutzer wird nicht akzeptiert

Problem der Biometrie:

- authentische Benutzer werden abgewiesen (Convenience-Aspekt)
- nicht authentische Benutzer werden akzeptiert (Sicherheitsaspekt)

Das Ziel wird definiert durch das Mass an Toleranz !

- Toleranz wird u.a. festgelegt durch
- Anforderungen
  und
- Anwendungen

Anforderungen:

ausgerichtet durch Umfeld und Zweck:

↳

- *Umgebung*
- *Personen*
- *Anwendungen / Nutzung*
- *Technologie*

Technische Grundanforderungen

• verläßliche Identifikation	: Eindeutigkeit der Merkmale
• Zuverlässigkeit	: Langzeitbeständigkeit
• Verfügbarkeit Technik	: Chip, Algorithmen
• Integrität	: Schutz der Referenzdaten
• Hohe Akzeptanz/Komfort	: Verbreitung biometr. Merkmale, einfache Bedienung
• Sicherung der Vertraulichkeit	: Verschlüsselung, Zugriffschutz

IT-Sicherheitsanforderungen I

- Schutz vor verfälschter Erfassung
- Schutz vor Verfälschung des Merkmals (Integrität)
- Schutz vor Vortäuschung falscher Angaben (Authentizität)
- Schutz vor unberechtigter Verwendung der Daten (Vertraulichkeit)
- Schutz vor Angriff auf das System (Verfügbarkeit)

IT-Sicherheitsanforderungen II: mögliche Angriffe auf biometrische Systeme

- *Sensor:* Kamera, CMOS-Chip, Mikrofon, etc.
- Datenübertragung: seriell, parallel, USB, FBAS-Videosignal, etc. (teilw. klassische IT-Sicherheit, Beispielangriff: Replay-Attacken auf Video-Signal)
- Datenspeicherung (klassische IT-Sicherheit)

IT-Sicherheitsanforderungen III: Sicherheit am Sensor (1)

- gefährlichster Angriffspunkt, nicht baulich zu schützen, biometriespezifisch
- verschiedene Benutzer sollten verschiedene Merkmale haben ⇩ Abweisung von unbekannten Benutzern folgt aus der Erkennungsleistung (FAR), zufällige Falscherkennung bzw. algorithmische Schwäche
- Problem: Erkennung von Fälschungen („Lebenderkennung“) ⇩ es existiert (noch) keine (spezifische) Messmethode / Messwert für Überwindungssicherheit (CC: Strength of Function (SoF/SoM) / Widerstandsfähigkeit)

IT-Sicherheitsanforderungen IV: Sicherheit am Sensor (2)

mögliche Tradeoff-Kette:

- je mehr Lebenderkennung ⇩ komplexer die Erfassung
- je höher die Komplexität der Erfassung ⇩ schwieriger ist das

Erreichen guter Erkennungsleistungen

- und ⇩ teurer wird das biometrische System

↳ Zusammenfassung

- kein allgemein gültiger Ansatz, wir benötigen einen *zugeschnittenen Ansatz* (z.B. einfach, mittel, hoch)
- Biometrie Technologie ersetzt *nicht das Sicherheitspersonal*, d.h. keine voll automatisierte Kontrolle („grünes Licht Kontrolle“)
- Biometrie Technologie sollte verstanden werden als *Unterstützung für Sicherheit*
- Biometrie Technologie darf genutzt werden als Erweiterung/Verbesserung für Convenience

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?
Kontakt:
keus@bsi.bund.de
phone: + 49 (0)228 9582-141
fax: -455

Aktivitäten des Büros für Technikfolgen – Abschätzung beim Deutschen Bundestag (TAB) zum Thema „Biometrische Identifikationssysteme“

Herr Dr. Petermann, Büros für Technikfolgen – Abschätzung beim Deutschen Bundestag (TAB)

Es soll im Folgenden kurz berichtet werden über die bisherigen und zukünftigen Aktivitäten des TAB bezüglich biometrischer Identifikationssysteme. Zur besseren Einordnung dieser Aktivitäten wird zunächst das TAB als politikberatende Einrichtung des Deutschen Bundestages vorgestellt. Daran anschließend werden einige Ergebnisse des ersten TAB-Berichtes „Biometrische Identifikationssystem“ (TAB-Arbeitsbericht Nr. 76, Bauch erschienen als Bundestagsdrucksache [Nr. 14/10005]) zusammenfassend skizziert. Schließlich wird der Stand der augenblicklichen Analysearbeiten des TAB skizziert.

Das TAB-Ziele und Aufgaben

Das TAB ist eine selbständige wissenschaftliche Einrichtung, ihr Träger ist das Forschungszentrum Karlsruhe (FZK) bzw. das dortige Institut für Technikfolgenabschätzung und Systemanalyse (ITAS). Das TAB – mit Sitz in Berlin – arbeitet auf der Basis eines Vertrages zwischen FZK und Deutschem Bundestag, der die Ziele der Arbeit des TAB definiert und die Rechte und Pflichten der Beteiligten regelt.

Ziel des TAB und seiner Aktivitäten ist allgemein, den Deutschen Bundestag und seine Ausschüsse in Fragen der wissenschaftlich-technischen Entwicklung zu beraten. Diesem Ziel nachgeordnet – aber dennoch von großer Bedeutung – ist die Aufgabe, Beiträge zur öffentlichen Debatte über Wissenschaft und Technik zu liefern.

Unmittelbarer Ansprechpartner und Auftraggeber des TAB ist der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung. Dieser sammelt und koordiniert die Anfragen der Fachausschüsse nach Analysen und Projekten, die das TAB durchführen soll. Aufgrund seiner Entscheidungen kommt letztlich das Arbeitsprogramm des TAB zustande.

Das TAB bearbeitet seine Themen grundsätzlich in enger Kooperation mit externem Sachverstand. Im Rahmen seiner Projekte werden Aufträge an Gutachter zu vom TAB präzise definierten Aufgabenstellungen vergeben. Die Ergebnisse seiner Analysen führt das TAB in einem Bericht zusammen und verantwortet diesen vor dem Deutschen Bundestag.

Zahlreiche Berichte werden als Bundestagsdrucksache veröffentlicht und finden auf diesem Weg Eingang in die Beratungen der Bundestagsausschüsse. Alle Berichte des TAB stehen auch der interessierten Öffentlichkeit kostenlos zur Verfügung. Weitere Informationen zum TAB finden sich unter www.tab.fzk.de.

Der TAB-Sachstandsbericht „Biometrische Identifikationssysteme“ (TAB-Arbeitsbericht Nr. 76, Februar 2002, Verfasser: Thomas Petermann, Arnold Sauter)

Im Herbst 2000 begann das TAB mit ersten Arbeiten zum Thema „Biometrische Identifikationssysteme“ gemäß einem Beschluss aus dem Kreis der Berichterstatter für TA.

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 Be-standsaufnahme 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. Wie bei anderen Themen arbeitete das TAB auch hier mit fachlich ausgewiesenen Personen und Institutionen zusammen. Eine Auswahl aus den Ergebnissen wird im Folgenden skizziert.

Leistungsfähigkeit biometrischer Verfahren

Weltweit sind zahlreiche Systeme in unterschiedlichen Anwendungskontexten, z. B. zur Überprüfung der Handlungsberechtigung von Personen bei E-Banking- und E-Commerce-Transaktionen oder im Rahmen von Zugangskontrollen zu sicherheitsrelevanten Bereichen, in Betrieb. Am häufigsten eingesetzt werden die Erkennung von Fingerbild, Handgeometrie, Gesicht, Stimme, Iris/Retina und Unterschrift/Handschrift, die nach physiologischen, technischen, ökonomischen und Nutzeraspekten beschrieben werden.

Die Leistungsfähigkeit verfügbarer biometrischer Systeme ist auf der Basis der – oftmals äußerst widersprüchlichen – Informationen nicht seriös einzuschätzen. Dies gilt 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. Hier müssen höchste Ansprüche an eine substantiierte 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.

Von besonderem Interesse sind die sog. „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 BioISW-Projekt.

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. Unter den europäischen Ländern gilt Großbritannien als besonders engagiert in öffentlicher und privater FuE. Die EU fördert im aktuellen IST-Programm einige größere Projekte zur Biometrie mit über 10 Mio. €.

Markteinschätzung

Allgemein gilt der Markt für Biometrie als Wachstumsmarkt. Vorliegende ökonomische Daten und Einschätzungen zum Einsatz biometrischer Systeme wirken allerdings häufig sehr punktuell und zufällig. In der Regel sind sie wenig transparent, auf keinen Fall geben sie ein vollständiges Bild. Auch die Daten der amtlichen Statistiken liefern keine Grundlage, um relevante Kennziffern für biometrische Produkte und Dienstleistungen (Produktionsumfang, Umsätze, Beschäftigte u. ä.) zu erhalten.

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.

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.

Datenschutz

Insofern biometrische Verfahren auf persönliche körperliche Merkmale zurückgreifen, sind Fragen des Datenschutzes berührt.

Wichtigste rechtliche Grundlage für die Bewertung von biometrischen Verfahren unter Aspekten des Datenschutzes ist das neugefasste Bundesdatenschutzgesetz (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. Bestimmte Daten in biometrischen Verfahren können einen Informationsgehalt haben, der in diesen besonderen Schutzbereich fällt.

Soweit mit Hilfe 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, bereisspezifische Regelungen erforderlich.

Ob und inwieweit 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 Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung (§ 4 Abs. 2 u. 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, das keine bzw. möglichst wenige personenbezogene Daten erhoben, verarbeitet und genutzt werden (§ 3a BDGS).

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

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. 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 ermöglich: 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 Besetz 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 fortentwikkelt werden sollte.

Neuere rechtliche Entwicklungen

Im Zuge der intensiven Diskussionen um Maßnahmen zur Verbesserung der Sicherheitslage seit dem 11.09.2001 wurde auch der Einsatz biometrischer Verfahren erörtert. Der Gesetzgeber ist hier entsprechend tätig geworden. 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 sollen 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 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.

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 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.

Forschungs- und Handlungsbedarf

Angesichts der wahrscheinlich wachsenden Bedeutung biometrischer Systeme in Wirtschaft und Gesellschaft ist erheblicher Bedarf an Forschung, Information, Diskussion und Aufklärung vorhanden.

Die Verbesserung der Informationslage angesichts der Dynamik der Entwicklung erscheint besonders dringlich. Zur weiteren Abklärung der zukünftigen Entwicklung biometrischer Systeme könnte beispielsweise eine umfassende Technikfolgen-Abschätzung 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.

Augenblickliche Aktivitäten des TAB

Nach einer Diskussion des TAB-Berichtes und der Vorschläge zum weiteren Forschungsbedarf beschloss der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, das TAB mit der Erstellung eines weiteren Sachstandsberichtes zu beauftragen. Dabei wurde zunächst festgelegt, das Thema „Leistungsfähigkeit biometrischer Identifikationssysteme“ zu bearbeiten. Diese Fragestellung sollte konkret für drei Bereiche untersucht werden: Ausweisdokumente, Endgeräte privater Verbraucher und E-Commerce-Anwendungen. Durch die Veröffentlichung im Internet und die gezielte Ansprache wurden Personen und Einrichtungen mit ausgewiesenem Sachverstand für die Erarbeitung von Gutachten zu diesen Themenbereichen gesucht.

Im weiteren Diskussionsprozess und nach Sichtung der eingegangenen Angebote wurde folgende Entscheidung gefällt: a) Die Thematik wurde fokussiert

auf den öffentlichen Bereich (Ausweisdokumente, E-Government-Anwendungen). B) Es wurden zwei parallele Gutachten zur Bearbeitung des Themas an folgende Gutachter vergeben: ZN Vision Technologies AG, Bochum (in Zusammenarbeit mit Bundesdruckerei GmbH, Berlin und Booz Allen und Hamilton GmbH, Düsseldorf) sowie Steinbeis GmbH & Co. KG für Technologietransfer, Unterhaching.

Die Gutachter haben im Oktober mit ihren Arbeiten begonnen. Das TAB wird gemeinsam mit diesen die Arbeitsschwerpunkte, Arbeitsschritte und die Zeitplanung absprechen und überwachen. Die Projektbearbeiter werden ihre eigenen Analysen fortführen und vor allem weitere Expertengespräche führen.

Die Vorlage der Gutachten ist im Februar 2003 vorgesehen, der Sachstandsbericht des TAB ist für Mai 2003 geplant.

Dr. Thomas Petermann

Dr. Arnold Sauter

Stand der gesellschaftspolitischen Diskussion zur Biometrie aus Sicht des Verbraucherschutzes

Michael Bobrowski, Verbraucherzentrale Bundesverband e. V. (vzbv), Berlin

Vorbemerkung

Auf der Grundlage des satzungsgemäßen Auftrags des „Verbraucherzentrale Bundesverband e. V.“, kurz „vzbv“, befasst sich dieser Beitrag zur Rolle der Biometrie im Verbraucheralltag nicht mit den Themen innere Sicherheit oder Terrorismusbekämpfung, sondern beschränkt sich auf die Aspekte des Verbraucherschutzes.

Der Verband

Der „Verbraucherzentrale Bundesverband e. V.“ wurde im November 2000 im Ergebnis einer durchgreifenden Strukturreform der Verbraucherarbeit in Deutschland als neuer Dachverband gegründet. Mitte 2001 wurden die schon seit mehreren Jahrzehnten bestehenden drei öffentlich geförderten Verbraucherorganisationen auf Bundesebene zusammen geführt. Es waren dies die „Arbeitsgemeinschaft der Verbraucherverbände e. V.“, kurz AgV, die „Stiftung Verbraucherinstitut“ und der „Verbraucherschutzverein“. Hauptziel der Strukturreform war es, die auf Bundesebene vorhandenen Kräfte zu bündeln und ein effektiveres Kompetenznetzwerk zwischen dem Dachverband und seinen Landesorganisationen zu schaffen.

Mitglieder des „Verbraucherzentrale Bundesverbandes“ sind die 16 Verbraucherzentralen und eine Reihe weiterer Verbraucher- und verbrauchernaher Verbände.

Der vzbv vertritt die Interessen der Verbraucher in kollektiv-rechtlicher, wirtschaftlicher und politischer Hinsicht. Er koordiniert die verbraucherpolitischen Arbeiten seiner Mitgliedsorganisationen und fördert die Verbraucherinformation.

Zur Themenstellung:

Biometrie in der Verbraucherarbeit

Schon früh haben sich Verbraucherorganisationen, seinerzeit vertreten durch die AGV, im Rahmen ihrer begrenzten Personalkapazitäten mit dem Thema Biometrie und den damit zusammenhängenden Fragestellungen beschäftigt. Einen Anlass boten die zunehmend kritisch bewerteten Schwachstellen beim Einsatz von EC-Karten und die damit verbundenen haftungsrechtlichen Konsequenzen für den Karteninhaber. Ein anderer Anlass ergab sich im Zuge der Beratungen über das deutsche Signaturgesetz und die zugehörige Verordnung. Auch stellt sich die Frage nach dem möglichen Substitutionspotential der Biometrie in Bezug auf wissensbasierte Verfahren beim Einsatz von Signaturkarten.

Nicht zuletzt hieraus entwickelte sich ein intensives Engagement der AgV, vor allem in den Fachgruppen von TeleTrusT und die aktive Mitarbeit im Projekt BioTrusT, für die in der AgV eine eigene Projektstelle eingerichtet wurde.

Die bisherigen Ergebnisse dieses Projektes hat Herr Professor Reimer vorgestellt.

In die zum Teil weiterhin kontrovers geführte Debatte über die Videoüberwachung öffentlicher Räume haben sich die Verbraucherorganisationen nicht eingebracht. Auch haben sie sich aufgrund ihres spezifischen Satzungsauftrages zu Fragen des Biometrieeinsatzes im Zusammenhang mit einer wirksameren Terrorprophylaxe nicht zu geäußert und werden dies auch künftig nicht tun.

Biometrie im Verbraucheralltag

Beim Kauf von Waren oder bei der Nutzung von Dienstleistungen könnten Verbraucher in Zukunft mit biometrischen Verfahren überall dort konfrontiert werden, wo die Überprüfung einer Zugangs- oder der Anspruchsberechtigung erforderlich ist. Dies betrifft den elektronischen Rechts- und Geschäftsverkehr ebenso wie die Verwendung der EC-Karte, die Freischaltung einer Signaturkarte oder den Zugang als Tourist beispielsweise zum Abflugbereich eines Flughafens.

Klare rechtliche Rahmenbedingungen und die richtige Gestaltung der Verfahren vorausgesetzt kann der Einsatz von Biometrie im Verbraucheralltag auch nach Einschätzung der Verbraucherorganisationen zu einer höheren Nutzersicherheit und zu mehr Bequemlichkeit auf Nutzerseite führen. Dabei müssen bei der Konzeption der Verfahren letztere Aspekte gleichrangig betrachtet werden. Je nach Anwendungsfeld, Sicherheitsanforderung und Risikopotential wären bei der Realisierung abgestufte Sicherheitskonzepte vorstellbar.

Eine erste Hilfestellung zur richtigen Gestaltung der Verfahren geben die „Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren“ der TeleTrusT AG 6, der sogenannte „Kriterienkatalog“.

Chancen und Risiken der Biometrie

Entsprechend der Nutzungsdauer wird die Biometrie durch die Anwender kritischer beurteilt. Das ist eines der Ergebnisse des BioTrusT-Projekts. Offenbar treten dabei zunehmend subjektive Befürchtungen in den Vordergrund. Insgesamt werden biometrische Verfahren im Vergleich zu herkömmlichen Techniken der Autorisierung in ihrer Anwendung intimer und persönlicher empfunden.

Grundsätzlich liegen Chancen und Risiken der Biometrie wegen der meist lebenslangen Personengebundenheit bestimmter Körpermerkmale oder Verhaltensmuster nahe beieinander. So können einerseits spezifische Schwächen wissensbasierter Verfahren überwunden werden. Andererseits ergeben sich beim Einsatz von Biometrie neuartige Risiken, die im Persönlichkeitsschutz und im Bereich der Datensicherheit liegen. Daher müssten vor der Anwendung der Biometrie aus unserer Sicht einige wesentliche Grundbedingungen geklärt sein bzw. geregelt werden.

Hierzu gehören:

a) Gesetzliche Rahmenbedingungen und Rechtssicherheit
b) Akzeptanz durch die potentiellen Nutzer und Vertrauensbildung
c) Sicherheit und Datenschutz
d) Nutzerfreundlichkeit unter Praxisbedingungen
e) Sozialverträglichkeit

Gesetzliche Rahmenbedingungen und Rechtssicherheit

In sensiblen verbraucherrelevanten Anwendungsbereichen (Zugangskontrollen, elektronischer Geschäftsverkehr u. ä.) oder dort, wo messbare wirtschaftliche oder rechtliche Risiken mit der Anwendung verbunden sind, wäre der Einsatz biometrischer Identifikationsverfahren ohne gesetzliche Absicherung nicht annehmbar. Vielmehr müssen gesetzliche Rahmenbedingungen für grundlegende Verfahrenselemente und für die datenschutzrechtlichen Auswirkungen geben.

Um die Rechtssicherheit bei der Anwendung biometrischer Verfahren zu erhöhen und das Risiko der neuen Technik nicht einseitig auf den Nutzer abzuwälzen, bedarf es kundenfreundlicher Haftungsregelungen. Dies erscheint um so wichtiger, als es für den tatsächlichen Merkmalsträger bei einer Kompromittierung biometrischer Daten ungleich schwerer wird nachzuweisen, dass eine missbräuchliche Verwendung dieser Daten vorliegt.

Akzeptanz durch die potentiellen Nutzer und Vertrauensbildung

BioTrusT hat gezeigt, dass auf der Anwenderseite ein hohes Informationsbedürfnis besteht. Dies betrifft insbesondere die Funktionsweise des Verfahrens, den Ort der Speicherung der Daten, die Art der Daten und deren Schutz, die Zugriffsberechtigung sowie die Abläufe im jeweiligen Endgerät (Geldautomat, Datenterminal usw.).

Darüber hinaus scheint der Grad der Bedenken in Bezug auf das Missbrauchspotential stark abhängig zu sein von der Vertrauenswürdigkeit des Verfahrensbetreibers. Schließlich ist die Akzeptanzfrage auch eng verknüpft mit der Sicherstellung einer weitreichenden Nutzerfreundlichkeit.

Vor- und Nachteile bestimmter biometrischer Identifikations- oder Erkennungsverfahren für den An-wender müssen je nach Missbrauchspotential differenziert beachtet werden. Die unterschiedlichen Anwendungsfelder (elektronischer Geschäftsverkehr, off-line-Finanzgeschäfte oder die Zugangsfreigabe) sind dabei ebenso wichtige Kriterien wie die Identifikationsmerkmale (Finger, Gesicht, Stimme, Unterschrift usw.) oder die sonstigen Systemparameter Sensorik, Enrolment, Datenverarbeitung und –speicherung, Verfahrenssicherheit, Nutzerfreundlichkeit usw.

Hinsichtlich der Akzeptanz biometrischer Verfahren zeigten sich im BioTrusT-Projekt punktuell Diskrepanzen zwischen der subjektiven Einschätzung von Nutzern und der verbraucherpolitischen Bewertung derselben Verfahren durch die Verbraucherorganisationen. Während viele Nutzer wenig Probleme mit dem Fingerabdruckverfahren hatten, stehen wir diesem Merkmal im Hinblick auf eine alltägliche Verbraucheranwendung eher kritisch bis ablehnend gegenüber. Wir befinden uns in dem Punkt aber mit den Kollegen vom Datenschutz auf derselben Linie. Hauptgründe für unsere Skepsis sind die Allgegenwärtigkeit von Fingerabdrücken und die noch immer nicht gelösten technischen Probleme bei der notwendigen Lebenderkennung. Daher bevorzugen wir solche Verfahren, bei denen der Nutzer einen aktiven Beitrag leisten muss.

Sicherheit und Datenschutz

Biometrische Identifikationsverfahren für sensible Verbraucheranwendungen müssen vor ihrer Markteinführung einer umfassenden Risikoanalyse unterzogen werden. Darüber hinaus ist ein in sich schlüssiges Sicherheitskonzept für die einzelne Anwendung unter strikter Beachtung datenschutzrechtlicher Erfordernisse zu erstellen. Schließlich sollte eine Erprobung in einem begrenzten, aber repräsentativen Anwendungsgebiet erfolgen, bevor ein Verfahren zur praktischen Anwendung freigegeben wird.

Zwar könnten Verbraucherorganisationen angesichts ihrer eingeschränkten Personalkapazitäten nicht an jeder derartigen Risikoanalyse mitwirken. In zentralen, d. h. grundlegenden Fragen zur Biometrie sollten sie jedoch gehört und bei Projekten mit Pilotfunktion einbezogen werden. Schließlich stehen Vertrauen in die Technik bzw. die Akzeptanz durch die Nutzer in direktem Zusammenhang zu den Kriterien Sicherheit und Nutzerfreundlichkeit. Man könnte fast von einem „Dreiecksverhältnis“ zwischen diesen Kriterien sprechen.

Bekanntlich sind nach herrschender Rechtsauffassung biometrische Daten per se personenbezogene Daten. Schon deshalb erfordert eine Anwendung der Biometrie im Verbraucheralltag eine klare gesetzliche Grundlage. Inwieweit bestehende Regelungen ausreichen, werden vor allem die Datenschutzexperten zu prüfen haben. Besonders wichtig ist aus unserer Sicht eine wirksame öffentliche Kontrolle der Einhaltung derartiger Rechtsvorschriften. Ein wichtiges Prüfkriterium wäre die Zweckbindung der Daten. Sie dürfen unseres Erachtens nur zum Zwecke der Erkennung, Identifizierung oder Authentifizierung verwendet werden. Eine zentrale Speicherung personenbeziehbarer biometrischer Daten im Rahmen von Verbraucheranwendungen muss hingegen ausgeschlossen sein.

Last but not least erscheinen die Einrichtung unabhängiger öffentlich kontrollierter Zertifizierungsstellen und die Einführung eines Prüfsiegels für biometrische Verfahren auf der Grundlage interoperabler Standards sinnvoll.

Nutzerfreundlichkeit unter Praxisbedingungen

Biometrische Verfahren bedürfen viel mehr als wissensbasierte Anwendungen der bereitwilligen Kooperation des Anwenders. Auch spielen die Ein-

satzmöglichkeiten und Stabilität der Verfahren unter praxisgerechten Einsatzbedingungen für die Nutzerfreundlichkeit eine entscheidende Rolle. Ein Verzicht auf die aktive Mitwirkung des Anwenders, um dadurch die Handhabung weniger kompliziert zu machen, verbietet sich aus Gründen des Datenschutzes.

Die Nutzerfreundlichkeit eines biometrischen Verfahrens steht aufgrund der Besonderheiten der Biometrie in einem umgekehrten Verhältnis zur Sicherheit. Im Gegensatz zur Ja-Nein-Aussage beim Einsatz einer PIN oder eines Passwortes gibt es bei der Biometrie keine 100%ige Erkennungssicherheit. Da dort die Entscheidung Pro oder Contra nur mit einem per Toleranzfeld einstellbaren Grad von Un-Sicherheit getroffen wird, beeinflusst der Systembetreiber mit der Einstellung der Toleranzschwelle nicht nur die Sicherheit, sondern gleichzeitig auch die Nutzerfreundlichkeit vor Ort. Einen gewissen Ausweg aus dem Dilemma können multimodale Verfahren liefern. Dies sind Verfahren, die durch die Verwendung unterschiedlicher biometrischer Verfahren oder durch die Kombination von PIN und biometrischem Merkmal die Sicherheit erhöhen und zugleich Nutzerfreundlichkeit verbessern.

Sozialverträglichkeit

Es gibt kein für alle Menschen gleich gültiges biometrisches Merkmal. Um dennoch eine breite Akzeptanz in der Verbraucherschaft für die Biometrie zu erreichen, muss ein diskriminierungsfreier Einsatz dieser Technik sichergestellt sein. Kein Verbraucher darf unbegründet durch die Wahl des Verfahrens vom Zugang zu bestimmten Anwendungen ausgeschlossen werden. Das gilt für die Nutzung öffentlicher Dienstleistungen wie für den privaten Geschäftsbereich.

Zusammenfassung und Fazit

Nach Auffassung der Verbraucherverbände bieten biometrische Identifikationsverfahren vom Ansatz her durchaus ein vergleichsweise höheres Maß an Sicherheit als herkömmliche, d. h. wissensbasierte Verfahren. Angesichts der spezifischen Risiken der Biometrie gilt diese positive Einschätzung jedoch nur unter der Voraussetzung, dass für ihre Anwendung eine rechtlich gesicherte Basis geschaffen wird, die auch die Haftungsfragen im Sinne der Anwender neu regelt.

Die Nutzer müssen vor der Anwendung umfassend über die Bedingungen und Folgen des jeweiligen Verfahrens aufgeklärt werden. Dabei geben die Verbraucherverbände solchen Verfahren den Vorzug, die einen aktiven Beitrag des Anwenders verlangen oder mehrere Verfahren kombinieren (multimodale Verfahren). Verfahren, die ausschließlich den Nutzer als passives Verfahrensobjekt einbeziehen, werden bei alleiniger Anwendung von uns eher kritisch betrachtet und i. d. R. abgelehnt.

Vor der Einführung biometrischer Verfahren im Bereich sensibler, d. h. mit erheblichen wirtschaftlichen Risiken verbundenen Verbrauchergeschäften muss eine Akzeptanzuntersuchung vorgeschaltet werden. Nur so kann eine vertrauenswürdige Anwendungsumgebung geschaffen werden, in der ein adäquater Interessenausgleich zwischen den Beteiligten gesichert ist.

Jüngste Meldungen in der Fachpresse über zum Teil schon anderweitig bekannte Schwachstellen biometrischer Verfahren haben das Vertrauen in diese Technik nicht gerade befördert. Um so wichtiger ist es, in der öffentlichen Diskussion hierüber Sachlichkeit und Nüchternheit walten zu lassen. Wenngleich sich die bisherigen Diskussionen weitgehend auf die Fachkreise beschränkt haben, ist schon hier deutlich geworden, dass derart sensible Techniken nur dann auch eine halbwegs realistische Chance beim Verbraucher haben werden, wenn die entscheidenden Kriterien Vertrauenswürdigkeit, Sicherheit und Datenschutz, Nutzerfreundlichkeit und Sozialverträglichkeit hinreichend geklärt sind. Andersfalls ist ein Scheitern programmiert.

Stand der gesellschaftspolitischen Diskussion zur Prävention insbesondere unter dem Aspekt des Datenschutzes

Roland Bachmeier, Direktor beim BUNDESBEAUFTRAGTEN FÜR DEN DATENSCHUTZ

Sehr geehrter Herr Ziercke,
meine Damen und Herren,

als Vertreter des Bundesbeauftragten für den Datenschutz danke ich für die freundliche Einladung und nehme gerne die Gelegenheit zu einem datenschutzrechtlichen Statement in der Auftaktveranstaltung des Arbeitskreises „Kriminalprävention und Biometrie" wahr. Der Bundesbeauftragte für den Datenschutz misst der Prävention und speziell der Kriminalprävention große Bedeutung bei, nicht nur weil dadurch Straftaten verhütet werden, sondern weil die damit verbundenen Maßnahmen in der Regel weniger tief in das Persönlichkeitsrecht der Bürger eingreifen als im repressiven Bereich. Auch bei der Kriminalpräventi-on ist jedoch darauf zu achten, dass nicht unbescholtene Bürger, die also weder Verdächtige noch Störer sind, durch vorbeugende Maßnahmen einer Art Generalverdacht unterzogen werden. Ich freue mich des-halb, dass ich Gelegenheit habe, datenschutzrechtliche Aspekte zum Thema Biometrie vorzutragen.

Wir haben heute von den vielfältigen und bereits realisierten Anwendungsbereichen biometrischer Ver-fahren als Zugangsmedium zu Gebäude- und DV-Systemen gehört. Dennoch fanden diese Methoden, die langfristig die Verwendung von PIN's, SmartCards oder des Passworts obsolet machen, in der breiten Öffentlichkeit bisher keine große Resonanz, wenn man von der Daktyloskopie absieht. Das liegt wohl darin begründet, dass es sich meistens um innerbetriebliche Maßnahmen handelt, die nur einen be-grenzten Kreis von Nutzern betraf. Auch die Einführung biometrischer Verfahren u.a. zur vereinfachten Grenzabfertigung auf Flughäfen, wird bei uns zwar seit langem diskutiert, aber nicht im Wirkbetrieb er-probt, ganz im Gegensatz zu Flughäfen im Ausland. Lediglich am Flughafen Nürnberg ist kürzlich ein auf drei Monate befristeter biometrischer Feldversuch zur Gesichtsfelderkennung von der bayerischen Polizei gestartet worden.

Das Thema „Biometrie" hat sich allerdings mit den Ereignissen vom 11. September 2001 schlagartig zugespitzt.

Denn mit Verabschiedung des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 hat der Gesetzge-ber zum Zweck der Prävention eine grundsätzliche Weichenstellung zur Einführung weiterer biometri-scher Merkmale von Fingern, Händen oder Gesicht in Personaldokumenten und in sonstigen Aufent-haltstiteln getroffen. Darüber hinaus wurde festgelegt, dass solche Merkmale in verschlüsselter Form in das Dokument eingebracht werden. Nähere Einzelheiten zum Verfahren, insbesondere die Art der Merk-male, bleiben einem besonderen Gesetz vorbehalten. Zudem hat der Gesetzgeber, nicht zuletzt auf Drängen der Datenschützer, entschieden, dass eine bundesweite Datei mit biometrischen Referenzdaten zum Zweck der Identifizierung nicht eingerichtet werden darf. Die Einführung biometrischer Merkmale auf den Personaldokumenten war eine der umstrittensten Maßnahmen im Rahmen des Anti-Terror-Paketes II. Ich möchte diese Debatte aber nicht erneut aufnehmen, da die Entscheidung des Gesetzgebers zu respektieren ist; die bundesweite Umsetzung dürfte jedoch noch viel Zeit und Geld erfordern.

Der Bundesbeauftragte für den Datenschutz sieht jedenfalls keinen grundlegenden Gegensatz zwischen biometrischen Verfahren und dem Datenschutz. Im Gegenteil: Der technische Fortschritt ist zu begrüßen, wenn er datenschutzfreundlich ausgestaltet ist. Bei der Einführung und Anwendung biometrischer Verfah-ren müssen deshalb zur Wahrung des Rechts auf informationelle Selbstbestimmung folgende Anforde-rungen erfüllt sein:

Der Einsatz biometrischer Verfahren bedingt die Erhebung und Verarbeitung höchstpersönlicher Daten über körperliche Merkmale. Die Erhebung dieser Daten muss in jedem Fall offen erfolgen, also nicht ohne Wissen des Betroffenen. Das gewählte Verfahren muss unter Berücksichtigung des Zwecks und des Umfangs (Anzahl der Nutzer usw.) möglichst transparent sein. Das Recht auf Auskunft über Art und Umfang der gespeicherten Daten muss gewährleistet sein.

Es dürfen nur diejenigen Daten erfasst werden, die zur Identifizierung bzw. Verifizierung im Rahmen des jeweiligen Verfahrens erforderlich sind. Die erforderlichen Referenzdaten, die nur bei Verifizierungsverfahren erforderlich sind, sollten nicht zentral, sondern dezentral gespeichert werden. Die datenschutz-freundlichste Lösung wäre dabei auch hier die Erfassung auf einem Ident-Träger, den der Betroffene mit sich führt. Damit wäre am besten gewährleistet, dass die Daten nicht missbraucht werden.

In jedem Fall müssen der **Umfang und der Zweck der Nutzung eindeutig festgelegt werden**. Eine Zusammenführung der biometrischen Daten mit anderen Datenbeständen darf nicht erfolgen. Jegliche zweckändernde Nutzung ist nur auf gesetzlicher oder vertraglicher Grundlage zulässig.

Es muss dasjenige biometrische Verfahren gewählt werden, bei dem die Toleranzwerte möglichst niedrig sind. Die **Daten** müssen sich also **möglichst weitgehend eindeutig und fehlerfrei einer bestimmten Person zuordnen** lassen. Je höher der Sicherheitsfaktor des biometrischen Verfahrens ist, je geringer die Fehlerrate ausfällt, desto größer ist die Akzeptanz bei den Benutzern.

Eventuelle **Fehler** bei der Anwendung, z. B. durch Verwechslungen von Personen, müssen durch **Dokumentation nachvollziehbar** sein.

Der Erfolg biometrischer Verfahren ist abhängig vom **Vertrauen der Betroffenen**. Nur wenn diese über Art und Umfang der gespeicherten Daten, des gewählten Verfahrens und der Sicherheit der Methode (keine Verwechslungen!) sowie von der Benutzerfreundlichkeit überzeugt worden sind, werden sie bio-metrische Verfahren akzeptieren.

Der Persönlichkeitsschutz bildet, wenn diese Grundsätze beachtet werden, keinen Gegensatz zum tech-nischen Fortschritt auf dem Gebiet der Biometrie. Soweit neue Methoden der Informationsverarbeitung dem Gebot der Datensparsamkeit oder gar der Datenvermeidung Rechnung tragen, sind sie willkommen und werden von den Bürgern akzeptiert. Vor der bundesweiten Einführung weiterer biometrischer Merk-male auf Personaldokumenten usw. bedarf es jedoch intensiver Feldversuche, um einerseits die si-cherste Methode herauszufinden, die gleichzeitig mit den geringsten Eingriffen in das Persönlichkeits-recht verbunden ist. Der Bundesbeauftragte für den Datenschutz fordert deshalb, dass er rechtzeitig und umfassend in solche Testvorhaben eingebunden wird. Bereits gewonnene Erfahrungen aus bestehenden biometrischen Anwendungen stimmen hoffnungsfroh.