Zeitschrift für Datenrecht und Informationssicherheit

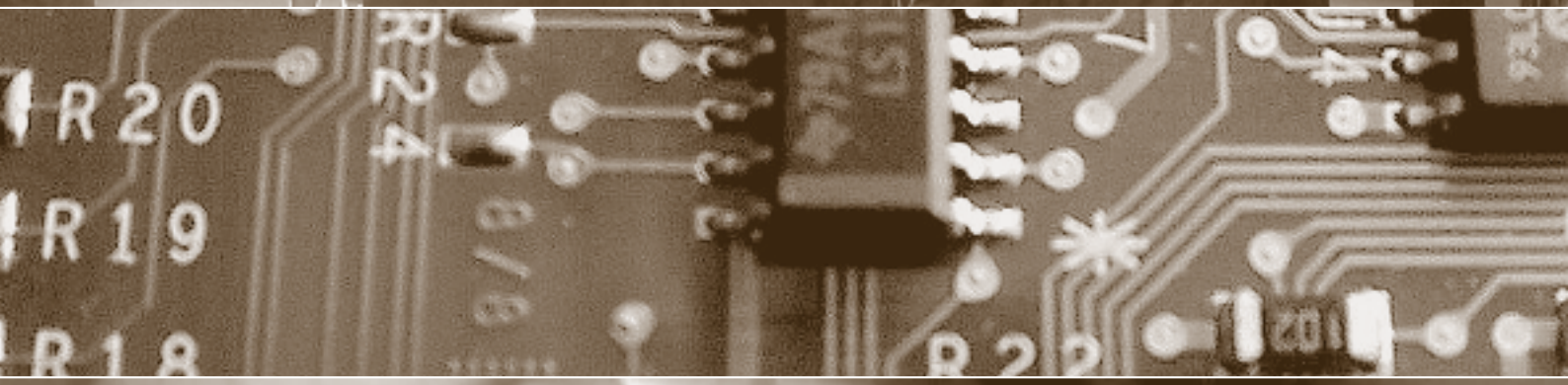
digma

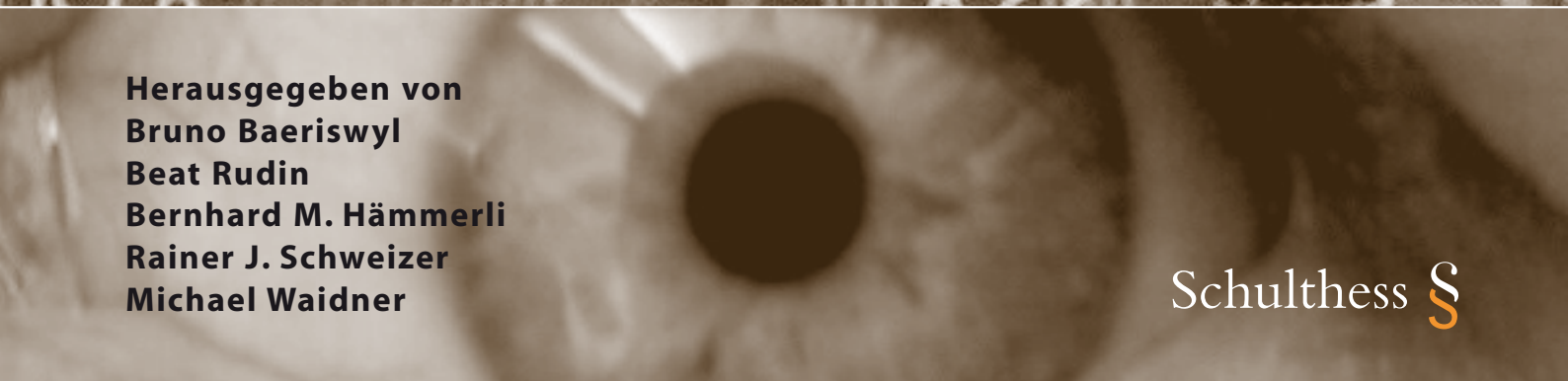
www.digma.info 5. Jahrgang, Heft 4, Dezember 2005

Schwerpunkt:

Biometrie

fokus: Der menschliche Körper als Datenträger
fokus: Die Vermessung des Verbrechermenschen
report: Das «Spam-Urteil» der EDSK





Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Michael Waidner

Schulthess §

fokus

Schwerpunkt:
Biometrie

Der Rechtsstaat auf der Bewährungsprobe

Die Balance zwischen Freiheit und Sicherheit zu finden, mag, zumal in Zeiten terroristischer Angriffe auf den liberalen Rechtsstaat, schwierig sein. Der Gesetzgeber – so mahnt der Nationalratspräsident – darf die Freiheit der Bürgerinnen und Bürger nicht leichtfertig aufs Spiel setzen.

Der menschliche Körper als Datenträger

Was ist neu am «Festmachen von Daten» am Körper? Verändert die Nähe etwas im Verhältnis zum Menschen und seinem Körper? Welche Fragen stellen sich aus philosophischer und ethischer Sicht?

Biometrie – wie einsetzen und wie nicht?

Biometrie wird als Lösung vieler Zugangskontrollprobleme angepriesen. Sie hat aber nicht nur Sicherheitsprobleme, sondern verursacht auch gravierende Sicherheitsprobleme. Was kann Biometrie, was nicht, und welche Gestaltungsaufgaben stellen sich?

Die Vermessung des Verbrechermenschen

Die Entwicklung der Menschenvermessung – von den «Körperlesern» über die «Psychojäger» bis heute – führt von der Makro- zur Mikrokontrolle. Abweichung soll erkannt werden: auf der neurologischen Ebene des Gehirns, im Molekularbereich des Genoms und mit einem feinmaschigen Überwachungsnetz, das die Gesellschaft sanft überzieht.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Michael Waidner

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 155.00, Jahresabo Ausland: Euro 126.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich
Tel. +41 (0)44 383 66 50, Fax +41 (0)44 383 79 45

Druck: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich, ISDN +41 (0)44 383 66 50

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Datenschutzfreundliche Missbrauchsentdeckung

Die Analyse eines Systems bei Missbrauchsverdacht erfordert Audit-Daten, die oft personenbezogene Merkmale enthalten. Eine Analyse ist datenschutzkonform möglich, wenn die Daten so pseudonymisiert werden, dass sie zu vorab definierten Zwecken analysiert werden können und Pseudonyme nur unter vorab spezifizierten Bedingungen aufdeckbar sind.

RFID: Datenschutzprobleme und -lösungen

RFID wird in Bibliotheken oder in der Warenlogistik, aber auch zur Identifikation hochwertiger Güter oder zur Personenidentifizierung eingesetzt. Dadurch entstehen Konflikte mit dem Datenschutz, etwa wegen der Gefahr des unbefugten Auslesens. Wie lässt sich dieses Problem lösen?

Unverlangt zugestellte Werbemails («Spam»)

Die EDSB hält in einem neuen Urteil fest: E-Mail-Adressen – selbst Phantasiebezeichnungen – sind Personendaten. Und wer per E-Mail massenweise und unverlangt Streuwerbung versendet, begeht eine widerrechtliche Persönlichkeitsverletzung.

Wireless LAN – aber sicher

Immer mehr User nützen Wireless LAN, im Büro, zu Hause oder unterwegs. Peter Heinzmann und Andreas Steffen unterhalten sich mit einem Gast über die Risiken des WLAN- Einsatzes.

report

forum

Biometrie – wie einsetzen und wie nicht?

Zum Umgang mit Sicherheitsproblemen von Biometrie und Sicherheits- und Datenschutzproblemen durch Biometrie

Prof. Dr. Andreas Pfitzmann[1], Professor für Datenschutz und Datensicherheit, Technische Universität Dresden, Dresden/Deutschland
pfitza@inf.tu-dresden.de

Biometrie wird als Lösung vieler Zugangskontrollprobleme angepriesen. Was kann sie, was nicht, und welche Gestaltungsaufgaben stellen sich?

Als Biometrie wird das Messen von Körper- oder Verhaltensmerkmalen bezeichnet. Gemessen werden können beispielsweise die *Körpermerkmale*

- Gesicht(sform),
- Temperaturverteilung des Gesichts,
- Fingerabdruck,
- Handgeometrie,
- Muster der Netzhaut,
- Muster der Iris und
- DNS

oder beispielsweise die *Verhaltensmerkmale*

- eigenhändige Unterschrift und
- gesprochener Text.

Unterschieden werden kann danach, ob der Mensch, dessen Körper- oder Verhaltensmerkmale gemessen werden, hierbei explizit mitwirken muss (*aktive* Biometrie), so dass er sich der Messung bewusst ist, oder ob seine explizite Mitwirkung nicht nötig ist (*passive* Biometrie), so dass solch eine Messung ohne seine Kenntnis erfolgen kann.

Wozu Biometrie?

Körper- oder Verhaltensmerkmale werden gemessen, um durch Vergleich mit Referenzwerten Menschen zu

- *authentifizieren* (Ist dies derjenige, der er behauptet zu sein?) oder gar zu
- *identifizieren* (Wer ist das?).

Beides wird umso schwieriger, je grösser die Menge ist, aus der Menschen authentifiziert oder gar identifiziert werden sollen. Besonders im Fall der Identifizierung nimmt die Genauigkeit biometrischer Verfahren mit der Anzahl möglicher Personen stark ab.

Sicherheitsprobleme von Biometrie

Wie bei allen Entscheidungsproblemen kann man auch bei biometrischen Authentifizierungs-/Identifizierungsverfahren zwei Arten von Fehlern beobachten:

- Menschen werden fälschlicherweise abgewiesen bzw. nicht erkannt.
- Menschen werden fälschlicherweise akzeptiert oder falsch identifiziert.

Das Dilemma der biometrischen Mustererkennung ist nun[2]: Macht man den Vergleich auf Ähnlichkeit strenger, dann werden zwar Menschen seltener fälschlicherweise akzeptiert oder falsch identifiziert – es kommt aber auch häufiger zu falschen Abweisungen bzw. Nichterkennen. Macht man den Vergleich lascher, dann werden Menschen zwar seltener fälschlicherweise abgewiesen bzw. nicht erkannt – es kommt aber auch häufiger zu falscher Akzeptanz oder falscher Identifizierung. Die Praxis hat gezeigt: Man kann die Häufigkeit höchstens einer Fehlerart klein bekommen – und dies nur um den Preis, dass die Häufigkeit der anderen steigt.

Ein biometrisches Verfahren ist für eine bestimmte Einsatzumgebung sicherer als ein anderes, wenn dort beide Fehlerarten seltener auftreten.

Zwar kann Biometrie über die Strenge des Vergleichs auf Ähnlichkeit an unterschiedliche Einsatzbereiche in gewissen Grenzen angepasst werden. Aber möchte man auch nur eine der beiden Fehlerraten soweit senken, wie wir dies von gut gemanagten Authentisierungs- bzw. Identifikationssystemen anderer Art kennen, die auf Wissen der Menschen (z.B. Passphrase) oder ihrem Besitz (z.B. Chipkarte) beruhen, haben die heutigen biometrischen Verfahren als andere Fehlerrate jeweils eine unakzeptabel hohe Fehlerrate.

Seit mehr als 20 Jahren wird angekündigt, die biometrische Forschung würde dies in zwei, spätestens vier Jahren ändern. Langsam zweifle ich daran, ob es solch ein biometrisches Verfahren überhaupt gibt, sofern man als zusätzliche Bedingungen die von den Ver-

fechtern der Biometrie versprochene Benutzungsfreundlichkeit sowie akzeptable Kosten trotz vom technischen Fortschritt ebenfalls profitierender Angreifer (s.u.) sieht.

Sicherheitsprobleme durch Biometrie

Biometrie *hat* nicht nur die gerade skizzierten Sicherheitsprobleme, sondern der Einsatz biometrischer Verfahren *verursacht* auch gravierende Sicherheitsprobleme. Beispiele hierfür werde ich im Folgenden darstellen.

Entwertung klassischer forensischer Techniken

Ein verbreiteter Einsatz von Biometrie kann klassische forensische Techniken entwerten, wie dies am Beispiel von Fingerabdrücken als Fahndungs- und Beweismittel skizziert wird:

- Datenbanken mit Fingerabdrücken oder weit verbreitetes qualitativ hochwertiges «Abgeben» des eigenen Fingerabdrucks erleichtern den Nachbau von «Fingern» und damit das Hinterlassen falscher Fingerabdrücke am Tatort erheblich.
- Wenn mittels Fingerabdruck-Biometrie grosse Werte gesichert werden, wird vermutlich eine Fingernachbau-«Industrie» entstehen.
- Da Infrastrukturen z.B. für Grenzkontrollen weniger schnell auf den neuesten Stand gebracht werden können als einzelne Maschinen zum Fingernachbau in den Händen der Angreifer, ist insgesamt ein Sicherheitsverlust zu erwarten.

Diebstahl von Körperteilen (Safety-Problem der Biometrie)

Es ging bereits eine Meldung durch die Presse, nach der dem Fahrer eines S-Klasse Mercedes ein Finger abgeschnitten worden sei, um sein Auto zu stehlen. Unabhängig vom Wahrheitsgehalt der Meldung verdeutlicht sie ein Problem, das ich das Safety-Problem der Biometrie nenne:

- Selbst eine temporäre (oder auch nur vermeintliche) Verbesserung der «Sicherheit» durch Biometrie ist nicht unbedingt ein Fortschritt, sondern gefährdet die körperliche Unversehrtheit ihrer Nutzer.
- Sollte biometrische Lebenderkennung jemals funktionieren, dürfte Entführung oder Erpressung an die Stelle des Diebstahls von Körperteilen treten.

Auch gewünschte Mehrfachidentitäten könnten leichter enttarnbar werden

Der naive Traum mancher Sicherheitspolitiker, Menschen biometrisch eindeutig (wieder)erkennen zu können, wird zum Alptraum, wenn wir nicht verdrängen, dass es in unseren Gesellschaften auch und gerade im Umfeld von Geheimdienst und Polizei akzeptierte und vielfältig nützliche Mehrfachidentitäten für Geheimdienstagenten, verdeckte Ermittler sowie Personen in Zeugenschutzprogrammen gibt und weiterhin geben muss. Die Auswirkungen eines weit verbreiteten Einsatzes von Biometrie wären:

- Um Geheimdienstagenten leichter enttarnen zu können, wird jeder Staat personenbezogene Biometrie-Datenbanken zumindest für alle «fremden» Staatsbürger anlegen.
- Um verdeckte Ermittler und Personen in Zeugenschutzprogrammen leichter enttarnen zu können, wird insbesondere die organisierte Kriminalität personenbezogene Biometrie-Datenbanken anlegen.

Wer also an den Erfolg biometrischer Authentifikation und Identifikation glaubt, sollte sie gerade nicht in den Masseneinsatz im Passwesen führen.

Biometrie hat nicht nur Sicherheitsprobleme, sondern der Einsatz biometrischer Verfahren verursacht auch gravierende Sicherheitsprobleme.

Kurz und bündig

Biometrie wird als Lösung vieler Authentifizierungs- und Identifizierungsprobleme angepriesen. DerArtikel referiert kurz das grundlegende Sicherheitsproblem der Biometrie. In den vergangenen 22 Jahren hat sich trotz anders lautender Ankündigungen an ihm wenig geändert – es wird uns wohl auf Dauer begleiten.

Zusätzlich verursacht Biometrie Sicherheitsprobleme: Beispielsweise werden klassische forensische Techniken entwertet, die körperliche Unversehrtheit riskiert (Safety-Problem) sowie gewünschte Mehrfachidentitäten für Geheimdienstagenten, verdeckte Ermittler und Personen in Zeugenschutzprogrammen gefährdet.

Biometrie verursacht Datenschutzprobleme, da jede biometrische Messung potentiell medizinisch relevante persönliche Daten des Vermessenen enthält, beispielsweise offenbart ein Netzhaut-Scan den Alkoholkonsum der letzten Tage. Zusätzlich können einige Arten biometrischer Messungen erfolgen, ohne dass dies dem Betroffenen bewusst wird, so z.B. bei verdeckter Gesichtserkennung.

Um die möglichen Vorteile von Biometrie, wie bequeme Benutzung bei moderater (Un-)Sicherheit zu nutzen, sollte Biometrie ausschliesslich zwischen Menschen und ihren eigenen Geräten eingesetzt werden. Dies vermeidet, bei geeigneter Implementierung, nahezu alle der genannten Probleme komplett und reduziert die übrigen erheblich.

Datenschutzprobleme durch Biometrie

Biometrie verursacht nicht nur Sicherheitsprobleme, sondern auch Datenschutzprobleme:

- Jede biometrische Messung liefert potentiell sensitive persönliche Daten, z.B. offenbart ein Netzhaut-Scan Daten über den Alkoholkonsum der vergangenen zwei Tage und es wird diskutiert, ob Fingerabdrücke Informationen über die sexuelle Orientierung von Männern liefern[3].
- Bei manchen biometrischen Verfahren (passive Biometrie) ist eine Messung und Auswertung möglich, ohne dass der Betroffene darüber informiert wird, z.B. bei Gesichts(form)erkennung.

In der Praxis werden die Sicherheitsprobleme von Biometrie ihre Datenschutzprobleme eskalieren:

- Die gleichzeitige Erfassung mehrerer biometrischer Merkmale, um die Unsicherheit einzelner Merkmale zu kompensieren, vervielfacht das Datenschutzproblem (vgl. Mosaiktheorie des Datenschutzes).

Zudem sei daran erinnert, dass Datenschutz durch Löschen von Daten in Rechnernetzen normalerweise nicht durchsetzbar ist, da man alle Kopien erwischen müsste. Also muss bereits die Erfassungsmöglichkeit der Daten vermieden werden, sprich die biometrische Messung unterbleiben.

Der naive Traum mancher Sicherheitspolitiker, Menschen biometrisch eindeutig (wieder-)erkennen zu können, wird zum Alptraum.

Wie einsetzen und wie keinesfalls?

Gerade weil Biometrie selbst Sicherheitsprobleme hat sowie zusätzliche Sicherheits- und Datenschutzprobleme verursachen kann, stellt sich die Frage, wie Biometrie eingesetzt werden sollte – und wie sie keinesfalls eingesetzt werden darf.

Zwischen Mensch und seinen Geräten

Selbst biometrische Verfahren, die Menschen häufiger fälschlicherweise akzeptieren, dafür aber selten fälschlicherweise zurückweisen, haben zwischen dem Menschen und seinen persönlichen Geräten ihren Anwendungsplatz, auch dann wenn sie in anderen Konstellationen viel zu unsicher wären oder dort völlig unakzeptable Datenschutzprobleme verursachen würden:

- Authentifizierung durch Besitz und/oder Wissen *und* Biometrie erreicht eine Steigerung der Sicherheit der Authentifizierung.
- Klassische forensische Techniken werden nicht entwertet, da die biometrischen Merkmale nicht die persönlichen Geräte verlassen und Menschen nicht daran gewöhnt werden, ihre biometrischen Merkmale «fremden» Geräten zu geben.
- Es gibt keine Datenschutzprobleme durch Biometrie, da jeder Mensch (hoffentlich) die Kontrolle über seine persönlichen Geräte hat (und behält).
- Zwar bleibt das Safety-Problem der Biometrie zunächst bestehen. Wird aber eine Abschaltmöglichkeit der Biometrie nach erfolgreicher biometrischer Authentifizierung vorgesehen und ist dies allgemein bekannt, dann gefährdet die Biometrie die körperliche Unversehrtheit kaum, sofern ihre Nutzer zur Kooperation mit entschlossenen Angreifern bereit sind.

Wie keinesfalls?

Leider ist zu erwarten, dass auch in anderen Konstellationen versucht wird, Biometrie einzusetzen:

- Aktive Biometrie beim Vorlegen von Pässen und/oder gegenüber «fremden» Geräten kann jedoch vom Betroffenen erkannt werden. Dies sollte ihm helfen, sie zu vermeiden!
- Passive Biometrie durch fremde Geräte ist leider vom Betroffenen nicht erkennbar und darum kaum zu verhindern. Zumindest verdeckt angewandte technisch unterstützte Biometrie sollte unter Strafe gestellt werden.

Was bedeutet dies nun in einer Welt, wo unterschiedliche Staaten mit höchst unterschiedlichen Sicherheitsinteressen (und meistens ohne jede Beachtung der Datenschutzinteressen von Ausländern) Visafreiheit nur gegen Aufnahme maschinenles- und -prüfbarer digitaler Biometriemerkmale bieten?

Visa mit Biometrie oder Reisepässe mit Biometrie?

Visa mit Biometrie sind bezüglich Datenschutz deutlich weniger gefährlich als Reisepässe mit Biometrie.

Fussnoten

[1] Rainer Böhme, Katrin Borcea-Pfitzmann, Rüdiger Dierstein, Marit Hansen und Thomas Kriegelstein danke ich für ein kritisches Lesen dieses Textes und viele konstruktive Verbesserungsvorschläge.

[2] Anil Jain/Lin Hong/Sharath Pankanti 2000.

[3] J. A. Y. Hall/D. Kimura 1994; Valter Forastieri 2002.

[4] Vgl. Unsicherheit der RFID-Chips gegen unautorisiertes Auslesen, <http://dud.inf.tu-dresden.de /literatur/BITKOM2005.06.29Biometrie.pdf> (31.10.2005).

[5] Andreas Pfitzmann 2005.

- Fremde Länder werden versuchen, über Besucher personenbezogene Biometrie-Datenbanken aufzubauen – wir sollten es ihnen weder durch Gewöhnung unserer Bürger an Biometrie erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen.
- Die organisierte Kriminalität wird versuchen, personenbezogene Biometrie-Datenbanken aufzubauen – wir sollten es ihr nicht erleichtern, indem wir das Abgeben biometrischer Merkmale an «fremden» Geräten zur Normalität erklären oder sogar noch durch unkontrollierte Maschinenlesbarkeit unserer Reisepässe unterstützen[4].
- Unterschiedliche Messungen und damit unterschiedliche Werte biometrischer Merkmale eignen sich – da biometrisches Identifizieren bei weitem nicht perfekt funktioniert – weniger als Personenkennzeichen als ein über 10 Jahre konstanter digitaler Referenzwert im Reisepass. Dies gilt natürlich nur, wenn die unterschiedlichen biometrischen Messergebnisse nicht sowieso immer von einem konstanten Personenkennzeichen wie bspw. der Passnummer «begleitet» werden.

Ausblick

Der Einsatz von Biometrie erfordert, wie bei jedem Sicherheitsmechanismus, Umsicht und ggf. Vorsicht. In jedem Fall ist in Demokratien vor dem breiten Einsatz von Biometrie etwa in Reisepässen und Ausweisen eine qualifizierte plurale Debatte nötig. Sie hat bisher höchstens ansatzweise stattgefunden und wird von den Innen- und Sicherheitspolitikern der westlichen Industriestaaten keineswegs gefördert, sondern verweigert oder – wo dies nicht möglich ist – durch unhaltbare Versprechungen oder grob einseitige Problemdarstellungen manipuliert. Dieser Aufsatz zeigt bisher unterschlagene oder gar bisher unbekannte Argumente auf und möchte so einen grundlegenden Beitrag zu einer sowohl qualifizierteren wie auch breiteren Diskussion zum Einsatz von Biometrie leisten.

In einer Güterabwägung zwischen innerer Sicherheit und Datenschutz und der entsprechenden Gestaltungsdiskussion für technische Authentisierungs- und Identifizierungsinfrastrukturen sollte erwogen werden[5]:

- Eine Balancierung zwischen Überwachbarkeit und Datenschutz sollte nicht nur innerhalb einzelner Anwendungen (wie Telefon, E-Mail, Zahlungsverkehr, Überwachungskameras, etc.), sondern über Anwendungen hinweg erfolgen.
- Genomdatenbanken werden möglicherweise die Sicherheit von Biometrie, die ererbte Körpermerkmale misst, untergraben.
- Genomdatenbanken und Ubiquitous Computing (= Pervasive Computing = vernetzte Rechner in allen Dingen) werden einen konsequenten Datenschutz in der physischen Welt weitgehend unmöglich machen.
- Freiräume sind notwendig. Sie sind in der digitalen Welt möglich und sollten deshalb dort geschaffen werden – anstatt mit hohen Kosten unsinnige (im Sinne einer Balancierung über Anwendungen hinweg) Erfassungsmöglichkeiten und Vorratsdatenspeicherung anzustreben. ■

Visa mit Biometrie sind bezüglich Datenschutz deutlich weniger gefährlich als Reisepässe mit Biometrie.

Literatur

- Valter Forastieri, Evidence against a Relationship between Dermatoglyphic Asymmetry and Male Sexual Orientation; Human Biology 74/6 (2002) 861–870.
- J. A. Y. Hall/ D. Kimura: Dermatoglyphic Asymmetry and Sexual Orientation in Men; Behavioral Neuroscience, 108 (1994) 1203–1206. <http://www.sfu.ca/~dkimura/articles/derm.htm> (31.10.2005).
- Anil Jain/ Lin Hong/ Sharath Pankanti, Biometric Identification; Communications of the ACM 43/2 (2000) 91–98.
- Andreas Pfitzmann, Wird Biometrie die IT-Sicherheitsdebatte vor neue Herausforderungen stellen? DuD 29/5 (2005) 286–289.

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 155.00** bzw. bei Zustellung ins Ausland **EUR 126.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §