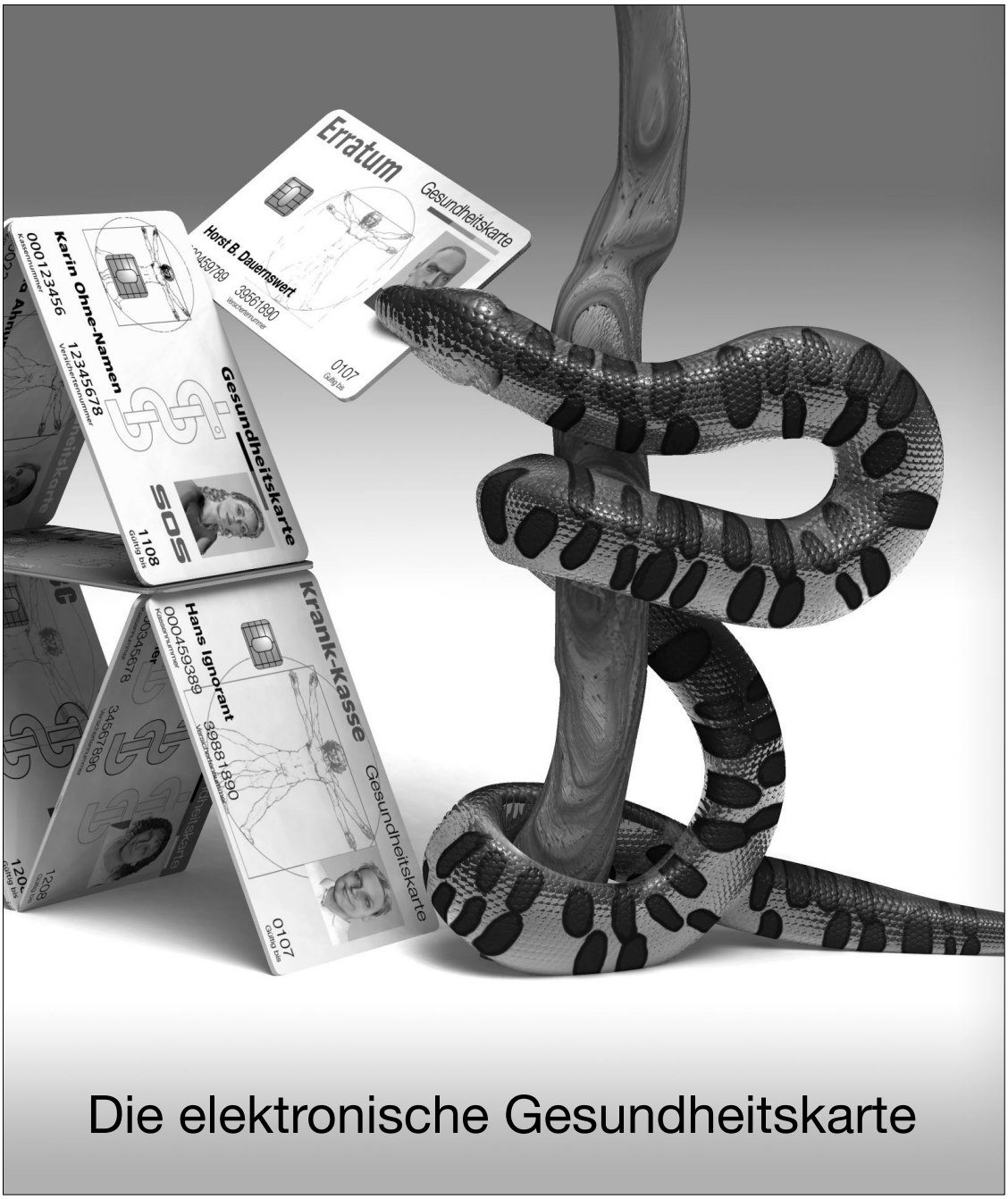
3/2005

Datenschutz Nachrichten

28. Jahrgang
ISSN 0137-7767
9,00 Euro



Die elektronische Gesundheitskarte

Das Labyrinth der elektronischen Gesundheitskarte ■ Produktionsprozesse der Gesundheitskarte ■ ULD-i – Datenschutz als Wettbewerbsvorteil ■ Anonymität einfach und legal mit AN.ON ■ Datenschutznachrichten ■ Technik ■ Gentechnik ■ Rechtsprechung ■ Buchbesprechungen ■ Pressemitteilungen

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Autoren dieser DANA

Hans-Jürgen Burger

Berater für Datenschutz und IT-Sicherheit, Leipheim
Mitglied des Vorstandes der Deutschen Vereinigung für Datenschutz
hans-juergen.burger@datenschutzbuero.net

Kai Janneck

Dipl. Kfm., Innovationszentrum Datenschutz & Datensicherheit (ULD-i)
beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
janneck@datenschutzzentrum.de

Franz-Georg John

Deutscher Genossenschafts-Verlag eG
fgjohn@dgverlag.de

Henry Krasemann

Jurist, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel
Rechtliche Betreuung der Bereiche Identitätsmanagement (Projekte PRIME und FIDIS)
und Anonymität (Projekt AN.ON)
Krasemann@datenschutzzentrum.de

Termine

22.10.2005
DVD-Vorstandssitzung in Bonn
(interessierte DVD-Mitglieder können gerne teilnehmen, bitte in der Geschäftsstelle melden)

23.10.2005 (voraussichtlich)
DVD-Mitgliederversammlung in Bonn

28.10.2005
Verleihung der Big Brother Awards in Bielefeld
www.bigbrotherawards.de

07.11.2005
Redaktionsschluss DANA 4/2005
Big Brother Awards 2005

16.11.-18.11.2005
23. RDV-Forum / 28. DAFTA
Köln, www.datakontext.de

06.02.2005
Redaktionsschluss DANA 1/2006
Europäischer Datenschutz

Nachruf für Ulrich Briefs †

Am 7.6.2005 ist unser langjähriges Mitglied, Prof. Dr. Ulrich Briefs nach schwerer Krankheit gestorben.

Er hat sich über lange Jahre an den verschiedensten Wirkungsstätten für die menschliche und sozialverträgliche Gestaltung von Technik im Arbeitsalltag eingesetzt. Dazu gehörten insbesondere sinnvolle Technikfolgenabschätzung, Mitbestimmungsorganisation und Datenschutzanforderungen im Arbeitsverhältnis.

Nach seiner Arbeit beim Wirtschafts- und Sozialforschungsinstitut des DGB hat er in verschiedenen Positionen hauptsächlich im Wissenschaftsbetrieb gearbeitet. Diverse Lehraufträge und Professuren in Frankreich und den Niederlanden zeugen von seiner ausgeprägten Liebe für diese beiden Nachbarländer, die er uns häufig und in vielerlei Hinsicht als Vorbilder darstellte.

Ulrich Briefs war von 1987-1990 Mitglied der Fraktion Die Grünen im 11. Deutschen Bundestag und wurde in den 12. Deutschen Bundestag über die Liste der PDS gewählt.

In der DVD hat er viele kontroverse, aber gleichzeitig fruchtbare und im Sinne kritischer Solidarität ausgetragene Diskussionen angestoßen.

Wir freuen uns, dass er die DVD zu seinen Lebzeiten als Mitglied über Jahre hinweg begleitet hat.

DANA
Datenschutz Nachrichten
ISSN 0137-7767
28. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Bonner Talweg 33-35, 53113 Bonn,
Fon 0228-222498,
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Rainer Scholl
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0,
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Copyright
Die Urheber- und Vervielfältigungsrechte liegen bei den Autoren. Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gestattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild: Frans Jozef Valenta

Kranke Gesundheitskarte

Die Qualität der medizinischen Behandlung verbessern und gleichzeitig einen Beitrag zur Wirtschaftlichkeit leisten soll die neue elektronische Gesundheitskarte, an der fieberhaft gearbeitet wird. Wann sie endlich einsatzbereit sein wird, scheint niemand wirklich zu wissen. Denn wie eine geeignete technische Infrastruktur aussehen muss, damit alle erhofften positiven Effekte eintreten, darüber scheiden sich die beteiligten Geister. Fairerweise muss man zugeben, dass die Schaffung einer solchen eierlegenden Wollmilchsau wie der elektronischen Gesundheitskarte eben nicht einfach ist. Zu groß sind die Widersprüche, die gelöst werden müssen.

Sicher soll sie sein, aber auch Kosten einsparen. Leider ist IT-Sicherheit immer mit Kosten verbunden; die Absicherung einer Infrastruktur mit Millionen zugriffsberechtigter Menschen und einer Datenspeicherung im Internet und auf Hunderttausenden beteiligten Rechnern erscheint sowieso hoffnungslos angesichts der täglichen Meldungen über erfolgreiche Angriffe auf deutlich kleinere und besser absicherbare Computersysteme.
Durch eine möglichst vollständige und lückenlose Dokumentation sollen Doppeluntersuchungen vermieden und die Arzneimittelsicherheit verbessert werden. Die Selbstbestimmung der Patienten, insbesondere über den Umfang der Datenverarbeitung soll dabei aber noch verstärkt werden.
Mehr Transparenz und Überschaubarkeit wird den Patienten versprochen, dabei werden selbst die Ärzte die komplexe Infrastruktur nicht überblicken können.

Man muss kein notorischer Schwarzmaler sein, um zu erkennen, dass am Ende deutliche Abstriche gemacht und diese vor allem bei der Sicherheit und dem Datenschutz erfolgen werden. Zu groß sind bereits jetzt die Begehrlichkeiten von Krankenkassen, Pharmaindustrie und Strafverfolgungsbehörden.
Forderungen zur Nutzung der Gesundheitsdaten zur Terrorbekämpfung stehen bereits im Raum. Die Gesundheitsdaten sind wertvoll; nicht nur die Pharmaindustrie ist gerne bereit, hohe Beträge dafür zu bezahlen. Dass IT-Sicherheit und Datenschutz absolut kein Thema für öffentliche Auftraggeber sind, wenn ehrgeizige Projekte die Handlungsfähigkeit der Politik unter Beweis stellen sollen, haben bereits die haarsträubenden Vorfälle um Harz IV gezeigt.

Die Bürger wird man bestimmt nicht nach ihrer Meinung fragen.

Rainer Scholl

Inhalt

Hans-Jürgen Burger

Das Labyrinth der elektronischen Gesundheitskarte (eGK)

Lassen Sie uns einen kleinen Ausflug in die Natur machen. Der Herbst kommt auf uns zu und wundersame Pflanzen treiben in letzter Zeit noch aus im Garten Deutschland. Pflanzen mit den Namen Maut, Biometrischer Ausweis, JobCard, Hartz IV-Gesetz und elektronische Gesundheitskarte gedeihen bereits und einzelne Blüten kommen schon zum Vorschein. Durch gute Pflege und Mechanismen zur Überwachung des Wachstums der Pflanzen versucht der Gärtner, das Optimale aus seinen Pflanzen herauszuholen. Ob immer legitim oder mit unerlaubten Düngemitteln sei dahin gestellt. Wichtig ist nur bei all der Pflege, dass das Unkraut nicht außer Acht gelassen wird.

Der zunehmende Wandel im Gesundheitswesen vollzieht sich durch eine neue Pflanze Namens »elektronische Gesundheitskarte«. Diese »elektronische Gesundheitskarte« ist schon ein seltsames Gewächs in unserer technologischen Natur. Sie soll, ähnlich wie Heilkräuter es versprechen, in geringen Dosierungseinheiten zur Genesung des kranken Patienten beitragen. Ob die Behandlungsmethode allerdings wirklich hilft und uns Patienten genesen lässt, das können uns die Ärzte, die uns diese Medizin verschrieben haben, nicht sagen.

Die elektronische Gesundheitskarte (eGK)

Da die elektronische Gesundheitskarte bereits in vielen Fachartikeln ausführlich beschrieben und gewürdigt wurde[1] und es schon Regionen in unserem Lande gibt, in denen die ersten Modellprojekte[2] ihre Gehversuche absolvieren, hoffen wir, dass sich die Versprechen, die uns gegeben wurden, auch alle halten lassen. Hinsichtlich des Datenschutzes würde das ein Mehr an Transparenz bedeuten, die uns helfen kann, die Informations- und Kommunikationsdefizite im Gesundheitswesen zu minimieren. Darum möchte ich hier nicht mehr näher auf die elektronische Gesundheitskarte (eGK) selber eingehen, sondern mich lieber den Nebenwirkungen, den vielen kleinen Trieben und Verästelungen zuwenden. Meist sind es diese, die nicht offensichtlich zu Tage treten und viel später Sorge bereiten. Im Fachjargon des Gärtners nennt man es Unkraut.

Im Garten der Gesundheitstelematik[3]

Die Rahmenbedingungen zum Telematikeinsatz im Gesundheitswesen sind durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG) seit dem 1. Januar 2004 geregelt.

Die Gesundheitstelematik als Labyrinth im Garten wird uns als das all umspannende Netzwerk angeboten, mit dem, wie bereits oben erwähnt, mehr Transparenz erzielt und gleichzeitig Kosten gesenkt werden sollen. Als wunderbaren Nebeneffekt erhofft man sich dabei eine Verbesserung der medizinischen Versorgung.

Wie das allerdings funktionieren soll, konnte bis heute nicht vollständig von der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik mbH) erklärt werden. Diese Institution ist federführend bei der Einführung der elektronischen Gesundheitskarte.[4]

Um so erstaunlicher ist der Web-Auftritt dieser am 11. Januar 2005 gegründeten Gesellschaft.[5] Er ist praktisch nicht vorhanden. Ist dies ein eindeutiges Indiz für Transparenz und Vertrauen, die der Bevölkerung unseres Landes entgegen gebracht werden? Schreibt man eine E-Mail an die Institution, erhält man als Antwort »… ich bitte um Verständnis, dass wir nur gestuft Informationen zu den internen Arbeiten der gematik frei geben …« zurück. Hier liegt noch eine Menge Arbeit vor dem Gärtner, um die Transparenz etwas deutlicher zum Vorschein zu bringen, um das Labyrinth begehbar zu machen.

Da bei der Nutzung telematischer Anwendungen eine Vielzahl von Daten anfallen werden, bringen sich die Beteiligten (Arzt, Apotheker, Krankenhäuser, Personen mit Heilberufen, Krankenkassen, Pharmaindustrie, Versicherungen, etc.) in Stellung, um die Kontrolle über diese Daten zu erlangen und um das Gesundheitssystem entsprechend zu beeinflussen. Diese Art von Lobbyarbeit, die großen Interessenunterschiede zwischen den Beteiligten sowie die noch fehlenden oder unzureichenden Rahmenbedingungen, recht-

[1] www.bundesregierung.de/artikel-413.469273/Elektronische-Gesundheitskarte.htm, www.heise.de, FAZ 13. April 2005, S. 16.

[2] www.bundesaerztekammer.de/30/eArztausweis/30Modellprojekte/index.html.

[3] Das Wort Telematik ist die Zusammensetzung aus den Begriffen Telekommunikation und Informatik. Es bedeutet nichts anderes als die Vernetzung von Datenbeständen auf Rechnern mittels einer Telekommunikationsleitung. Die Telematik selbst besteht aus verschiedenen Informations-Komponenten (Leitlinien, Klassifikationen, Spezifikationen, Datenbanken mit medizinischem Inhalt, wissensbasierte Anwendungen etc.) sowie Kommunikation (elektronische Gesundheitskarte, medizinische Dokumentation, elektronische Patientenakte, elektronisches Rezept, etc.).

[4] www.heise.de/newsticker/meldung/58820.

[5] Die am 11. Januar 2005 in Anwesenheit von Frau Bundesministerin für Gesundheit und Soziale Sicherung Frau Ulla Schmidt in Berlin gegründete Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik mbH) hatte bis einschließlich am 31.7.2005 noch keinen Web-Auftritt. Gesellschafter sind zu je 50 % Leistungserbringer und Kostenträger. http://www.heise.de/newsticker/meldung/58820.

lich wie ökonomisch, haben die Einigung auf konkrete Lösungen doch sehr erschwert. Es wird mit Hochdruck im BMGS[6] daran gearbeitet, die einzelnen Verästelungen im Rahmen der Modellprojekte nicht zu weit aus den Augen zu verlieren. Der Versuch, verbindliche Standards durchzusetzen, gleicht dem Kampf gegen Windmühlen. Dies liegt vor allem daran, dass die Akzeptanz für eine umfangreiche Nutzung telematischer Anwendungen noch nicht bei allen Beteiligten gegeben ist. Die Vorbehalte bezüglich Transparenz und Effizienz des Systems bei Patienten wie auch bei Anwendern müssen noch überzeugend aus dem Weg geräumt werden. Dies bedeutet noch eine Menge Wissenstransfer hinsichtlich der Technik, der Anwendung und des Datenschutzes sowie der rechtlichen Rahmenbedingungen. Eine Pflanze zu düngen ist das Eine, sie erfolgreich zu züchten das Andere.

Viel interessanter noch ist der Aspekt der Nutzung dieser Gesundheitstelematik-Infrastruktur. Seit dem Einzug der jetzigen Krankenversichertenkarte in den Jahren 1993 bis 1994 war der Einzug der EDV in die Arztpraxen, Krankenhäuser, Apotheken und bei den Abrechnungsträgern nicht mehr aufzuhalten. Derzeit sind ca. 80 – 90 % der Arztpraxen mit EDV versorgt. Prima für die Infrastruktur der Gesundheitstelematik, der Grundstock ist gelegt. Ein Problem unter vielen ist hierbei nur, dass mit über 180 durch die KBV[7] zugelassenen Systemen eine sehr heterogene Umgebung existiert. Bei näherer Betrachtung stellt man fest, dass unterschiedlichste Betriebssysteme im Einsatz sind und keine einheitlich geregelte Schnittstelle existiert. Dabei wäre letztere zwingend notwendig, um die Kommunikation für die Vernetzung klar zu definieren.[8]

Durch das Zusammenspiel zahlreicher Anwendungen[9] erlangen die Beteiligten die Kontrolle über Daten (z.B. ausführliche Diagnose, Aufnahmebefund, Einzelheiten über Therapien, Verlauf von Medikamentenbehandlungen,

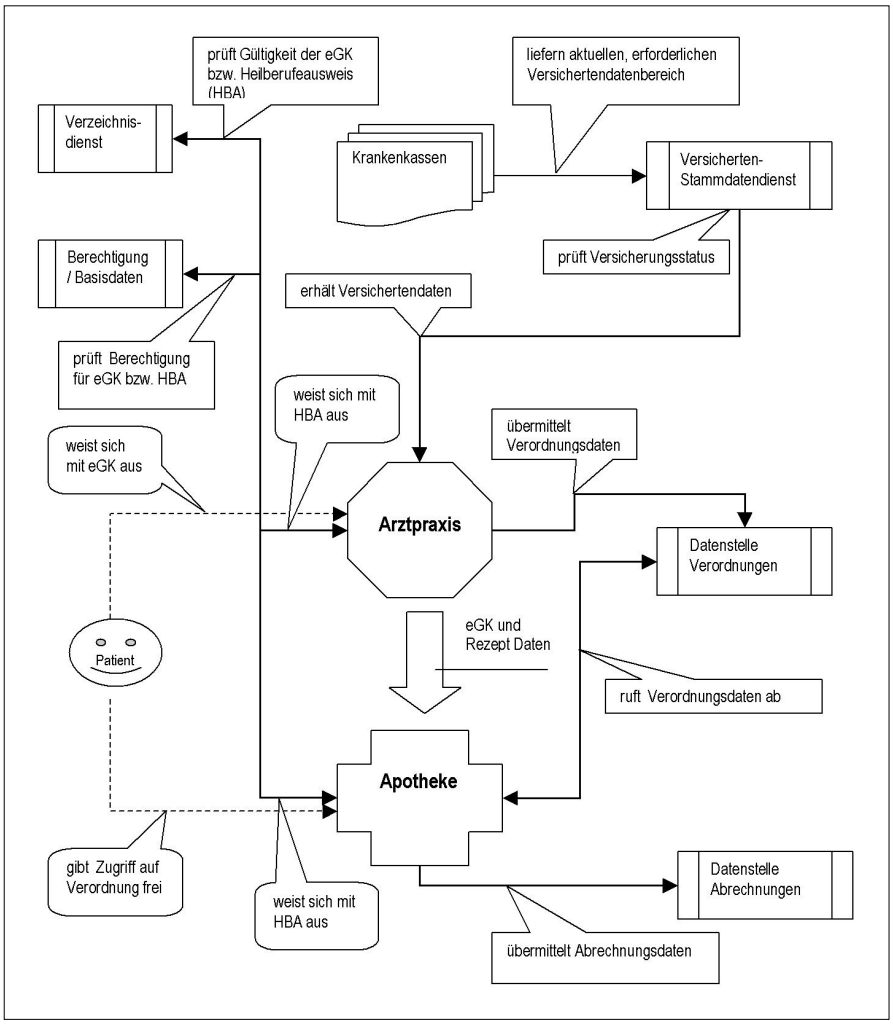


Abb. 1: »eRezept«, Stand 15. Juni 2005 laut Information der gematik mbH

Dosierungen, etc.), von denen sie sich viel versprechen. Prozesse werden angestoßen und Informationen transportiert, ohne dass der Patient je Kenntnis davon erlangt, was mit seinen Daten überhaupt geschieht.

Wir können nur hoffen, dass alles berücksichtigt worden ist, was in solch einer Prozesskette passieren kann.

Am Beispiel der Überprüfungsmechanismen bei der Einlösung des elektronischen Rezeptes »eRezept« wird klar, dass dieser doch sehr kleine Vorgang einen großen Prozess im Hintergrund auslöst (s. Abb. 1). Bereits diese Infrastruktur mit ihren Verästelungen kann im ungünstigsten Fall zu einem Chaos führen.

Was passiert, wenn was passiert? Dümmsten Falls rennt der Patient ohne Medikament wieder aus der Apotheke! Alle Informationen sind vorhanden, aber die Verordnungsdaten sind nicht zugänglich.

MiST ~ Monitoring im Sinne der Transparenz oder Begehrlichkeiten an medizinischen Informationen

Sehen wir uns weiter um und entdecken eine Pflanze Namens »Monitoring«. Die wenigsten Patienten wissen, dass ein Teil der Arztpraxen und Krankenhäuser an Systemen hängt, die Patienten-Informationen gegen Bezahlung an Firmen[10] liefern. Auf den medizinischen Datenschutz[11] der Patienten angesprochen, winden sich die Beteiligten

[6] Bundesministerium für Gesundheit und Soziale Sicherung; www.die-gesunheitsreform.de.

[7] Kassenärztliche Bundesvereinigung, www.kbv.de.

[8] Es gibt eine stattliche Anzahl an Projekten, die im Auftrag der Krankenkassen, der Regierung (BMSG) und sonstiger Interessengruppen durchgeführt wurden, aber kein wirklich durchgreifendes Ergebnis erbracht haben.

[9] Die Anwendungen betreffen jeweils Teilbereiche wie die elektronische Gesundheitskarte, die elektronische Patientenakte, das elektronisches Rezept, die elektronische Krankenakte, den elektronischen Arztbrief, die Rollen von Versicherungsnehmer und der Patienten, das Arzneimittel-Risiko beim Patienten, etc.

[10] Siehe auch www.datenschutzzentrum.de/medizin/artzprax/monitoring. htm.

Vertragsauszug:[1]

1 **Vertragsgegenstand**

1. 1 Gegenstand dieser Vereinbarung ist die Überlassung von anonymisierten praxisbezogenen Daten nach Vorgaben von XYZ (Anlage 1).

1. 2 Der Arzt wird die nach den Vorgaben erforderlichen Daten vollständig registrieren und anonymisiert monatlich innerhalb der ersten fünf Arbeitstage eines Monats auf elektronischem Datenträger (Diskette), per Post oder via Datenfernübertragung an XYZ übersenden. Die Kosten für den Versand trägt der Arzt.

1.3 Der Arzt wird sich ohne gesonderte Vergütung an Arztbefragungen beteiligen und die gestellten Fragen (schriftlich, telefonisch oder per E-Mail) ausreichend beantworten. Diese Befragungen werden maximal zweimal pro Jahr durchgeführt.

3 **Recht an den Daten**

3. 1 Der Arzt räumt XYZ das unwiderrufliche Recht ein, die Daten zu nutzen, zu verwerten und zu verarbeiten sowie Dritten Nutzungsrechte und sonstige Rechte daran einzuräumen.

3. 2 Der Arzt ist berechtigt, die mit Hilfe des gemäß diesem Vertrag genutzten Anwendungsprogramms erstellten Daten für eigene praxisinterne Zwecke auszuwerten. Der Arzt verpflichtet sich, die Daten keinem Dritten zugänglich zu machen.

4 **Vergütung**

4. 1 XYZ vergütet die in dieser Vereinbarung beschriebenen Leistungen monatlich mit € 50,00, sofern die Daten vertragsgemäß erhoben und XYZ zur Verfügung gestellt worden sind. Die Vergütung wird jeweils dreimonatsweise im darauffolgenden Monat ausgezahlt.

5 **Datenschutz**

XYZ verpflichtet sich, die Daten der Praxis zur statistischen Auswertung unter Einhaltung des Bundesdatenschutzgesetzes (BDSG) zu verwenden. Die erhobenen Daten sowie die Informationen über die Mitarbeit der Praxis werden streng vertraulich behandelt. XYZ ergreift alle zumutbaren Maßnahmen, um die Daten vor einem unberechtigten Zugriff Dritter zu schützen.

Anlage 1: **XYZ Datenerhebung**

Folgende Daten werden anonymisiert erhoben:

Praxisstammdaten: Fachrichtung, Praxisform, Anzahl Ärzte, Anzahl Mitarbeiter, technische Ausstattung, fachliche Schwerpunkte, Ortsgröße

Arztstammdaten: Geschlecht, Geburtsjahr, Niederlassungsjahr, Anzahl Klinikjahre

Patientenstammdaten: Patientennummer, Geschlecht, Geburtsjahr, Versichertenart, Kassenart

Diagnosen: Dauer- und Akutdiagnosen

Verordnungen: alle Verordnungen
- mit Zuordnung der Diagnosen
- ggf. mit Dosierungsangabe
- Therapiewechsel, Therapieabbruch mit Erläuterungen
- Musterabgaben

Risikofaktoren: Größe, Gewicht, Adipositas, Raucher, Blutdruckwerte

Laborwerte: alle dokumentierten Laborwerte

Sonstige Daten zur Behandlung und Therapie:

Nach Vorgabe von XYZ (Überweisungen, Krankmeldungen, Krankenhauseinweisungen, Leistungsziffern). XYZ ist berechtigt, diese Vorgaben zu erweitern oder zu ändern.

[1] Die Originale liegen vor.

Abb. 2: Vertrag über den Verkauf von Patientendaten durch den Arzt

meist mit fadenscheinigen Argumenten heraus. »Unsere Patienten unterschreiben eine Einwilligung zur Verarbeitung ihrer Daten« ist die Standardantwort.

Informiert der Arzt den Patienten ausreichend oder handelt es sich womöglich um eine uninformierte Einwilligung?

Die Aufklärungspflicht in Bezug auf den Datenschutz, z.B. wohin die Patientendaten geliefert werden, welchen Informationsinhalt die Daten tatsächlich haben, wie sie verarbeitet werden und wer noch alles darauf zugreifen kann, hierüber herrscht großes Schweigen! Diese Informationen und die entsprechenden Detailangaben werden dem Patienten schlicht vorenthalten. Aufklärung? Fehlanzeige!

Hier herrscht Handlungsbedarf! Das Bundesdatenschutzgesetz sieht mit dem § 39 „Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen“ (Arztgeheimnis) einen Schutz für Patienten vor. Doch prüfende Blicke würden nicht schaden.[12]

Somit stellt sich die Frage: Kann der Patient dem Arzt noch vertrauen oder ist der Arzt bereits Gehilfe eines Systems, dem er sich gar nicht mehr entziehen kann?[13]

Die Unternehmen, die diese medizinischen Patienten-Daten erhalten und verarbeiten sind bekannt, ihre Zahl ist überschaubar. Sie gehören meistens international tätigen Konzernen[14] an. In der Regel werden die gesammelten Patientendaten in Rechenzentren im Ausland verarbeitet, ohne Wissen des Patienten. Ab diesem Zeitpunkt haben wir keinerlei Kontrolle mehr darüber, was mit den Patientendaten tatsächlich passiert.

Oft arbeiten diese Unternehmen in rechtlichen Grauzonen und versuchen, sich durch fragwürdige Verträge eine Legitimierung zu verschaffen.

Ein vorliegender Vertrag, der zwischen der Firma und dem Arzt geschlossen werden soll, dokumentiert die fraglichen Datenübermittlungen und -verwendungen (s. Abb. 2).

Punkt 3.1 im Vertragswerk gibt der Käufer-Firma einen Freibrief, nach Belieben mit den Daten zu verfahren. Es

[11] Holger Koch, Medizinischer Datenschutz – in der Praxis ein Fremdwort, in: Datenschutz-Berater DSB 2/2005, S. 15.

[12] § 39 Abs. 2 BDSG: »Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonders Gesetz zugelassen ist«.

[13] Rainer Scholl, Das Hausarzt-Spar-Modell der Barmer, in: DANA 2/2005, S. 28 ff.

[14] www.imshealth.de, einer der führenden Anbieter im Bereich Gesundheitsmonitoring wurde im Monat Juli 2005 von einem Holländischen Unternehmen aufgekauft. www.imshealth.de/media/15/VNU_IMS.PDF.

handelt sich aber um personenbezogene Patientendaten und deshalb hat nur der Patient das Recht, darüber zu verfügen.[15] Doch leider wird er nie erfahren, was in solchen Verträgen über ihn alles abgeschlossen wird.

Gräbt man nun etwas tiefer in den Boden und versucht, an die Wurzel der Pflanzen zu gelangen, stößt man doch auf einigen Widerstand. Auf das Thema Anonymisierung angesprochen, versichert einem diese Firma, dass sie den »höchst möglichen Standard« erfüllt. Angesprochen auf Zertifizierung wird dankend abgewinkt.

Wie schnell eine scheinbare Anonymisierung aufgehoben oder rückgängig gemacht werden kann, dazu gibt es bereits Vorlesungen an Hochschulen und einschlägige Informationen aus dem Internet.

Begründet wird das Monitoring von den Unternehmen, wie bereits oben erwähnt, mit den Schlagworten der Transparenz, der Kostenminimierung im Krankenkassenumfeld und natürlich »nur« zum Nutzen des Patienten. In Wirklichkeit kann das Monitoring zu ganz anderen Zwecken herangezogen werden, wie sich aus dem Vertrag unschwer erkennen lässt.

Anhand der Informationen, die diese Firmen bereits über Patienten, Ärzte und Krankenhäuser in ihren Datenbanken gesammelt haben, lassen sich vielfältige Auswertungen vornehmen. Auswertbare Verordnungsmerkmale sind z.B. Zugehörigkeit zu GKV oder PKV, Facharztgruppen, Hersteller der Medikamente, Herstellerhistorie, Konzern, Pharmazentralnummer, Produkte, Substanzen (inkl. Wirkstoffkombinationen), Packungsgrößen, Dosierstärke, Original/Generika, Festbetrag, Patientenalter, Risikofaktoren, Abgabebestimmung etc. Die Liste lässt sich um ein Vielfaches erweitern. Hiermit soll verdeutlicht werden, dass bereits im heutigen Stadium genügend Informationen vorliegen, die bestimmt nicht alle zweckgebunden erhoben und verarbeitet werden, so wie es im Bundesdatenschutzgesetz und im SGB V – Gesetzliche Krankenversicherung[16] vorgesehen ist. Diese Auswertungen werden der Pharma-Industrie und deren Institutionen verkauft. Natürlich erhält der Arzt ebenfalls eine Auswertung, um seine Verschreibungsquote und seine Verordnungsentscheidung dem Trend anpassen zu können.

Da durch die Reform im Gesundheitswesen noch mehr Patienteninformationen hinzukommen werden, wird sich die Lage für den Patienten nicht unbedingt zum Vorteil wenden. Der Patient mit seinen Daten wird dadurch immer gläserner und die große Gefahr besteht darin, dass all diese Informationen missbräuchlich verwendet werden können, ohne dass der Patient davon in Kenntnis gesetzt wird.

Patientenprofile (Tracking) – die Gefahr der Bewegung im Garten der Gesundheitsreform

Heutzutage ist es ein Leichtes, den Weg eines aufgegebenen Paketes mittels EDV vollständig zu verfolgen. Neudeutsch nennt man dies »tracking«. Durch das Anlegen von Bewegungsprofilen lässt sich der zurückgelegte Weg des Paketes genau nachvollziehen.

Mit dem Einsatz der eGK hinterlässt auch jeder Patient eindeutige Spuren auf den unterschiedlichsten Rechnern mit Chipkartenlesegerät und an den unterschiedlichsten Orten im Gesundheitssystem. Somit können bald problemlos Bewegungsprofile über Patienten erstellt werden, da die Informationen mit Ausgabe der eGK und dem Start des elektronischen Rezeptes in Kürze an unterschiedlichen Behandlungseinrichtungen (alle Heilberufe, Arzt, Apotheken, Krankenhäusern, Reha-Kliniken usw.) vorhanden sein werden.

Zu Beginn der Gesundheitsreform steht nur das „elektronische Rezept" gespeichert auf der eGK zur Verfügung. Beispiel: Wann und in welcher Apotheke es eingelöst worden ist. Auch die Information, welches Medikament verordnet wurde und welcher Arzt uns das Rezept ausgestellt hat, kann in Zukunft eingesehen werden. Natürlich nur, wenn wir als Patient einwilligen (SGB V § 291a Abs. 6). Doch haben wir, die die Zustimmung gegeben haben, auch das Recht erworben, die Infrastruktur zu kontrollieren?

In Anbetracht der Tatsache, dass das Gesundheitssystem erst am Anfang steht, mutet die weitere Entwicklung beängstigend an. Die Gefahr besteht darin, dass diese Patientendaten in die zukünftige elektronische Patientenakte mit einfließen werden. Zur Zeit befindet sich immer noch ein Großteil der Patientendaten in Akten, schriftlich festgehalten und an einem einigermaßen geschützten Platz in der Arztpraxis. Da diese Daten in näherer Zukunft auf Rechnern digitalisiert zur Verfügung stehen werden, wird es auch möglich sein, mit der dazu passenden Software ein Patientenbewegungsprofil bis ins Detail zu erstellen. Patientendatensammelstellen (alle Heilberufe, Arzt, Apotheken, Krankenhäusern, Reha-Kliniken usw.) im Gesundheitswesen wird es ja zur Genüge geben, da sie bereits vorhanden sind. Der Patient als Datenquelle digital angezapft, das ist die Möglichkeit der all umfassenden Vorsorge und Transparenz oder anders ausgedrückt, Telemedizin á la Toll Collect.

Verknüpft man nun diese Informationen mit den bereits vorhandenen in der Privatwirtschaft, so tritt der Patient – ohne es zu wissen – in das Labyrinth ein. Ab diesem Zeitpunkt ist er dem (Gesundheits)System völlig schutzlos ausgesetzt. Jede einzelne Spur, die dann hinterlassen wird, wird protokolliert und kann auch entsprechend ausgewertet werden.

Zu viele Patienten-Informationen werden bald auf Rechnern digitalisiert zur Verarbeitung bereitliegen. Die Wirtschaft bezahlt solche Informationen vorzüglich, die Begehrlichkeit an den Daten wird steigen. Die Möglichkeiten der Datenauswertung werden grenzenlos sein und die vollständige Beobachtung eines Patienten (wo er sich gerade befindet und wie sein Gesundheitszustand ist) ist nicht mehr nur fiktiv. Werden wir in näherer Zukunft Schnupfenmedikament-Rabatte von verschiedenen Pharmakonzernen in unserem Briefkasten vorfinden?

Das Labyrinth werden wir Patienten nie durchschauen, geschweige denn die Vielzahl an Informationen, die über uns gespeichert sind, je überblicken. Hier ist der Gesetzgeber aufgefordert uns zu schützen. Er sollte klare Regelungen zur Benutzung und Sicherung der sensiblen Patientendaten definieren!

Dass die Methode des Trackings bei der Verbrechensbekämpfung im Bereich des Mobilfunks, z.B. bei einer Täterverfolgung angewandt wird und jetzt bereits auf die LKW–Maut ausgedehnt wird, mag als legitim angesehen werden. Was passiert aber, wenn man die Patientendaten zu strafrechtlichen Ermittlungen heranzieht? Wo gelangen wir dann hin, wo sind die Grenzen? Besteht die Gefahr, dass technische

[15] SGB V, 10. Kapitel, Erster Abschnitt; Informationsgrundlagen.

[16] www.bmgs.bund.de/download/gesetze_web/sgb05/sgb05x291a.htm.

Kontrollsysteme und eine Überwachungsstruktur aufgebaut werden?

Manches in der Gesundheitsreform ist eine Frage der Sichtweise. Guck mal, wer da guckt und guck mal, wer da mitguckt.

Medizinisches Scoring oder Standardisierung der Patienten?

Wird das Scoring[17] von Patienten kommen? Viele Bundesbürger werden bereits ohne es zu wissen anhand der Informationen, die schon erfasst und bekannt sind, benotet. Wer heute ein Auto oder eine Wohnung finanzieren will, wird unweigerlich mittels bereits bekannter Techniken klassifiziert. An die Daten kommt in der Zwischenzeit jeder, der bereit ist, dafür zu zahlen. Einschlägig bekannte Unternehmen[18] stellen Informationen wie z.B. Telefondaten, Schuldnerlisten, Konten, Kontowarnungen, Kredite, Finanzierungsart, Zahlungsstatus, Geodaten mit Haustyp, Familienstruktur, Altersstruktur bis hin zum Kaufkraft-Index zu Verfügung. Da das Scoring-Verfahren bereits in einem stattlichen Umfang quer durch alle Branchen zum Einsatz kommt, stellt sich unweigerlich die Frage: Wann gibt es so etwas im Gesundheitsumfeld?

Die bereits bekannten Informationen lassen sich wunderbar mit Behandlungsdaten erweitern und dann bewerten. Jeder Arzt- oder Krankenhaus-Fragebogen, den ein Patient ausfüllt, kann in ein Bewertungssystem mit einfließen. Die Verknüpfung stellt dann keine große Herausforderung mehr dar. Der Patient selbst wird von den Scoring-Verfahren kaum etwas wahrnehmen, denn oft sind die Hinweise darauf nur sehr vage.

Es besteht durchaus auch die Möglichkeit, dass in Zukunft Gesundheitsdaten Einfluss auf die Kreditvergabe oder den Kauf eines Autos haben können. Der Kunde wird abgewiesen, da er zu häufig erkrankt ist. Womöglich wird der Kunde bei der privaten Altersvorsorge schlechter eingestuft. Vielleicht gewährt aber ein Unternehmen der Konsumgüterindustrie der Person einen Ratenkredit mit besonders schlechten Konditionen. Das Unternehmen verfügt über die Möglichkeit, den Score zur Bewertung der Person heranzuziehen.

Werden Szenarien dieser Art auf uns zukommen? Zwar setzt der Datenschutz[19] Grenzen bei der automatisierten Einzelentscheidung, aber die Fragen die sich hierbei stellen, lauten: Wird der Patient informiert? Welche Möglichkeit der Kontrolle hat er beim Scoring? Was passiert genau bei der Ablehnung eines Kreditantrags aufgrund eines Krankheitsmerkmals? Wird der Patient anhand von Krankheitsmerkmalen tatsächlich bewertet?

Unsere Gesundheitsreform

Vorschläge, Fachspezifikationen, Experten aus Forschung und Wissenschaft, Interessenverbände, Fachgesellschaften, Vertreter von Selbstverwaltungsorganisationen im Gesundheitswesen, Betreibergesellschaften, Krankenkassen und deren Verbände, Ärzte und deren Verbände – um nur einige zu nennen – wollen uns den Segen der Gesundheitsreform einschließlich der elektronischen Gesundheitskarte bringen. Allein die stattliche Anzahl von Struktur-Vorschlägen der oben genannten Interessenten stellt ein Problem dar. Jedem kann man es nicht Recht machen.

Hier gilt das alte Sprichwort »zu viele Köche verderben den Brei«. Oft weiß man anhand der vielen Meldungen, angefangen bei Tageszeitungen bis hin zu Internetportalen, nicht, was wirklich gilt und wie der Stand zurzeit aussieht.

Die Patientenbeteiligung ist in allen Phasen der medizinischen Datenerhebung zwingend erforderlich, erfolgt in der Realität aber nicht!

Fazit

Zurück zur Natur, die uns ein Stück weit begleitet hat und von der der Mensch noch viel lernen kann. [20]

Wir sitzen bereits im Netzwerk der Gesundheitsreform, dem Labyrinth der Demokratie, fühlen uns sicher und vertrauen darauf, dass unser Wohl als Patient bei der Gesundheitsreform im Mittelpunkt steht. Dabei übersehen wir aber gleichzeitig die Gefahr, die von so einem Netzwerk ausgehen kann. Datensparsamkeit und Zweckbindung im medizinischen Umfeld sind nicht gegeben und dies gefährdet uns als Patient und Bürger einer freien Demokratie zunehmend. Wir können nicht mehr entscheiden, wem wir welche Daten geben, sondern nur die Möglichkeit auswählen, wie wir zustimmen.

Zu Guter Letzt

Der Verfassungszeitraum des Artikels liegt in den Monaten Juni bis Juli 2005. Allein in den letzten beiden Wochen des Monats Juli 2005 haben sich durch die vorgezogene Bundestagswahl einige Änderungen ergeben. Durch die Verzögerung[21] des gesamten Projektes kann mit einer schnellen Umsetzung und der einhergehenden Ausgabe der elektronischen Gesundheitskarte zum 01.01.2006 nicht mehr gerechnet werden. Bis zum 31.07.2005 gab es noch keine konkrete Aussage, welches Betriebssystem die Gesundheitskarte erhalten soll.

Links:

www.die-gesundheitsreform.de
www.die-gesundheitsreform.de/zukunft_entwickeln/elektronische_gesundheitskarte/
www.bmgs.bund.de
www.dimdi.de
www.uld-i.de/themen/gesundheitskarte/
www.datenschutzzentrum.de/medizin/gesundheitskarte/
www.innovations-report.de/html/berichte/studien/bericht-46242.html

[17] Score bedeutet zu deutsch: Auswertung oder Note.

[18] Die Schufa (www.schufa.de) dürfte jedem bekannt sein, der ein Bankkonto eröffnet hat. Alleine die Schober Information Group (www.schober.de) biete bereits heute 400 unterschiedliche Klassifizierungsmerkmale an, und das für über 90 % der Haushalte in Deutschland. Die www.ceg-plus.de bietet detaillierte Informationen für die Kreditvergabe an.

[19] BDSG § 6a: »Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.«

[20] Bereits seit 2001 wird daran gearbeitet, www.innovations-report.de/html/berichte/medizin_gesundheit/bericht-4269.html, www.heise.de/newsticker/meldung/61654 www.stnetwork.de/node/413, www.heise.de/newsticker/meldung/58750.

[21] www.heise.de/newsticker/meldung/61920.

Franz-Georg John

Beschreibung der Prozesse zur Produktion der elektronischen Gesundheitskarte aus produktionstechnischer Sicht

In dem anschließenden Beitrag stütze ich mich im Wesentlichen auf die Ausführungen in der bestehenden Lösungsarchitektur in der Version 1.0 vom 14.03.2005, welche in diesem Jahr zur Umsetzung an Frau Ulla Schmidt im Rahmen einer feierlichen Veranstaltung auf der CeBIT übergeben wurde.[1]

Für die in der Lösungsarchitektur beschriebenen Abläufe werden zur Zeit durch die gematik mbH die entsprechenden Spezifikationen für alle geforderten Komponenten erstellt. Auf Basis dieser Spezifikationen können die Krankenkassen Ausschreibungen gestalten und diese auf bekannten Wegen veröffentlichen.

Worin besteht hierbei für die Krankenkassen die Herausforderung ?

1. Vervielfachung der zu verarbeitenden Prozesse

In der Abbildung 1 sind die Daten der bestehenden Krankenversichertenkarte (KVK) den Daten der neuen eGK gegenübergestellt. Diese sind in den §§ 291 und 291 a SGB V manifestiert und müssen so verbindlich übernommen werden. Das Thema »Lichtbild« wird hier seitens des BMGS als ein zusätzliches Sicherheitsmerkmal betrachtet. Die praktischen Erfahrungen haben in Pilotversuchen, bei denen heute KVKs mit Lichtbild eingesetzt werden, jedoch gezeigt, dass es heute ohne Probleme möglich ist, von Ärzten behandelt zu werden, obwohl keinerlei Übereinstimmung mit dem Lichtbild erkennbar ist. Auf Nachfrage bei den Ärzten argumentierten diese, dass sie in erster Linie Arzt und nicht die Polizei der Krankenversicherungen sind. Anschließende Versuche, die Anforderung an ein Lichtbild auf der eGK wieder zu verwerfen, sind gescheitert. Dass der Prozess der Lichtbildbeschaffung und deren zweckgebundenen Verwaltung zu erheblichen Mehrkosten führt, muss an dieser Stelle nicht weiter ausgeführt werden.

[1] Da zwischen dem Zeitpunkt der Erstellung dieses Artikels und der Artikelveröffentlichung einige Zeit verstrichen ist, kann es zwischendurch zu Veränderungen an den hier zugrunde gelegten Rahmenbedingungen gekommen sein. Diese Veränderungen können sich auch nachhaltig auf die hier beschriebenen Prozesse auswirken.

2. Herkunft der eGK-Daten

In der geplanten Struktur werden folgende Datenlieferanten zur eGK definiert:

2.1. Krankenversicherer

Der Krankenversicherer ist der Vertragsnehmer zum Patienten. Der Krankenversicherer hat die bekannten Stammdaten des Versicherten. Diese Daten werden »Versichertenstammdaten« oder auch »VSD« bezeichnet. Diese Daten werden heute bei den Krankenkassen entweder auf eigenen EDV-Anlagen verwaltet oder es werden externe Rechenzentren mit der Verwaltung beauftragt.

2.2. Versichertenstammdatendienst

Die o.g. Versichertenstammdaten können einer Instanz namens »Versichertenstammdatendienst« auch »VSDD« genannt, zur Verwaltung übergeben werden. Selbstverständlich kann die Krankenversicherung diese Funktion eigenständig übernehmen oder eben auch an externe Rechenzentren übergeben.

2.3. Bilddatendienst

Die Lichtbilder der Versicherten werden vom so genannten »Bilddatendienst« im Auftrag des Krankenversicherers erfasst und verwaltet. Selbstverständlich kann auch hier diese Funktion von der Versicherung in Eigenregie übernommen werden. Falls aber die bestehenden Ressourcen und Anforderungen an das eigene Callcenter nicht ausreichen um die Bildmengen in der geforderten Qualität zu verarbeiten, muss auch hier die Hinzunahme von externen Dienstleistern in Erwägung gezogen werden.

2.3. Anwendungsanbieter

Die eGK ist technisch so vorbereitet, dass diese während ihrer Nutzungsphase im Feld mit weiteren Anwendungen nachgeladen werden kann. Ob eine Anwendung nachgeladen werden soll oder auch nicht, obliegt der Entscheidung des Versicherten. Damit bei einer Neu- oder auch Nachproduktion der Patient die Karte mit den identischen Funktionen wieder in seine Hände bekommt, müssen die für ihn verwendeten Anwendungen bei einem »Anwendungsanbieter« gespeichert werden.

2.4. Kartenverwalter

Der Kartenverwalter übernimmt eine der wesentlichsten Aufgaben in dem neuen System. Er verwaltet die eGK von ihrer Herstellung und Ausgabe über die komplette Nutzungsphase bis hin zum Einzug oder Ablauf der eGK. Der Gesetzgeber erlaubt, dass ein Kartenverwalter seine Tätigkeit mehreren Krankenversicherungen anbieten darf. Aber auch diese Funktion kann selbstverständlich von den Versicherern in eigener Verantwortung übernommen werden.

2.5 Kartenverwaltung (im engeren Sinne)

Unter der Kartenverwaltung im engeren Sinne versteht man das Verwal-

Vergleich der Daten der alten Krankenversichertenkarte mit der der neuen elektronischen Gesundheitskarte

Alt	Zusätzlich neu
Stammdaten: Identifikation	
Name Geburtsdatum Anschrift Unterschrift	Geschlechtsangabe Lichtbild (ab 15. Lebensjahr)
Stammdaten: Verwaltungsdaten	
Ausstellende Krankenversicherung Versichertenstatus Ablaufdatum Versicherungsschutz	Einheitliche Krankenversichertennummer Zuständige Kassenärztliche Vereinigung Zuzahlungsstatus Tag des Beginns der Versicherung Dokumentation für die Einwilligung Löschung einzelner Daten Einzug der Karte Daten über Leistungen bzw. vorläufige Kosten Behandlung im europäischen Ausland (E-111)
Medizinische Daten	
	Elektronischer Arztbrief Angaben zur elektr. Patientenakte Notfalldaten Arzneimitteldokumentation Freiwillige Daten des Patienten Elektronisches Rezept
Sicherheit	
	Verschlüsselung Authentifizierung Digitale Signatur Auslesungsbeschränkung auf bestimmte Nutzer Protokollierung der letzten 50 Zugriffe auf die eGK

Quelle: BMGS; §291 SGB V

Abbildung 1

tungssystem, welches sich um die klassische Verwaltung der Karteninhalte kümmert. Zur Produktion einer eGK müssen dem Kartenverwalter die Versichertenstammdaten vom VSDD und die Bilddaten zur Verfügung gestellt werden.

Erst wenn diese Daten um die Anwendungen ergänzt beim Kartenverwalter vorhanden sind, kann dieser einen Kartenhersteller mit der Produktion beauftragen. Diese hier beschriebene Funktion wird in der Literatur auch als »CMS« oder »KMS« bezeichnet.

2.6 Schlüsselverwaltung

Die eGK muss per gesetzlicher Vorgabe so vorbereitet sein, dass auf ihr auch kryptographische Schlüssel verwendet werden können. Hierzu ist ein Key Management System, auch »KM« genannt erforderlich.

2.7 Anwendungsverwaltung

Dieser Dienst verwaltet die für die jeweilige eGK vorgesehene Anwendungen über den gesamten Lebenszyklus hinweg. Diese Systemkomponente wird allgemein als »CAMS« oder auch »KAMS« genannt. Eine dieser Anwendungen ist z.B. die »elektronische Patientenakte«, die auch schon in ein paar regional begrenzten Tests unter verschiedenen Aspekten auf Tauglichkeit im Praxiseinsatz geprüft und weiterentwickelt wird.

3. Produktion der elektronischen Gesundheitskarte

Der Anstoß zur Produktion einer elektronischen Gesundheitskarte ist gegeben,

- wenn ein neues Vertragsverhältnis entsteht, bzw. die existierende eGK einer anderen Versicherung zwar existiert, aber nicht weiter verwendet werden soll,
- wenn die Laufzeit der bestehenden Karte ausläuft, aber das Vertragsverhältnis noch besteht,
- bei Diebstahl, Verlust oder technischem Defekt der Karte,
- wenn optisch personalisierte Stammdaten nicht mehr mit den Daten im Chip übereinstimmen wie z.B. bei Namensänderung.

Vor dem eigentlichen Anstoß der Produktion erteilt der Versicherer dem Kartenverwalter den Auftrag zur Produktion. Der Kartenverwalter erhält wie oben beschrieben die hierzu erforderlichen Daten von den unterschiedlichen Datenlieferanten.

Der Herstellungsprozess beim Kartenhersteller teilt sich in folgende Teilschritte auf:

1. Virginalkarten-Produktion (Kartenvorproduktion)

Unter einer »Virginalkarte« verstehen Kartenhersteller den beidseitig bedruckten Kartenkörper mit dem Layout des Versicherers auf der Vorderseite und dem »E-111« Vordruck auf der Rückseite (Standardfall). Bei Personen ohne Anspruch auf Versicherungsleistung im EU-Ausland wird die Rückseite anders bedruckt, ggfs. die Datenfelder mit »X« ausgefüllt. Um als Kartenhersteller eine zeitnahe Nachproduktion zu gewährleisten, müssen immer ausreichende Mengen Virginalkarten in einer gesicherten Umgebung gelagert werden. Dieses ist ein Prozess, wie er im Bankenbereich schon lange üblich ist.

2. Initialisierung

Während der Initialisierung werden betriebssystemabhängige Initialisierungskommandos in den Chip gebracht. Es wird dadurch die für alle Karten gleiche Verzeichnis- und Datenstruktur zur eGK aufgebracht. Der Initialisierungsprozess ist von erheblicher Bedeutung, denn hierbei werden schon alle grundlegenden erlaubten Prozesse definiert.

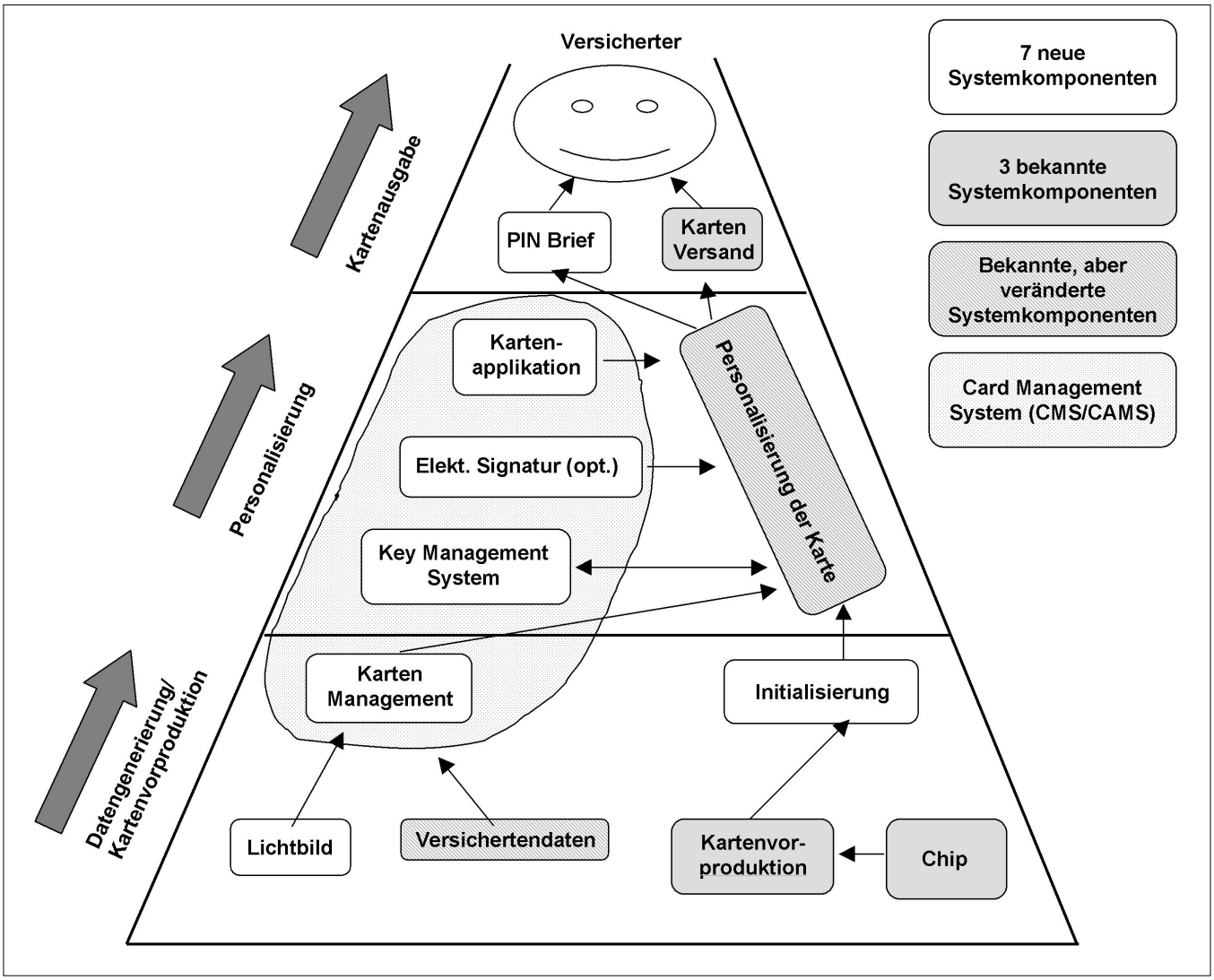


Abbildung 2

Eine Erweiterung dieser quasi »eingebrannten« Prozesse ist nachträglich nur mit erheblichen Aufwänden (Patch) möglich.

3. Personalisierung

Der Vorgang der Personalisierung wird in die optische Personalisierung des Kartenkörpers und die elektrische Personalisierung des Chips unterteilt. Zur optischen Personalisierung gehören bei der eGK die bekannten Stammdaten wie Name und Krankenversicherungsnummer, aber auch der Versichertenstatus und das Lichtbild des Versicherten.

Bei der elektrischen Personalisierung werden alle Daten aus der Abbildung Nr. 1 in den Chip eingebracht. In dieser Phase können auch Zertifikate des Karteninhabers eingebracht werden, falls diese schon zu diesem frühen Zeitpunkt bereitstehen sollten.

Die elektronische Signaturfunktion für die qualifizierte Signatur ist aber auch nachladbar, wenn die Karte bereits im Einsatz ist. Zusätzlich werden bei der Personalisierung auch auftragsbezogene Daten wie Angaben für das zugehörige Begleitschreiben verarbeitet.

Selbstverständlich müssen die personenbezogenen Daten vom Zeitpunkt ihrer Generierung bis zur Personalisierung auf dem Chip vertraulich transportiert werden. Hierfür ist eine Ende-zu-Ende-Verschlüsselung vorgesehen. Die Details zur dieser Datenübergabeschnittstelle werden aktuell von der gematik mbh erstellt; ein Vorgriff auf die Ergebnisse ist somit nicht möglich.

Die oben genannten Prozesse sind in Abbildung 2 nochmals graphisch dargestellt.

Aber der Teufel steckt bekanntlich im Detail wie z.B. bei der Laufzeit der eGK: Die Laufzeit einer eGK befindet sich sowohl im Chip als auch optisch auf der Rückseite der eGK. Die Daten der Rückseite der eGK ersetzen den auch unter »Auslandskrankenschein« bekannten E-111 Vordruck. Karteninhaber mit ausgefüllter Kartenrückseite haben somit Anspruch auf eine Behandlung bei vorübergehendem Aufenthalt in der EU. Wenn z.B. aufgrund einer Vertragskündigung die eGK nicht mehr gültig und noch nicht zurückgegeben ist, kann die Karte durch eine Aktualisierung vom Versicherer über das Kartenmanagementsystem in der Infrastruktur als ungültig markiert werden.

Da aber der Zugriff auf die Infrastruktur vom EU-Ausland nicht möglich ist, kann sich der Karteninhaber weiterhin im EU-Ausland behandeln lassen.

Kai Janneck

Datenschutz als Wettbewerbsvorteil

Innovationszentrum Datenschutz & Datensicherheit (ULD-i)

Das Innovationszentrum Datenschutz & Datensicherheit (ULD-i) ist ein Angebot des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an die Wirtschaft, den Datenschutz als Wettbewerbsvorteil zu nutzen. Mit dem ULD-i wurde in Schleswig-Holstein, nach dem Datenschutz-Gütesiegel, das zweite bundesweit einzigartige Angebot zur Stärkung des Wirtschaftsstandorts »Deutschland« konzipiert.

Das Ziel des ULD-i ist es, innovative Ideen rund um Datenschutz und Datensicherheit zu bündeln, um so neue und Erfolg versprechende Datenschutzprojekte zu initiieren. Die Projektbeteiligten sollen dabei erfolgreich datenschutzgerechte Produkte entwickeln und mit dem Alleinstellungsmerkmal »Datenschutz« die eigene Marktposition stärken und sich von Mitbewerbern absetzen. Dies ist eine entscheidende Motivation für die Entwicklung von Privacy Enhancing Technologies, also datenschutzfördernder Technik.

Wettbewerbsvorteil

Datenschutz wird in den Projekten und den daraus entstehenden Produkten als ein entscheidendes Produktmerkmal herausgearbeitet. Mit dem ULD-i wird so der Datenschutz über die Anbieterseite in den Markt gedrückt (Push-Strategie); daneben arbeiten Datenschutzorganisationen und Verbraucherschutzorganisationen daran, über die Aufklärung der Verbraucher einen Nachfragesog auf datenschutzgerechten Produkten ausüben (Pull-Strategie).

Der Datenschutz ist somit nicht Makulatur und Pflichterfüllung im Rahmen der gesetzlichen Auflagen, sondern ein Entscheidungskriterium beim Produktkauf und führt bei Missachtung zum Vertrauensverlust beim Kunden, der allenfalls durch hohe Marketinganstrengungen kompensiert werden könnte – wenn überhaupt.

Die Serviceleistungen

Das ULD-i versteht sich als Innovations- und Servicezentrum für Datenschutz und Datensicherheit. Mit Hilfe des ULD-i werden Kontakte zwischen Wirtschaft, Wissenschaft und anderen Ideenträgern geknüpft, aussichtsreiche Projektideen entwickelt und entsprechende Projektkonsortien gebildet. Das ULD-i unterstützt dabei mit Förderungsmanagement, Vermittlung von Projektpartnern, Projektmanagement, Wissenstransfer oder Entwicklung von Geschäftsmodellen.

Das ULD-i stellt seine Serviceleistungen flexibel in den einzelnen Projektphasen oder projektbegleitend nach Bedarf zur Verfügung (siehe Abb. 1).

Kompetenz

Organisatorisch ist das ULD-i an das ULD angegliedert. Durch diese enge Verbindung kann das ULD-i in seiner täglichen Arbeit flexibel auf die Erfahrungen und das Know-how des ULD zurückgreifen. Das ULD-i muss sich so kein zusätzliches Spezialwissen im Bereich Datenschutz und Datensicherheit aufbauen, sondern konzentriert sich auf seine Kernaufgaben im Servicebereich.

Das ULD hat durch eine Reihe innovativer Projekte wie AN.ON – Anonymität online[1], Virtuelles Datenschutzbüro[2], P3P – Datenschutz für Internetsurfer, Datenschutz-Audit und Datenschutz-Gütesiegel sowie PRIME[3] und FIDIS[4] aus dem Bereich Identitätsmanagement eine auch außerhalb Schleswig-Holsteins anerkannte Kompetenz in den Fragen des Datenschutzes durch Technik erworben. Die Bündelung und Effektivierung dieser Kompetenz im ULD-i ist Teil der Gesamtstrategie des ULD, die auf Datenschutz durch Technik und Datenschutz als Wettbewerbsvorteil ausgerichtet ist. Dem ULD-i kommt dabei die spezielle Aufgabe zu, die Umsetzung dieser Ideen in konkrete Produkte und Projekte zu unterstützen.

[1] http://www.anon-online.de/; vgl. S. 13 ff.
[2] http://www.datenschutz.de/.
[3] http://www.prime-project.eu.org/.
[4] http://www.fidis.net/.

www.uld-i.de

Neben dem persönlichen Kontakt steht das ULD-i mit seinen Informationen zum Serviceangebot natürlich auch im Internet zur Verfügung. Unter http://www.uld-i.de/ präsentiert das Innovationszentrum aktuelle Projekte, Gutachten und neue Technologien zum Thema Datenschutz und Datensicherheit.

Das ULD-i wird im Rahmen des Regionalprogramms 2000 von der Europäischen Union kofinanziert. Die Leistungen des ULD-i stehen Interessierten kostenlos zur Verfügung.

Sie haben eine Idee für »Datenschutz durch Technik«?

Nehmen Sie Kontakt zum ULD-i auf! Gemeinsam erarbeiten wir eine Idee für ein Projekt oder eine Produktentwicklung. Wir unterstützen Sie bei der Suche nach Fördermöglichkeiten und nach interessierten Kooperationspartnern, z.B. Firmen, Diplomanden oder andere Ideenträger im Wissenschaftsbereich, die das Projektteam sinnvoll ergänzen können.

Das Spektrum für solche Ideen ist sehr umfassend: Es reicht von der Entwicklung von Software für Verwaltung und Wirtschaft zur datenschutzgerechten Datenverarbeitung über Selbstdatenschutz-Tools für Nutzer bis hin zur Erarbeitung und Bereitstellung von Musterlösungen für Policies und Konfigurationen von IT-Systemen. Auch eine innovative Gestaltung von Benutzungsoberflächen oder durch bauliche Maßnahmen bei der architektonischen Pla-

nung von Geschäftsstellen zu mehr Datenschutz ist denkbar. Konzepte für Ausbildung, Wissensvermittlung und Schaffung von Datenschutzbewusstsein gehören ebenfalls zum Themenspektrum, in dem das ULD-i gern unterstützt. Und schließlich gibt es noch den Bereich der Technikfolgenabschätzung zu neuen technischen Entwicklungen wie Ubiquitäres Computing oder Überwachungsinfrastrukturen und die Untersuchung von Ansätzen wie Privacy Management Languages oder kryptographische Anonymisierungs- und Pseudonymisierungskonzepte.

Kontakt:
Innovationszentrum Datenschutz & Datensicherheit (ULD-i)
beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98 – 24103 Kiel
Tel: 0431/ 988-1399
kontakt@uld-i.de – www.uld-i.de

Henry Krasemann

Anonymität ganz einfach und legal

Die Tarnkappe für das Internet – nicht nur für Langstreckenflieger

Wer das Internet nutzt, hinterlässt Spuren und ist identifizierbar. Anonymisierungsdienste helfen dem Nutzer sein Recht auf Anonymität umzusetzen und diese Spuren zu verwischen.

Frau K traute ihren Ohren nicht. Was der aus Pakistan stammenden Bundesbürgerin von den so genannten »Border Agents« bei ihrer Einreise in die USA entgegengehalten wurde, klang unglaublich. Man habe bei einem der größten Onlineversender für Bücher recherchiert und festgestellt, dass sie sich für »Bücher über Zweitsprachen« interessiere. Die Einreise wurde ihr verwehrt.[1]

Spuren im Netz

Wer sich im Internet bewegt, hinterlässt Spuren. Jeder Rechner, der online ist, ist durch eine Nummer, die so genannte IP-Adresse, eindeutig identifizierbar. Dies ist auch technisch notwendig, um überhaupt die einzelnen Rechner adressieren zu können. Die Datenpakete wüssten sonst nicht, wo sie hin müssten. Dabei wird bei jeder Abfrage, sei es einer Webseite oder eines anderen Webdienstes wie Onlinebanking oder Chat, stets diese Nummer mit weiteren Daten etwa über die Beschaffenheit des Rechners, Suchmaschinenabfragen oder Ursprungswebseiten an den Diensteanbieter bzw. Webseitenbetreiber übermittelt. In der Regel speichert dieser diese Daten dann, um sie später für Auswertungszwecke nutzen zu können. Die deutschen Datenschutzgesetze setzen dem zwar enge Grenzen. Kaum ein Anbieter hält sich jedoch hieran – schon in Deutschland nicht, noch weniger im globalen Internet. Das Surfverhalten einzelner Nutzer lässt sich so noch Monate oder gar Jahre später nachvollziehen.

Die festen IP-Adressen, die stets und eindeutig einem Computer zugeordnet sind, stellen heutzutage die Ausnahme dar. Üblicher ist es, dass die IP-Adressen dynamisch vergeben werden. Wer sich zum Beispiel bei T-Online einwählt, bekommt eine freie Adresse aus dem diesem Provider zugeordneten Pool von IP-Adressen zugewiesen. Beendet er die Verbindung, steht die IP-Adresse wieder für andere Nutzer zur Verfügung.

Dieses Verfahren bietet jedoch nur vordergründig Sicherheit gegenüber wissbegierigen Webdiensteanbietern. So führen viele Provider Listen, welcher ihrer Kunden wann welche IP-Adresse zugewiesen bekommen hat. Zulässig ist dieses nach der wohl herrschenden Meinung grundsätzlich nur, soweit es für die Erbringung des Dienstes und die Abrechnung notwendig ist.[2] Dies gilt ungeachtet der Frage, ob es sich hierbei um einen Telekommunikationsdienst oder Teledienst handelt. Denn sowohl § 97 Abs. 3 Telekommunikationsgesetz als auch § 6 Abs. 4 Teledienstedatenschutzgesetz verlangen eine entsprechende Löschung nicht benötigter personenbezogener Daten.[3] Aber selbst über Flatrate-Kunden speichern einige Provider für mehrere Monate entsprechende Logfiles.[4]

Führt man die Daten des Diensteanbieters und des Providers zusammen, sind die Aktionen wieder einem Nutzer eindeutig zuzuordnen. Einige Provider haben sich schon früher durchaus freigiebig hinsichtlich dieser Daten gezeigt, wenn ihnen mit Klage gedroht wurde.[5] Und bei größeren Providern, die gleichzeitig auch Inhalte zum Abruf anbieten, ist es zumindest technisch kein Problem, einen derartigen Abgleich durchzuführen.

Teilweise sind die Nutzer aber auch selber dafür verantwortlich, ob ihre Identität aufgedeckt werden kann. Füllt man ein Webformular wahrheitsgemäß aus, weiß schon einmal der Betreiber dieses Angebots, wer sich im Moment

[1] Vgl. zu einem ähnlichen Fall www.heise.de/tp/r4/artikel/16/16039/1.html.

[2] Vgl. Tätigkeitsbericht 2005 des ULD SH, Rn. 7.4, S. 106f.; Dix, DuD 2003, S. 234 ff.; Heidrich, DuD 2003, S. 237 ff.

[3] Vgl. AG Darmstadt, Urteil vom 30.06.2005, Az.: 300 C 397/04.

[4] Vgl. z.B. zur Speicherung von IP-Adressen bei T-Online Heise-Meldung www.heise.de/newsticker/meldung/61293.

[5] Teilweise wehren sich die Provider jedoch auch gegen das Herausgabeverlangen etwa von Inhabern von Verwertungsrechten, die sich auf § 101a UrhG berufen. Vgl. hierzu auch www.heise.de/newsticker/meldung/57111.

hinter der entsprechenden IP-Adresse verbirgt. Ist er auch etwa Werbepartner zahlreicher anderer Seiten im Netz, kann er zumindest eingeschränkt das weitere Verhalten des Nutzers im Netz verfolgen. Dies gilt erst recht, wenn Cookies eingesetzt werden.

Visitenkarten fürs Kaufhaus

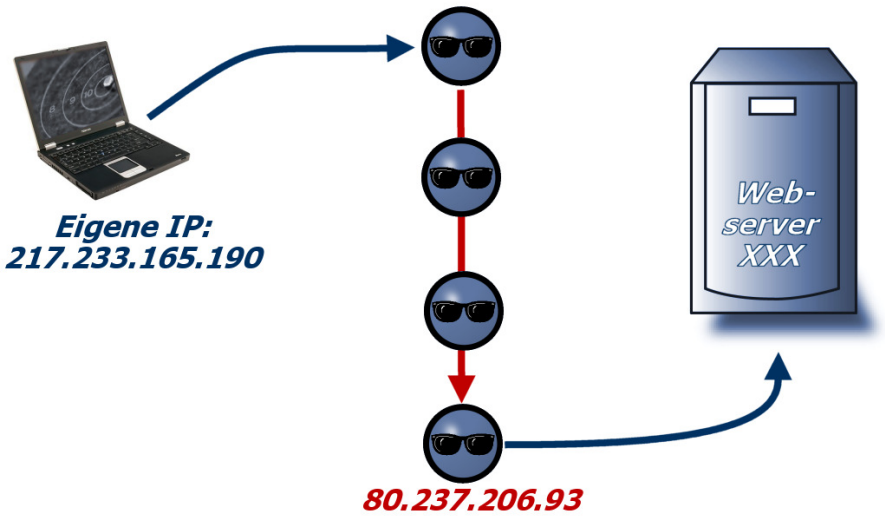
Im Gegensatz zum traditionellen Einkaufsbummel gibt man somit beim Shoppen im Internet stets eine mehr oder weniger gut zuordenbare Visitenkarte beim Betreten ab. Dies widerstrebt dem Recht des Einzelnen auf Anonymität. So schreibt § 4 Abs. 6 Teledienstedatenschutzgesetz eindeutig vor, dass »der Diensteanbieter [...] dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen [habe], soweit dies technisch möglich und zumutbar ist.« Einige Firmen und Organisationen haben dieses Problem erkannt und bieten Anonymisierungsdienste im Internet an. Das Verfahren ist zunächst recht simpel. Statt selber nach außen hin auf Webangebote zuzugreifen, bedient man sich eines Boten. Dieser Zwischenhändler bzw. »Proxy«-Rechner nimmt die Anfrage des Nutzers an und leitet sie an die entsprechende Empfängeradresse weiter. Die Antwort geht dann denselben Weg. Der Empfänger bzw. Diensteanbieter sieht somit nur die IP-Adresse dieses zwischengeschalteten Proxy und kann keine Rückschlüsse auf den sich dahinter befindenden Nutzer ziehen. Der Nachteil dieser Lösung ist jedoch, dass der Nutzer dem Betreiber des Proxys vertrauen muss. Denn dort geht sein sämtlicher Webverkehr durch, inklusive Absender- und Zieladresse. Ein Mitloggen und Analysieren der Daten auf bestimmte Stichworte wäre technisch kein Problem. Etwas weitergehend sind Lösungen, die regelmäßig den eingeschalteten Proxy wechseln. Stehen diese jedoch auch wiederum unter der Kontrolle des Anbieters, hat sich an der Gefahrenlage nichts geändert.

AN.ON macht das TOR auf

Weitergehend sind Lösungen, die mehrere Zwischenhändler hintereinander schalten. Vertreter dieser Lösungen ist zum einen der vom Bundesministerium für Wirtschaft und Arbeit geförderte Dienst AN.ON (vgl. www.anon-online.de), der von den Universitäten Dresden, Regensburg und Berlin in Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betrieben wird. Zum anderen existiert insbesondere in den USA ein System mit dem Namen TOR (vgl. tor.eff.org).

Bei AN.ON wird schon der Webverkehr vom Computer des Nutzers zum ersten Proxy (hier Mix genannt) verschlüsselt. Durch Einsatz entsprechender Verschlüsselungsverfahren ist es möglich, dass dieser erste Mix zwar erfährt, von wo die Daten kommen. Er kann jedoch nicht sehen, wohin die Daten gehen sollen und welchen Inhalt sie haben. Daher schickt er das Paket entsprechend weiter an den zweiten Mix. Dieser weiß nur, dass die Daten vom vorhergehenden Mix kommen und dass er sie an den dritten Mix weiterleiten muss. Erst der letzte Mix in der Kette (»Kaskade« genannt) kann entschlüsseln, an welchen Webdienst er das Paket schicken soll. Er kann aber nicht mehr erkennen, wo es ursprünglich mal herkam. Nur wenn alle Betreiber der Mixe zusammenarbeiten würden, wäre eine Aufdeckung des Nutzers wieder möglich. Daher ist es Bestreben der Betreiber des AN.ON-Dienstes, eine möglichst weite Streuung zu erreichen. Ideal wären Mix-Kaskaden wie New York - Teheran - Kiel oder auch ULD - Amnesty International - Bundeskriminalamt.. Das Risiko des Zusammenwirkens sämtlicher Mix-Betreiber zu Ungunsten des Nutzers wäre zu vernachlässigen, die Anonymität bliebe gewahrt. Und Polizeibeamte dürften ohnehin bei ihren Ermittlungsarbeiten zu den Nutzern das AN.ON-Dienstes zählen.

Werden bei AN.ON bisher vor allem Betreiber geführt, die sich gegenüber den Nutzern identifizieren, kann bei TOR jeder einen entsprechenden Mix (dort »Node« bzw. »Knoten« bezeichnet) betreiben. Der Anwender sucht sich zuvor keine feste Kaskade aus, die er nutzen möchte, sondern das System wählt selbstständig einen Weg durch das Knoten-Gewirr. Dieses wilde System scheint auf den ersten Blick noch sicherer zu sein. Jedoch bringt es auch neue Gefahren mit sich: Es wäre problemlos für größere Organisationen möglich, zahlreiche neue Knoten anzumelden, um so die Wahrscheinlichkeit zu erhöhen, wiederum die Kontrolle über den kompletten Weg der Datenpakete zu erhalten.



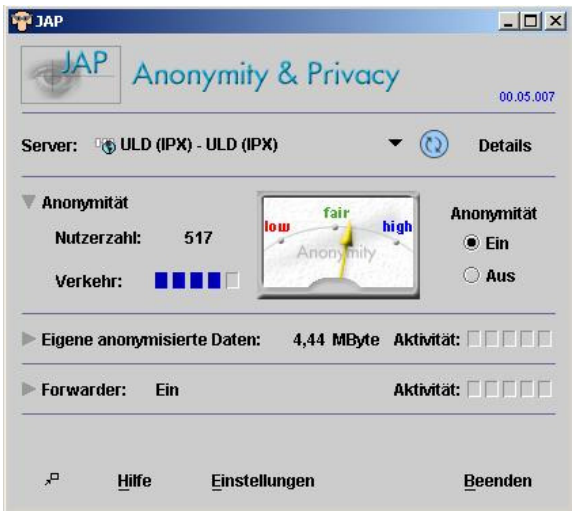
Im Einsatz

Die Nutzung beider Systeme ist für den Anwender kostenlos. Zum Betrieb muss man Zusatz-Software installieren: Es empfiehlt sich, die Software JAP zu verwenden, die von dem AN.ON-Dienst zur Verfügung gestellt wird und nicht nur das eigene System, sondern neuerdings auch TOR unterstützt.

Die Software kann kostenlos von der Website www.anon-online.de heruntergeladen werden und ist auf allen gängigen Systemen wie Windows, Mac OS, Linux und Pocket PC lauffähig. Notwendig ist einzig eine aktuelle Java-Version. Der Mac bringt diese meist schon mit. Bei Windows ist eine vorherige Installation notwendig. Die entsprechenden Daten befinden sich in der vollständigen JAP-Installation, so dass

dieses keine Mühe machen sollte.

In der Regel sollten nach der Installation keine weiteren Anpassungen notwendig sein. In Ausnahmefällen, wenn vor allem der benutzte Browser nicht erkannt wird und die automatische Konfiguration nicht vollständig läuft, ist einmalig manuell bei den Proxy-Einstellungen als Adresse 127.0.0.1 und als Port 3128 einzutragen. Ab dann wird beim Surfen der Internetverkehr über das JAP-Tool geleitet. Dabei kann der Nutzer stets auswählen, ob er die Anonymisierung einschaltet (»ein«) oder auf herkömmliche Weise (»aus«) surfen will. Weitere Einstellungen sind auch bei ausgeschalteter JAP-Software nicht erforderlich. Nur gestartet sein muss sie. Das Ausschalten bietet sich insbesondere dann an, wenn man eine Anonymisierung nicht benötigt und die volle Geschwindigkeit etwa eines DSL-Zugangs nutzen möchte. Denn eine zumindest leichte Geschwindigkeitseinbuße geht mit der Anonymisierung meist einher. Durch die Gewinnung neuer Betreiber von Mix-Rechnern und damit Verteilung des Internetverkehrs auf mehr Kaskaden kann diese in Zukunft allerdings geringer werden. Eine gewisse Nutzerzahl pro Kaskade (Anonymitätsgruppe) ist jedoch erforderlich, um die Anonymität der Nutzer zu erreichen.



Unter »Server« im JAP-Tool lassen sich die aktuell aktiven Kaskaden anzeigen und auswählen. Und wenn hinter »Eigene anonymisierte Daten:« eine stetig wachsende Zahl zu erkennen ist, kann man sicher sein, dass die Anonymisierung funktioniert. Auf Seiten wie Leader.ru (http://www.leader.ru/secure/who.html) kann die Wirkung der Anonymisierung überprüft werden. Zu beachten ist dabei, dass AN.ON nur die IP-Adresse anonymisiert, nicht jedoch weitere Daten, die der Browser an die Diensteanbieter übermittelt. Dies betrifft Angaben wie etwa Betriebssystem, Browsertyp, oder auch die Angabe über die Internetseite, von der man gerade kommt (Referrer). Dies kann man entweder direkt im Browser einstellen, oder aber mittels zusätzlicher Tools beeinflussen.[6]

Eine weitere neue Funktionalität der JAP-Software ist das »Forwarding«. Hiermit stellt man seinen eigenen Rechner als Zugangspunkt ins Internet für andere zur Verfügung. Dies ist vor allem sinnvoll für Bewohner von totalitären Staaten, wo der Zugang zum Internet reguliert und eingeschränkt wird. Diese können dann über die zusätzlichen Zugangspunkte auf das freie Internet zugreifen. Will man die Forwarding-Funktion aktivieren, sollte man sich allerdings auch Gedanken darüber machen, dass man selber ins Fadenkreuz von Ermittlungen gelangen kann, sollte derjenige, den man so huckepack ins Netz mitgenommen hat, dort Schindluder treiben.

Das TOR-System wird vom JAP-Tool automatisch verwendet, wenn auf Internet-Dienste außerhalb des normalen Surfens (z.B. Peer-to-Peer, FTP) zugegriffen werden soll. Hierzu ist es jedoch erforderlich, nach dem Start des JAP unter »Einstellungen – Dienste – Tor« auf »Liste neu laden« zu klicken, um ein Verzeichnis aktueller Knoten bereit zu haben.

Fazit

Anonymisierer können sicherlich nicht den kompletten Internetverkehr absichern und vor jeglicher Aufdeckung schützen. Der normale Nutzer kann sich jedoch mit ihnen zumindest ein Stück seines Rechts auf Anonymität zurückholen.

Im Ausgangsfall war Frau K eine selbst erstellte, öffentliche »Wunschliste« auf den Seiten des Buchversenders zum Verhängnis geworden, die ihre mutmaßlichen Interessen widerspiegelten. Selbst wenn man nicht solche Informationen öffentlich macht, könnten Beobachter im Netz mit entsprechenden Zugriffsmöglichkeiten das Surfverhalten und damit die Interessen von Internetnutzern detailliert analysieren. Anonymisierer helfen nicht nur bei der Entspannung auf Langstreckenflügen ins Ausland, sondern auch darüber hinaus.

Fact Sheet AN.ON:
Name: AN.ON – Anonymität Online
URL: www.anon-online.de/
Förderung: Bundesministerium für Wirtschaft und Arbeit seit: 2001
Partner: TU Dresden, Universität Regensburg, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, HU Berlin
Weitere Mix-Betreiber: FU Berlin, CCC, Ulmer Akademie für Datenschutz und IT-Sicherheit
Aktuell aktive Mix-Kaskaden: ca. 8
Gleichzeitige Nutzer: ca. 3.000
Datendurchsatz pro Monat: ca. 10 TBytes

Weitere interessante Quellen und Literatur zum Thema:

- AN.ON Projektseite des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein: www.datenschutzzentrum.de/anon/
- Informationen über TOR: tor.eff.org/
- AN.ON und Strafverfolgung: www.anonymitaet.com/bka/
- Zur Technik der Mixe: David Chaum: »Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms«. Communications of the ACM, February 1981, Volume 24, Number 2
- Hannes Federrath: Das AN.ON-System: Starke Anonymität und Unbeobachtbarkeit im Internet. in: Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Verlag Vieweg, 2003, 172
- Stefan Köpsell, Hannes Federrath, Marit Hansen: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003),139
- Martin Rost: Zur gesellschaftlichen Funktion von Anonymität – Anonymität im soziologischen Kontext, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003), 155

[6] Vgl. z.B. für Firefox die Web Developer Tools unter http://chrispederick.com/work/firefox/webdeveloper/.

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund
Forensische DNA-Analyse neu geregelt

Am 08.07.2005 hat der CDU-dominierte Bundesrat den von der rot-grünen Bundesregierung vorgelegten Gesetzentwurf zur Neuregelung der DNA-Analyse für Strafverfolgungszwecke passieren lassen. Die Änderung des § 81f Abs. 1 Strafprozessordnung (StPO) ermöglicht bei Zustimmung der Betroffenen oder Gefahr im Verzug die Durchführung von DNA-Analysen ohne richterliche Anordnung. Bei wiederholten geringen Straftaten wird auf das Erfordernis einer erheblichen Straftat verzichtet. Außerdem werden in einem neuen § 81h StPO sog. molekulargenetische Reihenuntersuchungen (DNA-Massentests) erlaubt. Vorläufig vom Tisch ist damit die von CDU/CSU-Politikern und Vertretern von Sicherheitsbehörden geforderte Gleichstellung des »genetischen Fingerabdrucks« mit der klassischen Daktyloskopie. Die Union hat angekündigt, im Fall eines Wahlsieges den genetischen Fingerabdruck erheblich auszuweiten. Der potenzielle Koalitionspartner FDP meldete hiergegen Widerstand an.

Die Gesetzesänderung wird von der Bundesvorsitzenden der Humanistischen Union, Prof. Dr. Rosemarie Will, kritisiert: »Jede DNA-Analyse stellt einen schwer wiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar. Dieser ist nach rechtsstaatlichen Kriterien nur zulässig, wenn er zum Schutz des öffentlichen Interesses unerlässlich ist. Dass die Erfassung des genetischen Fingerabdrucks eines mehrfachen Ladendiebs zum Schutz des öffentlichen Interesses nötig sei, leuchtet nicht ein.« Außerdem könne bei den eingeholten Einwilligungen nicht immer von Freiwilligkeit die Rede sein: »Der Humanistischen Union sind Fälle bekannt geworden, in denen Verweigerer ›freiwilliger‹ Tests allein auf Grund ihrer Ablehnung zu Tatverdächtigen in polizeilichen Ermittlungsverfahren wurden.« Häufig würden solche Tests im Strafvollzug durchgeführt, wobei die Betroffenen bei Nichtteilnahme negative Sanktionen befürchten müssten. Wenn die massenweise DNA-Analyse zum normalen Ermittlungsinstrument wird, gerieten alle TeilnehmerInnen zu potenziell Verdächtigen (SZ 09./10.07.2005, 6; PE HU Nr. 10-2005 30.06.2005; PE BT-Fraktion Bündnis 90/Die Grünen Nr. 614 30.06.2005; Die Welt 09.06.2005, 2).

Bund
Managergehälter werden offen gelegt

Wenige Tage vor der Landtagswahl in Nordrhein-Westfalen beschloss das Bundeskabinett am 17.05.2005 einen Gesetzentwurf, der börsennotierte Firmen zwingt, die Gehälter ihrer Top-Manager ab dem Jahr 2006 offen zu legen. Kurz vor der parlamentarischen Sommerpause und dem Misstrauensvotum gegen den Bundeskanzler verständigten sich am 24.06.2005 die Regierung mit der Union über dieses Gesetz, das am 30.06.2005 vom Bundestag beschlossen wurde.

Ursprünglich hatte Bundesjustizministerin Brigitte Zypries noch warten wollen, ob deutsche Firmen freiwillig jene Regeln befolgen, die eine von Thyssen-Krupp-Aufsichtsratschef Gerhard Cromme geleitete Regierungskommission seit langem empfiehlt. In den USA oder Großbritannien ist es gang und gäbe, dass Unternehmen die Vorstandsgehälter einzeln ausweisen. In Deutschland leisten bislang gerade einmal 20 der 30 DAX-Konzerne diesem Rat Folge. Drei weitere geben zumindest die Bezüge des Vorstandsvorsitzenden an. Konzerne wie BMW, DaimlerChrysler, Münchner Rück, MAN und BASF lehnten die Offenlegung bis zuletzt ab. Von der Offenlegungsregelung werden knapp 1000 börsennotierte Aktiengesellschaften betroffen sein. Vor ca. einem Jahr hatte Zypries vor einer hochkarätigen Managerrunde angekündigt, sie wolle der Wirtschaft noch ein, zwei Jahre Schonfrist geben. Zypries beteuerte, das Gesetz solle nicht die allgemeine Neugier stillen oder eine Neiddebatte befördern, sondern das Vertrauen in die Konzernlenker stärken.

Das Gesetz verpflichtet alle börsennotierten Firmen, für jeden Vorstand Grundgehalt, Zulagen und sonstige Leistungen offen zu legen. Unternehmen müssen mit einer Strafe von bis zu 50.000 Euro je Vorstandsmitglied rechnen, wenn sie die Bezüge ihrer Vorstände verheimlichen. Erfasst werden auch Aktienoptionen, Dienstvillen und ähnliche Vorteile – es sei denn, die Aktionäre des Unternehmens beschließen mit 3/4-Mehrheit, die Angaben zu verweigern. Diese Ausnahme, das sog. Lex Wiedeking, stieß auf Kritik bei Gewerkschaften und Aktionärsschützern. Firmen in Familienbesitz, wie z.B. der von Wendelin Wiedeking geführte Autohersteller Porsche, können das Gesetz damit umgehen. Auch der Autobauer BMW wird mehrheitlich von der Eigentümerfamilie Quandt dominiert.

Ein weiterer Kritikpunkt ist, dass sich das Gesetz nur auf börsennotierte Unternehmen bezieht. Der Deutsche Gewerkschaftsbund (DGB) fordert, die Vorschriften auf alle großen Kapitalgesellschaften auszuweiten. Vertreter der Opposition forderten, auch öffentliche Unternehmen einzubeziehen (zu Krankenkassen siehe in diesem Heft S. 33). Nach Ausscheiden von Vorständen bleiben zudem Zahlungen häufig weiter geheim. Aktionärsschützer kritisieren, dass sie keine Informationen über die häufig millionenschweren Abfindungen an Manager erhalten. Ebenso undurchsichtig seien oft die Pensionsvereinbarungen. Insgesamt bewerten die Kritiker aber das Gesetz als einen Fortschritt. Auch aus den Konzernen und von den Wirtschaftslobbyisten kommt nur vereinzelt Kritik. Der Manager-Elite dürfte längst bewusst sein, dass mehr Transparenz bei Vorstandsgehältern überfällig ist. Dies gilt nicht für Porsche-Vorstandschef Wendelin Wiedeking, der zu bedenken gab, dass

das Gesetz gegen das Recht auf informationelle Selbstbestimmung verstoße und damit verfassungswidrig sei (§§ 285 S. 1 Nr. 9, 314 Abs. 1 Nr. 6a HGB; BT-Drs. 15/5577; BR-Drs. 451/05; Bovensiepen, SZ 18.05.2005, 2; 25./26.06.2005, 1, 21; Deckstein/Schäfer, SZ 01.07.2005, 19; BT-Drs. 15/5577 v. 31.05.2005).

Bund
Initiative für ein Register für klinische Studien

Am 12.07.2005 veröffentlichten der Verbraucherzentrale Bundesverband (vzbv), der Wissenschaftsrat, die Bundesärztekammer und knapp ein Dutzend weiterer Organisationen einen »Aufruf« zur Gründung einer frei zugänglichen Datenbank, in der Versuche an PatientInnen lückenlos erfasst werden sollen. Solche Register existieren in den USA, Großbritannien und Australien seit Jahren. In Deutschland gibt es nur kleine Initiativen wie das »Deutsche Register für somatische Genstudien« oder das »Studienzentrum der Deutschen Gesellschaft für Chirurgie«. Gerd Antes, Sprecher der Initiativgruppe Studienregistrierung, die treibende Kraft hinter der Allianz: »Wir fordern, dass in Zukunft alle klinische Studien zugänglich sein müssen.« Dabei soll es sich nicht um eine bürokratische Maßnahme handeln. Vielmehr sollen künftig PatientInnen, ÄrztInnen und WissenschaftlerInnen leicht einen Überblick über den Stand der medizinischen Forschung erhalten. Klinische Studien sind ein wichtiges Mittel, um wirksame von unwirksamen Therapien unterscheiden zu können. Die Ergebnisse dieser Studien werden zur Grundlage für die Zulassung neuer Medikamente oder für die Kostenübernahme durch Krankenkassen genommen.

Zugleich besteht der Verdacht, dass viele Studien missbraucht werden: So sollen von den in Deutschland stattfindenden mehreren tausend Studien nur die Ergebnisse etwa der Hälfte veröffentlicht werden, weil die anderen nicht die gewünschten Ergebnisse erbracht haben. Thomas Isenberg vom vzbv: »Wenn Studienergebnisse in der Schublade verschwinden, ist das Betrug am Patienten«. Eigentlich sollten nur Studien durchgeführt werden, wenn die Frage, die sie beantworten soll, noch nicht beantwortet ist. Dies wird oft nicht beachtet, wie das Beispiel des Medikaments Aprotinin gegen Blutungen zeigt, das seit 1987 in 64 Studien erprobt wurde. Redundante Studien sind nach Ansicht von Norbert Victor von der Universität Heidelberg nicht nur Verschwendung von Forschungsmitteln, »sondern auch eine Täuschung der Patienten, die zur Teilnahme an solchen Studien bereit sind«. Verhindert wird mit dieser Transparenzmaßnahme zudem – im Interesse der Datensparsamkeit – die unnötige Erhebung und Verarbeitung personenbezogener Daten im Rahmen der Forschungsprojekte. Die Initiative wird vom Bundesministerium für Bildung und Forschung unterstützt. Bis Mitte 2006 soll durch eine Ausschreibung entschieden werden, wer Geld zum Aufbau des Registers erhält. Bis dahin hofft die Allianz auf die Ethikkommissionen, ohne deren Einverständnis in Deutschland keine Studie beginnen darf. Victor fordert, »dass zukünftig eine Studie nur grünes Licht erhalten kann, wenn sie auch registriert wurde«. Für deutsche Ärzte, die in einer anerkannten Zeitschrift veröffentlichen wollen, führt schon heute kein Weg vorbei an Datenbanken wie »controlled-trials.com« oder »clinicaltrials.gov«. Ab dem 13.09. akzeptieren angesehene Journale wie das New England Journal of Medicine oder The Lancet keine Studien mehr, die nicht in einem offiziellen Register angemeldet wurden (Koch SZ 13.07.2005, 9).

Bund
Visa-Verfahren mit Biometrie-Einsatz

Das Auswärtige Amt weitet den Einsatz biometrischer Erkennungsmethoden in seinen Botschaften aus. Vom April 2004 bis zum März 2005 testete die deutsche Vertretung in Nigeria in einem Pilotversuch den parallelen Einsatz von elektronischer Gesichtserkennung und Fingerabdruckverfahren für alle NigerianerInnen, die ein langfristiges Visum für Deutschland beantragen.

40 % der 600 Antragstellenden hatten entweder bereits versucht, unter anderen Personalien einzureisen, waren in Deutschland als Kriminelle aufgefallen oder als Asylsuchende abgelehnt worden. Dies konnte v.a. durch den Vergleich der Fingerabdrücke ermittelt werden. Die Gesichtserkennung hätte nur 14 % der Antragstellenden als Betrüger entlarven können. Trotzdem urteilen die Behörden in einem Bericht weitgehend positiv über die Erfassung des Gesichts. Wenn die Qualität des Vergleichsfotos etwa im Ausländerzentralregister sich verbessere, könnten die Erkennungsraten noch erheblich steigen. Im Herbst 2005 will auch die deutsche Botschaft auf den Philippinen beginnen, die Fingerabdrücke der Antragstellenden dort zu scannen und ein digitales Foto des Gesichts zu machen. In Manila liegt die Zahl der Reisewilligen erheblich höher als in Lagos. So kann getestet werden, wie gut die Technik im Massenbetrieb funktioniert (Der Spiegel 31/2005, 20; vgl. DANA 2/2003, 15 f.).

Bund
Fußballfans werden kriminalisiert

In einer Sendung am 30.06.2005 berichtete das Fernsehmagazin Monitor, wie Fußballfans, denen nicht ansatzweise der Vorwurf von Straftaten oder Sicherheitsgefährdungen gemacht werden kann, erfasst, gegängelt und in ihren Rechten beeinträchtigt werden.

Fall 1: S.E. aus Rostock ist seit 10 Jahren Anhänger des FC Hansa und Gründungsmitglied eines offiziellen Fan-Clubs, der dem Motto »Fußball ohne Gewalt« verpflichtet ist. Als er Anfang Juni 2005 vom Flughafen Berlin-Schönefeld zu einem Freundschaftsspiel der deutschen Nationalmannschaft nach Irland fliegen wollte, wurde er von den BGS-Beamten festgehalten. Ihm wurde mitgeteilt, dass Reisepass und Personalausweis eingezogen würden und er bis nach dem Fußballspiel nicht ausreisen dürfe. Erst auf intensive Nachfragen erfuhr er, dass er seit dem letzten Bundesligaspiel von Rostock in Dortmund in der Datei Gewalttäter Sport gespeichert sei. Er war in einen Polizeikessel geraten und polizeilich kontrolliert worden.

Fall 2: Der Fußball-Fan B.G. aus Cottbus wurde 14 Tage vor einem Fußballspiel in Island, an dem er teilnehmen wollte, telefonisch mitgeteilt, seine Reise werde storniert, weil er und ein Freund vom Deutschen Fußballbund (DFB) als Sicherheitsrisiko angesehen würden. Der DFB führte eine Liste von Personen, die aus Sicherheitsgründen keine Eintrittskarten für das gewünschte Auslandsspiel bekommen sollten. Der DFB hatte diese Liste an ein Reisebüro weitergegeben, die die Reise dann

stornierte, obwohl der DFB offiziell behauptet, persönliche Daten nur an Polizei und Bundesgrenzschutz weiterzugeben. Auf eine Klage beim Amtsgericht Frankfurt stellte dieses fest: »Tatsachen, die die Sicherheitsbedenken ... belegen könnten, sind weder vorprozessual noch im Rahmen dieses Verfahrens seitens des DFB vorgetragen worden.«

Fall 3: Stuttgart-Fan V.S. aus Schopfheim kam in Freiburg in eine Menschenmenge, hinter der es zu Ausschreitungen kam. Vor ihm bildete die Polizei darauf hin eine Kette, kontrollierte ihn und ermittelte wegen Landfriedensbruch. Der Vater von V.S., der 20 Jahre lang nicht mehr beim Fußball war, bekam darauf hin ebenso wie sein Sohn ein bundesweites Stadionverbot. Nachdem diese sich anwaltlich dagegen zur Wehr setzten und festgestellt wurde, dass die Vorwürfe unbegründet sind und das Ermittlungsverfahren eingestellt wurde, wurde mitgeteilt, dass die Speicherungen gelöscht seien. Dennoch wurde V.S. beim Grenzübertritt in die Schweiz von einem Beamten darauf hingewiesen, dass er schon mal beim Fußball aufgefallen sei. Und weitere vier Monate später wurde er bei einer Routinekontrolle von der Polizei darauf angesprochen, dass er »kein unbeschriebenes Blatt« sei (www.wdr.de).

Bund
Feuerwehr gegen gemeinsame Einsatzzentralen mit Polizei

Die Berufsfeuerwehren in Deutschland sind strikt gegen die Einrichtung gemeinsamer Einsatzzentralen mit der Polizei, so wie dies von einigen Bundesländern geplant ist. Hamburgs Feuerwehrchef Dieter Farrenkopf: »Die polizeilichen Bedürfnisse nach Beweissicherung und Strafverfolgung dürfen nicht mit dem reinen Hilfegrundsatz der Feuerwehr vermengt werden«. Es bestehe die Gefahr, dass bei den Einsätzen die polizeilichen Bedürfnisse überwiegen. Konflikte gebe es schon heute beim Datenschutz, wenn Strafverfolgung gegen medizinische Schweigepflicht stehe. Ursus Fuhrmann vom Deutschen Städtetag befürchtet, dass die Feuerwehr als polizeiliches Werkzeug missbraucht werden könnte. Es sei bereits vorgekommen, dass die Polizei Rettungswagen oder Feuerwehrkleidung als Tarnung für Einsätze angefordert habe (Der Spiegel 20/2003, 22).

Bund
Lufthansa-Boarding mit Fingerabdruck

Möglichst noch vor 2006 sollen nach den Planungen der Lufthansa deren Bordkarten durch einen Fingerabdruck personalisiert werden. Beim Einchecken gibt der Fluggast am Schalter seinen Fingerabdruck ab, der über einen zweidimensionalen Barcode optoelektronisch lesbar auf der Bordkarte aufgedruckt wird. Beim Betreten des Flugzeugs (Boarding) wird der Barcode auf der Bordkarte ausgelesen und automatisiert mit dem Fingerabdruck des Fluggastes verglichen. So will die Lufthansa verhindern, dass Reisende, die nicht auf der Passagierliste stehen, mitfliegen.

Seit Anfang Juli 2005 testet die Lufthansa solche Bordkarten in einem Laborversuch. Daneben wird Vielfliegern eine SmartCard mit eingescanntem Fingerabdruck angeboten. Die Biometriedaten der Wenigflieger werden nicht gespeichert bzw. sofort nach dem Check-In wieder gelöscht. Fluggäste, die überhaupt keinen Fingerabdruck abgeben wollen, können sich – wie bisher – einer klassischen Personenkontrolle unterziehen lassen. Allerdings wird den Inhabern biometrischer Bordkarten eine zügigere Abfertigung versprochen. Das Projekt zielt auf eine weniger kosten- und zeitaufwändige Passagierkontrolle ab. Schon seit Februar 2004 beteiligt sich die Lufthansa an dem Programm BIOP II, bei dem Vielflieger über eine »automatische biometriegestützte Grenzkontrolle« (ABG) per Iris auf ihre Identität geprüft werden. Nach einer einmaligen Registrierung und Speicherung dauert dieser Kontrollvorgang etwa 15 Sekunden. Dabei findet jedes Mal ein automatischer Abgleich mit den Fahndungsbeständen im INPOL- und im Schengen-Informations-System statt (DANA 2/2004, 27).

Die innenpolitische Sprecherin von Bündnis 90/Die Grünen im Bundestag Silke Stokar beurteilt das neue Projekt kritisch: »Jeder kann Happy Digits machen, aber die Gefahr wird immer größer, dass die biometrischen Daten missbraucht werden. Eines Tages verfügt die organisierte Kriminalität über Fingerabdrücke vieler Bürger.« Ähnlich Patrick von Braunmühl vom Verbraucherzentrale Bundesverband (vzbv): »Biometrische Daten in der Hand von privaten Unternehmen sehen wir kritisch«. Es handelt sich bei dem Verfahren um ein Verifikations-, nicht um ein Identifikationsverfahren, d.h. die Fluggäste werden nicht aus einem Datenbestand heraus eindeutig bestimmt, vielmehr wird nur die biometrische Übereinstimmung zwischen Check-In und Boarding festgestellt. Der Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Thilo Weichert, sieht hierin keine großen Probleme. Wichtig sei allerdings, dass beim Barcodeverfahren wie vor allem bei der Datenspeicherung auf der Chipkarte die Betroffenen präzise darüber aufgeklärt werden, was mit ihren Fingerabdrücken passiert und dass sie die Möglichkeit der Wahl haben«. Wichtig sei außerdem, dass die Bordkarten nach dem Gebrauch regelgerecht entsorgt werden und nicht achtlos weggeworfen werden (Junge, Der Tagesspiegel 06.07.2005; www.heise.de 06.07.05; Haas, SZ 07.07.2005, 19).

Bund
Kirche will vielleicht extremistische Pfarrer und Mitarbeiter überprüfen

Der für Arbeitsrecht zuständige Referatsleiter der Evangelischen Kirche in Deutschland (EKD), Detlev Frey, erklärte, Geistliche, die sich für die Linkspartei, das Bündnis aus PDS und WASG, engagieren, müssten mit einer Loyalitätsprüfung rechnen. Zunächst müsse aber noch abgewartet werden, wofür die neue Linkspartei stehe und welche konkreten Inhalte sie vertrete. 650.000 MitarbeiterInnen wären davon betroffen. Nach der neuen am 01.09.2005 in Kraft tretenden »Loyalitätsrichtlinie« für Mitarbeiter in Kirche und Diakonie dürfen Beschäftigte keine Zweifel an der Glaubwürdigkeit der Kirche hervorrufen. Davon könne bei einem Engagement für rechts- oder linksextremistische Gruppierungen ausgegangen werden. Schon ein Jahr zuvor hatte der Ratsvorsitzende der EKD, Bischof Wolfgang Huber, erklärt, nach seinem Verständnis seien Pfarramt und PDS-Mitgliedschaft unvereinbar: »Ein Pfarrer kann nach meinem Verständnis we-

der NPD- noch PDS-Mitglied sein. Die NPD ist totalitär, fremdenfeindlich, zum Teil antisemitisch, die PDS hat kein Verständnis für Religion und freie Religionsausübung.«

Umgehend widersprach der Pressesprecher der EKD, Christoph Vetter, der Unvereinbarkeitsfeststellung. Die jüngst beschlossene Loyalitätsrichtlinie des Rats »über die Anforderungen der privatrechtlichen beruflichen Mitarbeit in der EKD und dem Diakonischen Werk der EKD enthalte weder explizit noch implizit Regelungen zur PDS und der neu gegründeten Linkspartei. Das Pfarrerdienstrecht sehe vor, dass das Pfarramt »unparteilich« auszuüben sei. Dies schließe ein politisches Engagement von Pfarrerinnen und Pfarrern außerhalb des Dienstes nicht aus. Bei Kandidaturen werde geprüft, wie dies sich auf die Kirchengemeinde und den kirchlichen Dienstauftrag auswirken könne. Die Übernahme eines Abgeordnetenmandats führe unabhängig von der Partei regelmäßig zu einem Ruhen des Dienstverhältnisses (Handelsblatt 19.07.2005; PE EKD 19.07.2005).

Bund

Email wird immer weiter verbreitet

Email wird bei den BundesbürgerInnen immer beliebter. Nach Angaben des Statistischen Bundesamtes haben bereits die Hälfte (47 %) die elektronische Post über das Internet genutzt. Zwei Jahre zuvor waren es erst rund ein Drittel (35 %). Dagegen wagte sich nur einer von fünf BundesbürgerInnen (18 %) in Online-Foren oder chattete regelmäßig. Die Möglichkeit zu Videokonferenzen und Internet-Telefonie gebrauchten nur 2 % (SZ 14.-16.05.2005, 26).

Bund

Ein Drittel zahlt mit E-Cash

An den Kassen im Einzelhandel wird fast jedes dritte Geschäft mit Karte abgewickelt. Der Anteil von Kartenzahlungen am Gesamtumsatz erhöhte sich nach Angaben des Hauptverbandes des Deutschen Einzelhandels (HDE) im Jahr 2004 auf 31,6 % (2003: 30,5 %). Davon entfiel der größte Teil auf die Bezahlung mit EC-Karten mit Unterschrift oder Geheimzahl, gefolgt von Kreditkarten und Handelskarten. Die meisten KundInnen zahlen immer noch bar (64,9 %). Der Rest des Umsatzes verteilte sich auf Rechnungen oder z.B. Tauschgeschäfte (SZ 28.04.2005, 20).

Baden-Württemberg

Haus und Grund beschafft illegal Mieterdaten von Schufa

Durch einen »Praxistest« des Stuttgarter Mietervereins kam heraus, dass der Haus- und Grundbesitzerverein der baden-württembergischen Landeshauptstadt sich über seine selbständige Wohnungsverwaltungs-GmbH illegal Zugang zur Datensammlung der Schufa verschafft. Das Unternehmen leitete Anfragen von Mitgliedern des Haus- und Grundbesitzervereins weiter und händigte deren Antwort schriftlich und telefonisch an die Anfragenden zurück. Auf Initiative des Mietervereins fragte ein Mitglied von Haus & Grund an verschiedenen Tagen telefonisch Daten über insgesamt vier Personen ab. Haus & Grund forderte weder eine Einwilligungserklärung der Betroffenen noch eine Benachrichtigung. Die Antwort kam schnell gegen eine Gebühr von jeweils 10 Euro. Der Mietervereinschef Rolf Gaßmann forderte nun das Innenministerium Baden-Württemberg als zuständige Datenschutzaufsichtsbehörde auf, gegen die Schufa und Haus & Grund vorzugehen. Die Schufa hat sofort nach Bekanntwerden des Datenmissbrauchs den Vertrag mit der Wohnungsverwaltungs-GmbH fristlos gekündigt. Der Vorstandsvorsitzende der Schufa Rainer Neumann erklärte, die Wohnungsverwaltungsfirma hätte die Daten keinesfalls an Dritte weitergeben dürfen (MieterZeitung 3/2005, 30).

Bayern

Beckstein zur Islamistendatei

Am 30.06.2005 scheiterte eine Bundesratsinitiative zur Schaffung einer gemeinsamen Terrorismusdatei von Polizei und Geheimdiensten (vulgo »Islamistendatei«) am Votum sämtlicher Fraktionen im Bundestag – außer der von CDU/CSU. In der Datei sollten die deutschen Sicherheitsbehörden alle Informationen einstellen und abrufen können, die im Zusammenhang mit dem islamistischen Extremismus und Terrorismus stehen. Zwar unterstützen auch Abgeordnete in den Reihen der rot-grünen Regierungskoalition eine gemeinsame Datei, doch stieß der Bundesratsvorschlag auf zu starke Datenschutzvorbehalte. Der Bayerische Innenminister Günther Beckstein äußerte sich gegenüber der Süddeutschen Zeitung zur bisherigen behördlichen Zusammenarbeit bei der Terrorismusbekämpfung in Lagezentren (vgl. DANA 1/2005, 17) und zur Notwendigkeit einer gemeinsamen Datei:

»Dieses Lagezentrum ist falsch konstruiert. Ich trete dafür ein, die absurde Trennung zwischen dem polizeilichen Zentrum und dem Verfassungsschutz-Zentrum aufzulösen und die Leute auch mit Finanzermittlern enger zusammenarbeiten zu lassen. Und die Islamistendatei, die wir seit Jahren fordern, haben wir immer noch nicht. Wir haben einen Gesetzentwurf vorgelegt, weil Otto Schily sich mit seinem Vorschlag nicht bei den Grünen durchsetzen konnte. Jetzt hat er auf der jüngsten Innenministerkonferenz noch schnell einen neuen Vorschlag für eine Islamistendatei gemacht – doch der kommt bis zur Wahl nicht mehr durch. Auch die FDP wird es sich nicht leisten können, in Zeiten des Terrors die Liberalität über die Sicherheit zu stellen. Die FDP stellt jetzt den Innenminister in Nordrhein-Westfalen. In dem Moment, wo etwas passiert, wäre ein Innenminister, der schöne Reden über die Freiheit der Islamisten schwingt, weg. Wir werden solche Westerwellschen Illusionen nicht zulassen« (Interview mit Annette Ramelsberger, SZ 09./10.07.2005, 2; vgl. SZ 01.07.2005, 5).

Bayern/NRW/Thüringen

Schwule werden polizeilich erfasst

Die Polizeibehörden Bayerns, Thüringens und Nordrhein-Westfalens setzen für ihre elektronische Vorgangsdokumentation eine Software ein, die alle in Straf- und Ermittlungsverfahren verwickelten Personen – also Täter, Opfer und Zeugen – mit ihrer homosexuellen Orientierung registrieren kann. Homosexuelle werden als Tätergruppe klassifiziert und »Aufenthaltsorte von Homosexuellen« als potenzielle Tatorte ausgewiesen, obwohl seit 1994 der Homosexuellen-Paragraf gänzlich aus

dem Strafgesetzbuch gestrichen worden ist. Bei der Eingabe von Ermittlungsergebnissen in die Systeme »IGVP« und »PVP« kann die Polizei die jeweiligen Fälle und die beteiligten Personen mit der Kategorie »homosexuell« zuordnen. Mit dem Kürzel *omosex* ist es den Ermittlern möglich, sämtliche entsprechende Datensätze abzurufen, einschließlich der Personalien der gespeicherten Personen.

Die Datenschutzbeauftragte von Nordrhein-Westfalen Bettina Sokol hält das Verfahren für »höchst bedenklich«, weil Angaben über die sexuelle Orientierung zur Kategorie »besonders schützenswürdiger personenbezogener Daten, die nur unter strengen Voraussetzungen verarbeitet werden dürfen«, gehörten. Nordrhein-Westfalen und Bayern haben das Stichwort »Aufenthaltsort von Homosexuellen« inzwischen zwar sperren lassen. »Homosexuelle« als Tätergruppe bleibt aber nach wie vor gültig. Ein Sprecher des thüringischen Innenministeriums bezeichnet die Software als »historisch überholt« und sieht »Überarbeitungsbedarf«. In einem Schreiben an die Innenminister Thüringens und Bayerns schreibt der Grünen-Bundestagsabgeordnete Volker Beck, die Polizeisoftwares IGVP und PVP ließen »ungute Erinnerungen an die alte polizeiliche Praxis der ›Rosa Listen‹ wach werden«. Im »Dritten Reich« dienten die der Verfolgung von Schwulen. Der Verband lesbischer und schwuler Polizeibediensteter geht davon aus, dass die Speicherung der Daten von Homosexuellen nicht nur in Bayern, Thüringen und Nordrhein-Westfalen üblich ist, sondern auch in anderen Bundesländern (Der Spiegel 30/2005, 13).

Berlin
Diskussion über Überwachung der Moscheen

Als Konsequenz aus den Terroranschlägen von London am 07.07.2005 forderte die CDU-Fraktion im Berliner Abgeordnetenhaus eine nachrichtendienstliche Überwachung der Moscheen. Die Verfassungsschutzbehörde müsse, so Andreas Gram für die Fraktion, »mit allen ihr zur Verfügung stehenden rechtsstaatlichen Mitteln herausfinden, was in den Moscheen vor sich geht und wie viele gewaltbereite Islamisten in Berlin leben. Dass der Berliner Verfassungsschutz eine Überwachung von Moscheen, die nicht unbedingt als Nährboden für den gewaltbereiten Islamismus bekannt sind, ablehnt, ist nicht akzeptabel.« Zuvor hatte der Vorsitzende der Gewerkschaft der Polizei (GdP), Konrad Freiberg, eine verstärkte Beobachtung im Umfeld von Moscheen befürwortet. Es gehe nicht um einen Generalverdacht, doch gebe es »gewisse Moscheen«, in denen es zu einer »Selbstradikalisierung« komme.

Innensenator Ehrhart Körting (SPD) hatte die Zahl der Islamisten in Berlin zuvor mit etwa 4000 beziffert, nahezu 3000 davon seien in der als nicht gewaltbereit eingestuften türkischen Organisation Milli Görüs organisiert. Auch die Übrigen kämen nach den aktuellen Erkenntnissen nicht als Attentäter in Betracht. Für ihn ist die Forderung schärferer Moscheen-Überwachung, die unterstellt, von jeder Moschee gehe eine Gefahr für die öffentliche Sicherheit aus, »schlicht verfassungswidrig«. Ihn überrasche eine derartige Forderung z.B. von dem »gesetzestreuen Innenminister von Bayern«, also Günter Beckstein (CSU). Die Aufgaben des Verfassungsschutzes seien klar geregelt. Beckstein forderte die Überwachung mit V-Leuten: »Wir müssen wissen, was in jeder Moschee passiert«. Erstaunlich ist, dass auch unter Moslems die Forderung nach Videoüberwachung Befürworter findet. Anders als der Islam-Rat sprach sich der Zentralrat der Muslime für gezielte Videoüberwachung in Moscheen aus (SZ 19.07.2005, 6; dpa 19.07.2005; Zurawski www.heise.de 21.07.2005).

Brandenburg
Schönbohm droht Lafontaine mit Verfassungsschutz

Brandenburgs Innenminister Jörg Schönbohm hat Oskar Lafontaine damit gedroht, ihn wegen seiner populistischen Äußerungen durch den beamteten Verfassungsschutz beobachten zu lassen. Der Spitzenkandidat des Linksbündnisses (WASG und PDS) bei der Bundestagswahl suche »offenbar bei den Neo-Nazis seine Wähler«. Wenn Lafontaine weitermache, »könnte das ein Fall für den Verfassungsschutz werden«, meinte der CDU-Politiker Schönbohm gegenüber der Bild-Zeitung. Der »Sozialist« suche »offenbar bei den Neonazis seine Wähler«. Er bezog sich dabei auf Äußerungen Lafontaines, wonach die Nationalsozialisten in erster Linie rassistisch, aber nicht fremdenfeindlich gewesen seien. Führende PDS-Politiker bekräftigten ihre Kritik an der »Fremdarbeiter«-Äußerung Lafontaines, ohne aber die Tätigkeit des Verfassungsschutzes einzufordern. WASG-Sprecher Murat Cakir meinte: »Das ist völliger Unsinn«. Die Drohung Schönbohms gehöre zu den »Schmutzkampagnen«, die gegen das Linksbündnis gestartet würden: Anstatt den politischen Gegner zu diffamieren, solle »Schönbohm seiner Aufgabe als Verfassungsminister gerecht werden«. Lafontaine bekräftigte die Absicht, auch im rechten Wählerspektrum zu wildern. Dazu brauche man keine rechte Terminologie: »Man muss nur glaubwürdig die Rechte der Arbeitnehmer vertreten, und die wollen im Fall der Arbeitslosigkeit nicht mit solchen asozialen Bedingungen konfrontiert werden, wie sie durch Hartz IV geschaffen wurden« (www.spiegel.de 05.07.2005).

Sachsen-Anhalt
Von Bose warnt vor übereilten Anti-Terror-Gesetzen

Nach der Terroranschlägen vom 07.07.2005 in London hat der Landesbeauftragte für den Datenschutz von Sachsen Anhalt, Harald von Bose, eindringlich vor übereilten Forderungen nach verschärften Gesetzen in Deutschland gewarnt: »Die Anschläge eignen sich nicht, um hektisch und aktionistisch zusätzliche Sicherheitsmaßnahmen zu beschließen.« Sicherheitslücken seien nicht erkennbar. Teile der CDU/CSU und Kriminalisten hatten sofort nach den Anschlägen schärfere Gesetze und mehr Ermittlungsrechte gefordert.

Von Bose rief die Politik auf, sich stärker mit den Ursachen des Terrorismus zu beschäftigen: »Sicherheit, die allein auf Polizei, Verfassungsschutz und weitere Sicherheitsdienste abstellt, wird nicht zum Ziel führen.« Im Kampf gegen den Terror dürften nicht die Wurzeln des Rechtsstaates beschädigt werden. Der Kern des Privatlebens müsse vor staatlichen Eingriffen verschont bleiben. Daher müsse auch bei der geplanten Änderung des Verfassungsschutzgesetzes in Sachsen-Anhalt

behutsam vorgegangen werden (www.heise.de 11.07.2005).

Nordrhein-Westfalen

Krebsregister nimmt Arbeit auf

Vom 01.06.2005 nahm in Münster das Krebsregister des Landes Nordrhein-Westfalen seine Tätigkeit auf. Über das Register – angeblich das europaweit größte Krebsregister Europas – sollen mögliche regionale Häufungen von Krebserkrankungen oder deren verstärktes Auftreten in bestimmten Altersgruppen erforscht werden. Gespeist wird die Datenbank mit Informationen aus Kliniken und Arztpraxen auf Grund einer Meldepflicht zu Krebsart, Krankheitsstadium, Alter, Geschlecht. Die Daten seien, so Hans-Werner Hense vom Universitätsklinikum Münster, doppelt verschlüsselt, so dass niemand befürchten müsse, dass Informationen in falsche Hände gerieten (SZ 31.05.2005, 11).

Schleswig-Holstein

Mit Handy-Großfahndung gegen Serien-Brandstifter

Die Segeberger Polizei hat 700 Menschen, die über Handy innerhalb eines mehrere Kilometer großen Umkreises um den abgebrannte Jawoll-Markt an der Lindhofstraße geortet worden waren, schriftlich aufgefordert, sich als ZeugInnen zu melden und einen beigelegten Fragebogen auszufüllen, der als »Zeugen-Anhörung« deklariert ist mit der Überschrift »Die Kriminalpolizei bittet um ihre Mithilfe«. Gefragt wird u.a.: »Wo haben Sie sich bzw. der Handy-Nutzer in der o.g. Nacht in der Zeit von 00:00 – 03:00 aufgehalten? Frage 2 enthält den warnenden Zusatz: »Angaben können gegebenenfalls technisch nachgeprüft werden!«

Betroffene sind verunsichert, inwieweit sie jetzt als Beschuldigte der Brandstiftung angesehen werden und ob sie einen Rechtsanwalt nehmen müssen. Der Ermittlungsleiter Alexander Koplin riet davon ab, die Fragebögen einfach zu ignorieren: »Wenn gar keine Rückmeldung kommt, werden wir von uns aus den Kontakt zum Betreffenden suchen.« Die Angeschriebenen waren in der Nacht des 04. auf den 05.06.2005 mit ihrem eingeschalteten Gerät geortet worden, als sie sich in der Nähe des abgebrannten Segeberger Restepostenmarktes aufgehalten hatten. Das Feuer soll von einem Serienbrandstifter gelegt worden sein. Ein Richter des Amtsgerichts Segeberg hatte die Großfahndung genehmigt. Der Leiter der polizeilichen Ermittlungsgruppe, Ralf Lorenzen, erklärte: »Unser Ziel bei dieser Brandserie ist die Ermittlung des Täters.« Die angeschriebenen Personen seien wichtige Zeugen. Geortet wurden die Personen, die angerufen worden sind oder angerufen haben. Sollte jemand das Schreiben nicht zurücksenden, so habe dies keine Rechtsfolgen. Bisher gebe es aber eine sehr hohe Rücklaufquote.

Der stellvertretende Datenschutzbeauftragte des Landes Schleswig-Holstein Johann Bizer kritisierte die Aktion als unverhältnismäßig. »Es werden Datenbanken angelegt, in denen die betroffenen Personen gespeichert sind.« Solange der Fall nicht aufgeklärt sei, würden die betroffenen Personen auch gespeichert bleiben. »Jeder, der in dem Umkreis des Brandherdes mit seinem Handy telefoniert hat, wird zwar formal nur als Zeuge vernommen, ist aber quasi Verdächtiger.« Alle Betroffenen hätten die Möglichkeit, Beschwerde beim Landgericht gegen das Vorgehen einzulegen (Kieler Nachrichten 06.08.2005, 6; Beck Segeberger Zeitung nordclick/sz 02.08.2005).

Ausländische Datenschutznachrichten

Europa

Datenschutzzuständigkeit geht über auf »Freiheit, Justiz und Sicherheit«

In einer wenig beachteten Entscheidung der Europäischen Kommission vom 11.02.2005 ging die Zuständigkeit für Datenschutz von der Generaldirektion (GD) Binnenmarkt auf die Generaldirektion »Freiheit, Justiz und Sicherheit« über. Es erfolgte keine Anhörung der nationalen Parlamente oder des Europäischen Parlaments. Die GD Binnenmarkt war für den Datenschutz seit den 80er Jahren verantwortlich und erarbeitete viele Datenschutzvorschläge, u.a. die EU-Datenschutzrichtlinie von 1995, die sich auf die erste Säule der EU bezogen. Der EU-Rat setzte im Jahr 1997 für die dritte Säule (Innen- und Justizpolitik) zum Datenschutz eine Arbeitsgruppe ein, die im April 2001 wieder abgeschafft wurde. Im Memorandum zur Entscheidung der Kommissionsentscheidung vom 11.02.2005 wird diese wie folgt erklärt: »Um die Kohärenz und die Erkennbarkeit der Kommissionsaktivitäten im Bereich des Datenschutzes zu stärken, schlagen die Kommissare Frattini und McCreevy vor, die Verantwortlichkeit von der GD Binnenmarkt auf die GD Freiheit, Justiz und Sicherheit zu übertragen. Dies berücksichtigt, dass die Aktivitäten zunehmend sowohl in den Bereich der ersten wie der dritten Säule fallen und damit in den Verantwortungsbereich der GD Freiheit, Justiz und Sicherheit.«

Die Bürgerrechtsorganisation Statewatch sieht in der Veränderung einen »Putsch«: Derzeit erfolgten in der EU eine Vielzahl von Entscheidungen über die Sicherheitspolitik unter der Rubrik »Bekämpfung des Terrorismus«, die die Bürgerrechte völlig missachteten. Nach dem »Prinzip der Verfügbarkeit« sollten alle national verfügbaren personenbezogenen Daten den Sicherheitsbehörden aller anderen EU-Staaten zugänglich gemacht werden. Der Kommentar von Tony Bunyan von Statewatch: »Die EU ist auf dem Weg zu einer Big-Brother-Gesellschaft, in der Sicherheitsbehörden Zugang zu gewaltigen Datenbanken mit persönlichen und intimen Daten haben, bei denen Datenschutz nicht diesen Namen wert ist. Wird nun diese Aufgabe der Generaldirektion übertragen, die sich für das ›Prinzip der Verfügbarkeit‹ einsetzt, so bedeutet dies, den Wolf ins Schafsfell zu stecken. Eine Abteilung in dieser Generaldirek-

tion soll die Bürgerrechte sichern, am anderen Ende des Korridors wird eine andere dafür sorgen, dass diese Bürgerrechte nicht dem ›Prinzip der Verfügbarkeit‹ im Weg stehen. Dies führt zwangsläufig zu einem nicht akzeptablen Interessenkonflikt« (statewatch vol 15 no 2 March-April 2005, 1).

Europa

Gegenseitiger Zugriff auf nationale Sicherheitsregister

Deutschland und sechs weitere Staaten haben sich den gegenseitigen Zugriff auf nationale DNS-Datenbanken, Fingerabdruck-Sammlungen und Kfz-Register zugesichert. Die Innen- und Justizminister von Belgien, Deutschland, Frankreich, Luxemburg, den Niederlanden, Österreich und Spanien unterzeichneten einen entsprechenden Vertrag am 27.05.2005 in Prüm. Der Vertrag muss noch von den nationalen Parlamenten ratifiziert werden.

Europa

Wird SIS II zur »panoptischen Überwachungsmaschine«?

Die britische Bürgerrechtsorganisation »statewatch« warnt in einer Analyse vor dem Ausbau des EU-weiten Fahndungssystems Schengen-Informationssystem (SIS) zu einer »Big-Brother-Datenbank«: »Dieses System wird benutzt werden, um Millionen vom EU-Gebiet auszuschließen, Überwachung und Kontrolle über die verdächtige Bevölkerung auszuüben und um ein biometrisches Register aller Einreisenden in die EU ähnlich dem US-VISIT-Programm zu schaffen«. Das 1995 eingeführte SIS drohe Schritt für Schritt zu einer gewaltigen »panoptischen Maschine« und zu einem der »repressivsten politischen Instrumente der Moderne« ausgebaut zu werden. Das aktuelle SIS, dem 13 EU-Mitgliedstaaten sowie Norwegen und Island angeschlossen sind, platzt aus allen Nähten. Nach erfolgreicher Volksabstimmung wird sich auch die Schweiz am SIS beteiligen. Mitte 2003 waren in dem computergestützten Grenzkontrollsystem 15 Mio. Einträge gespeichert. Neben Vermerken über gestohlene oder verlorene Identitätsdokumente bezogen sich über ein Million der Datensätze auf Personen. Die Mehrheit davon betraf mit 780.922 Datensätzen Warnhinweise zu Personen, denen der Eintritt in das Schengen-Gebiet verwehrt werden soll. ¾ dieser Daten stammen aus Italien und Deutschland.

Das SIS der nächsten Generation soll alle 25 EU-Mitgliedstaaten erfassen und 2007 fertiggestellt sein. Geplant sei die Einfügung neuer Datenkategorien, insbesondere biometrische Daten wie das digitalisierte Gesichtsbild, sowie einfache und genetische Fingerabdrücke. Diese Entwicklung müsse im Kontext der drohenden zwangsweisen biometrischen Erfassung der rund 450 Mio. EU-BürgerInnen im Zuge der Einführung neuer Pässe und Ausweise sowie aller Visa-Antragsteller gesehen werden. Es bestehe zwischen den EU-Regierungen Einigkeit, dass die Fingerabdrücke mit denen Verdächtiger und aus Tatortspuren abgeglichen werden sollen. Statewatch erwartet die Aufnahme von personengebundenen Warnhinweisen wie »gewalttätige Unruhestifter«, »Terrorismusverdächtiger«, »Clan-Mitglieder«, »verdächtige Angehörige einer kriminellen Vereinigung« oder von »illegalen Einwanderungsnetzwerken«. Neben Europol und der EU-Staatsanwaltsinstanz Eurojust sollen immer mehr nationale Strafverfolgungsbehörden Zugang zu den Datenbeständen selbst »für andere Zwecke« erhalten, was eine Nutzung für Geheimdienste wahrscheinlich mache.

Argwöhnisch macht die Bürgerrechtler, dass das sich ebenfalls im Aufbau befindliche Visa-Informationssystem (VIS) bzgl. »zentralisierter Architektur«, »gemeinsamer technischer Plattform« und »Interoperabilität« von SIS II nicht wesentlich unterscheiden soll. Zwar sei vom EU-Rat offiziell zu hören, dass es sich um »zwei unterschiedliche Systeme mit strikt getrennten Daten und Zugang« handeln werde, doch sei dies angesichts der technischen Parallelität wenig glaubwürdig. Die neue Überwachungsarchitektur werde bereits von einem gemeinsamen Konsortium entwickelt, ohne dass das Europäische Parlament (EP), nationale Volksvertretungen oder Datenschutzbehörden konsultiert worden sind. Der EU-Rat habe keine rechtliche Prüfung vorgenommen. Im Rahmen eines abgekarteten »Furcht erregenden« Spiels würden Fakten geschaffen, die sich kaum noch rückgängig machen ließen. Erste Regelungsvorschläge hat die Kommission erst Anfang Juni 2005 vorgelegt. Danach soll das EU-Parlament nur bzgl. eines Bereichs der Datenbank etwas zu sagen haben: dem der Visa-Vergabe, da für den gesamten Bereich der Justiz- und Polizeipolitik nur eine »Konsultation« des Parlaments vorgesehen ist. Dies ist für die Berichterstatterin im EP, die britische Liberale Sarah Ludford, eine »unmögliche Situation«: »Wir können nicht nur über einen Teil der neuen Datenbank abstimmen, ohne nicht auch die anderen Funktionen zu prüfen« (Krempl www.heise.de 21.05.2005; Bolesch SZ 02.06.2005, 5; das PDF-Dokument der statewatch-Analyse ist zu finden unter http://www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf).

Europa

Deutschland zahlt Caroline 115.000 Euro Schadenersatz wegen Pressefotos

Weil sie die Veröffentlichung von Pressefotos aus ihrer Privatsphäre nicht gesetzlich verhindert hat, muss die deutsche Bundesregierung insgesamt 115.000 Euro Schadenersatz an Caroline von Hannover zahlen. Aufgrund einer außergerichtlichen Einigung erhält sie 10.000 Euro zum Ausgleich immaterieller Schäden sowie 105.000 Euro Kostenerstattung, gab der Europäische Gerichtshof für Menschenrechte in Straßburg bekannt.

Die Veröffentlichung der Fotos, die Caroline im Alltagsleben beim Einkaufen, Reiten und Radfahren zeigten, war vom Bundesverfassungsgericht für Rechtens erklärt worden, soweit nicht auch ihre Kinder mit abgelichtet waren. Bei ihr als absoluter Person der Zeitgeschichte sei die Pressefreiheit und das Interesse der Öffentlichkeit, zu erfahren, wie sie sich im Alltagsleben verhält, höher zu bewerten als ihr Recht am eigenen Bild und auf ihre Privatsphäre.

Die Straßburger Richter jedoch bewerteten Carolines Recht auf Achtung ihres Privatlebens nach Artikel 8 der Europäischen Menschrechtskonvention höher als die durch Artikel 10 der Konvention garantierte Freiheit der Meinungsäußerung. Ein legitimes Interesse der Öffentlichkeit am Privatleben der Prinzessin konnten sie nicht erken-

nen. Das Kriterium der deutschen Gerichte, zwischen »absoluten« und »relativen« Personen der Zeitgeschichte zu unterscheiden, sei nicht geeignet, einen wirksamen Schutz des Privatlebens von Caroline zu erreichen (AFP / yahoo 28.07.2005; BVerfG, 1 BvR 653/96 vom 15.12.1999; Europäischer Gerichtshof für Menschenrechte, 59320/00, 24. Juni 2004).

Europa
EU-Kommission will alle Überweisungen kontrollieren

Am 26.07.2005 legte der EU-Innenkommissar Charlie McCreevy den Entwurf einer EU-Verordnung vor, der vorsieht, dass bei allen Geldüberweisungen in die Europäische Union (EU) sowie bei Transfers aus der EU heraus die Auftraggeber verpflichtet werden sollen, Kontonummer, Name und Adresse anzugeben. Die Kreditinstitute sollen verpflichtet werden, die Daten fünf Jahre lang aufzubewahren und an Polizei und Justiz herauszugeben, wenn sie zur Bekämpfung von Terrorismus oder Geldwäsche benötigt würden. Die Vorschriften sollen unabhängig von der Höhe des überwiesenen Betrages gelten, erläuterte eine EU-Beamtin: »Auch mit kleinen Summen kann Terrorismus finanziert werden.« Bisher müssen die Überweisenden Adresse und Name nur auf Anfrage der empfangenden Bank mitteilen. Regelmäßig genügt die Kontonummer, so dass die Empfängerbank nicht weiß, wer das Geld geschickt hat. Nach Art. 5 können aber künftig Geldüberweisungen aus der EU an Begünstigte in Drittländern, die nicht über 1000 Euro hinausgehen, weniger streng überprüft werden, sofern kein Terrorverdacht besteht. Eine zu strenge Kontrolle würde v.a. denjenigen Menschen Probleme bereiten, die illegal in der EU leben und mit Geldüberweisungen ihre Angehörigen im Ausland unterstützen. Die Verordnung setzt u.a. die internationalen Empfehlungen der Financial Action Task Force (FATF) um, die 1989 von den G-7-Industriestaaten zur weltweiten Bekämpfung der Geldwäsche eingesetzt wurde. Das die Präsidentschaft innehabende Großbritannien will den Verordnungsentwurf bis Ende 2005 im EU-Finanzministerrat beschließen. Das Europaparlament muss zustimmen. Im Jahr 2007 soll die Verordnung dann in den Mitgliedsstaaten umgesetzt werden.

Die Überwachung der Geldtransfers ist Teil des EU-Aktionsplans zur Terrorismus-Bekämpfung, der nach den Terroranschlägen vom 11.09.2001 beschlossen wurde und seitdem regelmäßig ergänzt wird. Im Rahmen dieses Plans sollen auch Finanzströme, über die Terroranschläge bezahlt werden, unterbunden werden. Nach den Attentaten von London am 07.07.2005 waren Mitgliedstaaten erheblich unter Druck geraten, weil viele der von der Gemeinschaft geforderten Anti-Terror-Maßnahmen nur schleppend umgesetzt wurden. Auf einem Sondergipfel nach den Londoner Anschlägen wurde außerdem eine EU-Verordnung beschlossen, mittels derer Geldbewegungen an den EU-Grenzen überwacht werden können sollen. Diese EU-Verordnung wurde Anfang Juni vom EU-Parlament angenommen. Demnach müssen Bargeldsummen im Wert von 10.000 Euro oder mehr bei der Einreise in die EU angegeben werden. Gleiches soll für Schecks oder andere leicht in Bargeld umtauschbare Zahlungsmittel gelten. Die so gesammelten Daten sollen im Verdachtsfall zwischen den EU-Staaten ausgetauscht werden. 18 Monate nach Zustimmung des EU-Ministerrats tritt die Verordnung in Kraft.

Zudem soll die bereits beschlossene Neufassung der Geldwäscherichtlinie schnellstmöglich umgesetzt werden. Darin ist vorgesehen, dass nicht nur Banken und Finanzdienstleister, sondern auch Rechtsanwälte, Notare, Immobilienmakler und Kasinobetreiber verpflichtet werden, bei allen Transaktionen über 15.000 Euro die Kundenidentität festzustellen und sich sofort an die Behörden zu wenden, wenn sie jemanden verdächtigen, Finanzströme zu verschleiern oder Terrorakte finanzieren zu wollen. Die Mitgliedstaaten müssen die Richtlinie bis 2007 umgesetzt haben (Seith www.spiegel.de 26.07.2005; Bolesch, SZ 27.07.2005, 6, 20).

Deutschland/Großbritannien
Schüler unter Videoüberwachung

An einer privaten Grundschule in Großbritannien werden die Kinder permanent von einem guten Dutzend Kameras überwacht. Ob beim Spielen oder Lernen, ob im Klassenzimmer oder in der Turnhalle – das Videoband läuft immer mit. Die Eltern lassen sich die Überwachung einiges kosten, insgesamt 3000 Euro jährlich. Dafür können sie sich jederzeit ins Intranet der Schule einloggen und beobachten, was ihr Kind gerade macht. Nach Ansicht der Schulleiterin hat das Projekt pädagogischen Nutzen: »Wir haben den Schülern erklärt, dass wir das Videomaterial Papa und Mama zeigen, wenn sie nicht brav sind.«

Zwar gibt es in deutschen Schulen keine solche Rundumkontrolle, doch hält auch hier die Videoüberwachung in den Schulen Einzug. In der Handelsschule Berliner Tor in Hamburg, einem Brennpunkt von Vandalismus, Farbschmierereien und ähnlichen Problemen, sind 14 Kameras installiert, die das Geschehen in und um Klassenräume beobachten. Gemäß Angaben des Schulleiters Heinz Fänders würden auf dem Pausenhof »Rauschgift-Depots« angelegt, Dutzende nagelneue Laptops gestohlen und zuweilen betätigten sich Schüler auf dem Gelände als Zuhälter: »Da fahren 18jährige im Mercedes vor, holen Mädchen ab und bringen sie zu irgendwelchen Freiern.« Seit Beginn der Überwachung seien solche Vorfälle weniger geworden. Das Lehrerkollegium unterstütze daher die Videoüberwachung einmütig, ebenso wie die meisten Schüler. In einer anderen Hamburger Förderschule, Endstation für viele Jugendliche ohne Hauptschulabschluss, hat es zuletzt durch Vandalismus auf dem Pausenhof und im Schulgebäude monatlich einen Schaden von rund 10.000 Euro gegeben. Nun wachen 5 Kameras vor besonders gefährdeten Räumen, was die Schule zwischen 3000 und 4000 Euro kostete, aber zur Beruhigung in der Schule geführt haben soll.

An der Kreuzberger Friedrich-Jahn-Hauptschule in Berlin sollen 8 Kameras für mehr Sicherheit auf den beiden Schulhöfen sorgen. An der Heinrich-Mann-Gesamtschule habe es, so Schulleiter Detlev Arndt, Probleme mit ehemaligen Schülern gegeben, »bis Kameras installiert wurden«. Angesichts solcher Erfolgsgeschichten unterstützt der Verband Bildung und Erziehung (VBE) die technische Überwachung. Nach Ansicht des Bundesvorsitzenden Ludwig Eckinger ist Videoüberwachung ein geeignetes Mittel, um die zunehmende Gewalt »als Phänomen annehmen« zu können. Zugleich müsse man jedoch »aufklären, Vertrauen aufbauen und mit Gewalttätern reden«. Der Bundeselternrat ist skeptischer, gemäß dem Vor-

sitzenden Wilfried W. Steinert: »Auch das Massaker am Gutenberg-Gymnasium in Erfurt wäre mit Videoüberwachung nicht verhindert worden.« Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Peter Zimmermann, betont denn auch, dass es an Schulen keine Rundum-Kontrolle geben dürfe. Nur in Ausnahmefällen sei Videoüberwachung erlaubt, und auch das nur dann, wenn Alternativen zuvor wirkungslos geblieben seien. Eckinger bestätigt: »Für den Seelenzustand der Schüler ist eine permanente Überwachung mit Kameras ein Horrorszenario« (Schmilewski, SZ 04.07.2005, 11).

Frankreich

Biometrische Ausweis-Chipkarten geplant

Februar 2005 präsentierte der damalige französische Innenminister Dominique de Villepin einen Gesetzentwurf zur Einführung einer neuen Identitäts-Chipkarte mit einem Chip, auf dem u.a. biometrische Daten gespeichert werden (Gesicht, Iris, digitales Foto und Fingerabdrücke), Schlüssel zum Absichern von Daten, digitale Signaturen und Authentisierungmittel. Das INES-Programm (Programm für eine sichere nationale elektronische Identität) soll Anfang 2007 mit der Einführung neuer ID-Karten beginnen. Die seit 1955 in Frankreich abgeschaffte Ausweispflicht soll bei dieser Gelegenheit wieder eingeführt werden. Die Kosten des Dokuments soll die Bürgerin bzw. der Bürger selbst tragen. Als Ziel des Programms wird die Bekämpfung von Straftaten, illegaler Einwanderung, Identitätsdiebstahl und Terrorismus angegeben. Mitglieder der Commission Nationale de l´Informatique et de la Liberté (CNIL – Kommission für Informationstechnik und Freiheitsrechte – die französische Datenschutzbehörde) äußerten schon schwere Bedenken, bevor sie um eine offizielle Stellungnahme gebeten wurden. CNIL-Kommissionsmitglied Francois Giquel: »Die ID-Karte ist nicht nur ein Dokument oder ein geheimer Schlüssel; vielmehr wird ein hochpersönlicher Teil des eigenen Körpers zum Identifikationsmittel. Wenn Menschen zum Nachweis ihrer Identität ihr Auge, ihren Finger oder ihr Gesicht zur Verfügung stellen müssen, werden sie lebenslang markiert – dies ist eine soziale Revolution.«

Zur Verhinderung des Datenmissbrauchs sollen die Informationen in getrennten großen Datenbanken gespeichert werden. Dessen ungeachtet vertritt Alain Weber von der Liga für Menschenrechte (LDH – Ligue des Droits de l´Homme) die Ansicht, dass die Datentrenung durch die Verknüpfungsmöglichkeit neutralisiert werde. Das frühere CNIL-Mitglied Louis Jonet stellte fest, dass die Existenz einer solchen Datenbank zwischen 1940 und 1945 es manchem Juden unmöglich gemacht hätte, sich den Zusammentreibungen zu entziehen. Das INES-Programm wurde vom 01.02.2005 an öffentlich zur Diskussion gestellt und zog sich die Kritik von vielen Nichtregierungsorganisationen (NGO) zu. Sechs dieser Gruppen veröffentlichten am 26.05.2005 eine gemeinsame Stellungnahme mit dem Titel »INES – vom Verdacht zum allgemeinen Bewegungsprofil«. Mit einer offenen Unterschriftsliste forderten sie die Rücknahme des Programms. Der Gesetzentwurf wurde am 11.04.2005 von einem interministeriellen Komitee angenommen, noch bevor die öffentliche Anhörung beendet war. Es gehe, so die NGO-Stellungnahme, »weniger um eine offene Diskussion als um die Bestätigung schon getroffener Regierungsentscheidungen.« Das Schwergewicht des Entwurfes liege in Detailfragen zur Freiwilligkeit und zu den Kosten und nicht in der Frage nach der Notwendigkeit einer solchen Karte.

Identitätsdiebstahl und Terrorismus würden der ID-Karte nur als Alibi dienen. Es gebe keine Untersuchung über das Ausmaß der tatsächlichen Probleme. Zur Terrorismusbekämpfung sei das Mittel ungeeignet, da die Mehrzahl der terroristischen Angriffe von »Menschen durchgeführt wurden, die ihre tatsächliche Identität genutzt haben«. Identitätskontrollen würden massiv ausgeweitet und trivialisiert. Die verschiedenen Funktionen (zum Erhalt unterschiedlicher Dienstleistungen), die den Nutzenden vom Innenministerium als »Komfort« verkauft würden, könnten darin enden, dass sie gesetzlich verpflichtend werden; Verweigerer erhielten den Status von »Bürgern zweiter Klasse«. Die Stellungnahme warnt vor einem allgemeinen Gebrauch der neuen elektronischen ID-Karte, da dies zum Entstehen einer »übermäßigen Datenbank der gesamten französischen Bevölkerung« führen würde. Die Einrichtung der Fingerabdruckdatenbank würde dazu führen, dass die Zahl der Personen, die irrigerweise in Strafermittlungen hineingezogen werden, wegen der Ungenauigkeit der technischen Erkennungsverfahren zunehmen werde (Statewatch March-April 2005 vol 15 no 2, 8; vgl. http://www.ldh-france.org).

Großbritannien

Satelliten-PKW-Maut geplant

Das britische Verkehrsministerium hat Pläne für ein über Satelliten überwachtes PKW-Maut-System veröffentlicht. Danach soll jede zurückgelegte Meile erfasst werden; die Höhe der Maut soll von der Beliebtheit der Strecke und der Tageszeit abhängen. Wer zu Spitzenzeiten auf Staustrecken fährt, soll bis zu 1,34 Pfund bezahlen. Die erforderliche Technik soll bereits in großen Teilen bestehen. Lastwagen sollen schon ab 2007 zur Kasse gebeten werden. Die deutsche Telekom-Tochter T-Systems nimmt an der Ausschreibung um das britische Mautsystem – unterstützt von Toll-Collect – teil (Der Spiegel 24/2005).

Großbritannien

Weltweite Terrorismusdatenbank angekündigt

Die britische Regierung will mit einer weltweiten Extremistenliste gegen die Terrorgefahr im eigenen Land angehen. Innenminister Charles Clarke kündigte am 20.07.2005 vor dem Unterhaus an, eine Datenbank über Personen auf allen Erdteilen zu erstellen, die in Predigten, im Internet oder in Artikeln zum Terrorismus aufstacheln. Diejenigen, die auf dieser Liste stehen, könnten an der Einreise nach Großbritannien gehindert werden. Ausländer, die bereits im Land sind, könnten ausgewiesen werden (www.heise.de 20.07.2005).

Italien

Verschärfung der Anti-Terror-Gesetze

Nach den Anschlägen in London am 07.07.2005 bereitete die italienische Regierung umgehend eine Verschärfung ihrer Anti-Terror-Gesetze vor. Am 22.07.2005 wurde das Maßnahmenpa-

ket verabschiedet. Innenminister Guiseppe Pisanu setzte eine neue Regelung durch, wonach Terrorverdächtige auch ohne Anklage über längere Zeit festgehalten werden können. Die Dauer für vorläufige Festnahmen wurde von 12 auf 24 Stunden verlängert.

Italien sei ein denkbares Ziel von Anschlägen. Kurz nach den Attentaten in London hatte eine islamistische Gruppe die italienische und die dänische Regierung gewarnt, »dass sie die gleiche Strafe erhalten werden, wenn sie ihre Truppen nicht aus dem Irak und Afghanistan zurückziehen«. Zu dem Anti-Terror-Paket gehören weitgehendere Ermittlungsbefugnisse, u.a. eine striktere Telefon- und Internetüberwachung, zur Identifizierung von Verdächtigen die Zwangs-Entnahme von Speichel oder Haaren, die Schaffung einer Zentralbehörde zur Koordination der Ermittlungen sowie größere Polizeikompetenzen bei Razzien (SZ 13.07.2005, 7; SZ 23./24.07.2005, 8).

Österreich

Datenschutzkommission (wieder-) ernannt

Die Amtszeit der Österreichischen Datenschutzkommission endete am 30.06.2005. Vom Österreichischen Präsidenten wurden für weitere fünf Jahre folgende Mitglieder auf Vorschlag der Österreichischen Regierung (wieder-) benannt: Vorsitzender Dr. Anton Spendling, Geschäftsführerin Dr. Waltraut Kotschy, Mag. Helmut Hutterer, Dr. Claudia Rosenmayr-Klemenz, Dr. Ludwig Staudigl, Mag. Daniela Zimmer. Als Stellvertretende wurden benannt: Dr. Gerhard Kuras (Vorsitz), Dr. Eva Souhrada-Kirchmayer (Geschäftsführung), Dr. Michaela Blaha, Dr. Klaus Heissenberger, Mag. Huberta Maitz-Strassing, Mag. Joachim Preiss. Dem bisherigen Vorsitzenden Dr. Maier folgte also sein bisheriger Stellvertreter Dr. Spendling.

Polen/Vatikan

Dominikanerpater bespitzelte wohl Papst

Das polnische Institut für das Nationale Gedächtnis (IPN), das die Akten der polnischen Stasi SB verwaltet, hat den in Polen bekannten Dominikanerpater Konrad Hejmo als den Spitzel im Vatikan entlarvt, über den die Medien schon lange spekulierten. Hejmo leitete dort langjährig das große polnische Pilgerheim. Vor dem Tod Johannes Pauls II. war er fast täglich im Fernsehen zu sehen, wie er als »enger Freund des Papstes« zum Himmel schauend und mit gefalteten Händen salbungsvoll die aktuelle Entwicklung in den Gemäuern des Vatikans schilderte. Nach dem Tod Johannes Pauls II. gab er Interview um Interview.

Nun eröffnete Anfang Mai 2005 IPN-Direktor Leon Kieres, ein sonst eher zurückhaltender Rechtsprofessor: »Das IPN hat sich nach Abwägung aller Umstände entschlossen mitzuteilen, dass der Agent in der Nähe des Heiligen Vaters kein anderer war als Pater Konrad Hejmo.« Da Kieres die Beweise nicht sofort vollständig vorlegen konnte, brachte er Politiker und Publizisten gegen sich auf, die ihm vorwarfen, einen verdienten Priester an den Pranger zu stellen und die Trauerstimmung und das Gedenken an den verstorbenen Papst abrupt zerstört zu haben. Kieres hatte die frühe Aufdeckung damit begründet, dass bereits zwei andere bekannte Priester verdächtigt wurden, SB-Agenten im Vatikan gewesen zu sein. Ermutigt durch die heftige Kritik an Kieres, wehrte sich Hejmo: »Das ist eine böse Intrige.« Dessen Ordensoberen baten schließlich um Einsicht in die IPN-Materialien, die inzwischen ins Internet gestellt worden sind. Daraus ergibt sich, dass Hejmo seit Mitte der 70er Jahre der Kirchenabteilung des SB berichtet hat, u.a. gegen Geld, exklusive Alkoholika und ein »Stadtpanorama von Warschau in Metall und Plastik«. Als Hejmo vor mehr als 20 Jahren zur Betreuung polnischer Vatikan-Pilger nach Rom abgeordnet wurde, berichtete er weiter – allerdings dieses Mal für den deutschen Auslandgeheimdienst BND (Bundesnachrichtendienst). Zumindest gab sich sein neuer Führungsoffizier als Mann des BND aus. Hejmo bekam für seine Berichte Geld, über die Jahre hinweg knapp 20.000 Deutsche Mark, was er auf deutschsprachigen Formularen quittierte. Als Mitte Mai 2005 die ersten Nachrichten hierüber an die Presse durchgesickert waren, meinte Hejmo, es habe sich öfter mit einem deutschen Doktoranden zu einem Kaffeehausplausch getroffen. Wenig später tauchte der Mann mit dem schlohweißen Haar und der wehenden Kutte unter und verkündete in einer langen Erklärung, er sei »Opfer des selbstgerechten IPN. Man habe ihn »guillotiniert« und eine »Riesenspionageaffäre konstruiert«: »Dabei war ich nur, vielleicht in naiver Weise, offen für die Menschen« (Urban, SZ 08.06.2005, 11).

Schweiz/Cayman Islands

Daten reicher Bankkunden entwendet

Der Redaktion der Schweizer Wirtschaftszeitung Cash wurden vollständige Datensätze über vermögende KundInnen einer Tochter der renommierten Schweizer Bank Julius Bär anonym zugespielt. Die Daten waren bei der Bär-Tochter auf den Cayman Islands verwahrt worden. Gemäß einem Julius-Bär-Sprecher »handelt es sich um ältere Daten aus den Jahren 1997 bis 2003«. Die CD mit den Daten gibt Auskunft über Julius-Bär-KundInnen aus der ganzen Welt, über interne Konten und Protokolle von Manager-Treffen. Auf Cayman Islands würden v.a. die Kunden aus aller Welt betreut, die besonderen »Diskretionsschutz« wünschten: »Wir können mit Sicherheit ein technisches Problem ausschließen.« Offensichtlich habe ein ehemaliger Mitarbeiter die Daten entwendet: »Das Restrisiko ›Mitarbeiter‹ kann kein Unternehmen trotz modernster Infrastruktur und Sicherheitsmaßnahmen vollständig ausschließen. Mit einem solchen Risiko muss jedes Unternehmen leben. Trotz sorgfältiger Rekrutierung der Angestellten und laufender Prävention gibt es immer wieder unzufriedene Mitarbeiter und frustrierte Ex-Mitarbeiter. Der Vorfall ist ein unschöner Einzelfall.« Mit Hochdruck werde nun nach dem Datendieb in Kooperation mit den zuständigen Behörden geforscht (SZ 17.06.2005, 30).

Türkei

Telefonüberwachung in großem Umfang

Das türkische Massenblatt Hürriyet berichtete am 02.06.2005 unter Berufung auf einen anonymen Spionageexperten der Polizei, dass allein im Jahr 2004 fast 23.000 Handys und Festnetzanschlüsse überwacht worden seien. Zudem hätten Telekommunikationsanbieter Kundenrechnungen an Polizei und Geheimdienste weitergegeben, aus denen sich

die Verbindungsdaten ergeben. 90 Gerichtsbeschlüsse hätten diese Telefon-Massenüberwachung über 10 Jahre hinweg gestattet. Als Begründung wurde die Bekämpfung der Kurdenguerilla PKK angegeben. Mehrere Bombenanschläge seien so verhindert worden, darunter einer in der Touristenmetropole Antalya. Auch habe die Polizei größere Mengen des hochgefährlichen C4-Sprengstoffs aufspüren können.

Die Enthüllung fällt zeitlich mit dem Inkrafttreten eines neuen Strafgesetzbuches zusammen, mit dem Reform-Forderungen der EU erfüllt werden sollen. Dieses Gesetz verbietet die grenzenlose Telefonüberwachung, was Polizei und Geheimdiensten nicht gefällt. Über das Polizeiaufgabengesetz wollen sie, so der Hürriyet-Informant, wieder die alte Ordnung herstellen. Erst am Vortag war bekannt geworden, dass ein Gericht in Diyarbakir noch im April 2005 gestattet hatte, Telefone, SMS und Emails im ganzen Land auf »verdächtige« Verbindungen hin zu überprüfen. Der Chef der Anwaltskammer von Diyarbakir Sezgin Tanrikulu empfahl darauf hin allen Türken, sich an den Europäischen Gerichtshof zu wenden und Schadensersatz für den Bruch der Privatsphäre zu verlangen. Dann müsse der Staat beweisen, dass er seine Bürger nicht überwache. Der Vorsitzende eines Beirats im Premierministeramt Vahit Bicak ergänzte, abgehörte Personen müssten nach europäischem Recht nachträglich informiert werden. Der bisher spektakulärste Abhörskandal ereignete sich 2002. Damals waren Emails der EU-Botschafterin in Ankara, Karen Fogg, von türkischen Nationalisten veröffentlicht worden. Dass viele Türken hellhörig geworden sind, zeigte ein Test der Zeitung Radikal, die berichtete, man könne mit einem Code prüfen, ob Lauscher am Telefon hängen. Obwohl diese Behauptung völliger Unsinn ist, beteiligte sich das halbe Land an diesem Test (Schlötzer, SZ 03.06.05, 9).

Japan
Überwachungsroboter ersetzen Polizisten

Die japanische Firma Sohgo Securities Services hat einen 109 cm großen Roboter mit dem Namen »Guardrobo« entwickelt, der Einbrecher und Unfälle melden soll. Hierfür fährt dieser Roboter auf Rädern eine programmierte Route ab. Entdeckt er etwas Ungewöhnliches, so sendet er einen Notruf inclusive Video an die Sicherheitszentrale. Die Firma sieht in ihrem Angebot die Antwort auf eine alternde Gesellschaft mit einem steigenden Sicherheitsbedürfnis. Im Jahr 2006 wird jeder fünfte Japaner über 65 Jahre alt sein, im Jahr 2030 soll dies voraussichtlich auf jeden dritten Einwohner zutreffen. Die japanische Robot Association schätzt, dass sich der Weltmarkt für Serviceroboter in den nächsten fünf Jahren verdreifachen wird, von 5,4 Mrd. auf 17,1 Mrd. Dollar (Der Spiegel 27/2005, 59).

USA
Patriot Act soll entfristet werden

Nur wenige Stunden nach den Attentaten in London am 07.07.2005 stimmte das amerikanische Repräsentantenhaus mit 257 zu 171 einer unbefristeten Verlängerung des Patriot Act zu (vgl. DANA 4/2003, 30; 2/2005, 43). Dieses nach dem 11.09.2001 verabschiedete Anti-Terror-Gesetz räumt den Sicherheitskräften weitgehende Befugnisse im Kampf gegen den Terrorismus ein. Zentrale Bestimmungen waren damals auf vier Jahre befristet worden. Präsident George W. Bush hatte die unbegrenzte Verlängerung gefordert. Auch der Justizausschuss des Senats stimmte der Verlängerung am 21.07.2005 zu, verlangte aber Einschränkungen für die Ermittlungsbehörden. Die endgültige Verabschiedung des Patriot Act durch beide Häuser des Kongresses soll Herbst 2005 erfolgen. Besonders umstritten sind Bestimmungen, die den Behörden erlauben, die Daten von Verdächtigen bei Behörden oder in Bibliotheken abzufragen. Kritisiert werden zudem Abhörbestimmungen, die die Überwachung des gesamten Telefon- und Internetverkehrs eines Verdächtigen erlauben. Die Befugnis ist nicht auf einzelne Nummern beschränkt. Diese beiden Regelungen sollen nach dem Willen des Repräsentantenhaus auf 10 Jahre beschränkt werden.

Die demokratische Oppositionsführerin Nancy Pelosi stellte in Frage, ob der Patriot Act tatsächlich mehr Sicherheit bringe und vermutete, dass vor allem die verfassungsmäßigen Rechte unbescholtener Amerikaner eingeschränkt würden. Bush meinte dagegen, die Verlängerung des Gesetzes sei der Schlüssel für den Erfolg »unserer Anstrengungen, den Terror zu bekämpfen und das amerikanische Volk zu beschützen.«

Auch die verschärften Sicherheitsvorkehrungen im Nahverkehr in den USA nach dem 07.07.2005 stießen auf Protest von BürgerrechtlerInnen. Die New York Civil Liberties Union nannte die am 21.07.2005 angekündigten und praktizierten Taschenkontrolle vor U-Bahnstationen und Bushaltestellen der Stadt für verfassungswidrig. Die New Yorker Polizei stritt ab, dabei nach ethnischen Gesichtspunkten zu verfahren. Zur alltäglichen Überwachung des Nahverkehrs sind etwa 2700 PolizistInnen und Sicherheitsleute eingesetzt (Klüver SZ 23./24.07.2005, 6).

USA
Justizministerium veröffentlicht Sextäter im Internet

Das US-Justizministerium hat im Juli 2005 im Internet eine Webseite freigeschaltet, auf der Namen und Wohnorte zehntausender Sexualstraftäter aufgeführt sind. Die Datei enthält zudem Angaben zu den konkreten Taten und zu den Gerichtsverfahren sowie in vielen Fällen das Foto des Betroffenen. Erfasst sind Sexualstraftäter aus 22 Bundesstaaten. Justizminister Alberto Gonzales hatte die Einrichtung der Webseite zuvor im Mai angekündigt und alle Bundesstaaten zur Mitwirkung aufgefordert. Per Gesetz werden alle Bundesstaaten verpflichtet, die Daten von Sexualstraftätern öffentlich zugänglich zu machen. Anlass für die Initiative war eine Reihe von Sexualverbrechen, bei denen die Wiederholungstäter zwar in einzelnen Bundesstaaten erfasst waren, nicht aber in den Staaten, wo sie die neuen Straftaten begingen. Auf der Webseite werden die Dateien der Bundesstaaten zusammengeführt. Bis zum Herbst 2005 sollen die restlichen 29 Bundesstaaten angeschlossen sein. In den USA sind mehr als 500.000 Sexualstraftäter registriert. Nach Angaben des Ministeriums ist die Rückfallquote hoch.

Bürgerrechtsorganisationen kritisieren diese Prangerdateien, da hierüber eine Reintegration der Straftäter nach Verbüßung ihrer Strafe deutlich erschwert wird. Der Chef der Bürgerrechtsbewegung ACLU in Nevada, Allen Lichtenstein, wo gerade eine Erweiterung der Erfassung von Sextätern be-

schlossen wurde, fürchtet sogar Übergriffe: »Je mehr Informationen veröffentlicht werden, desto mehr gewaltsame Aktionen werden wir erleben.« Die Genauigkeit der Angaben ist je nach Bundesstaat und Stadt sehr unterschiedlich. In den Sextäter-Dateien von Washington DC oder Chicago etwa wird der Straßenabschnitt genannt, in dem der Täter lebt. In San Francisco wird lediglich die Postleitzahl angegeben. Die Gruppe der Anzuprangernden wird teilweise sehr weit gefasst: So stellte für 30 Tage die Polizei von Chicago auch die Fotos und Adressangaben von Freiern ins Netz, die bei Prostituierten festgenommen wurden (Graupner u. Klüver SZ 22.07.05, 4 u. 8; s.u.).

USA
Beugehaft gegen Journalistin wegen Quellenschutz

Gegen die 54jährige Journalistin Judith Miller der New York Times wurde von dem Richter Thomas Hogan Beugehaft angeordnet und vollzogen, weil sie sich weigerte, ihre Informanten bei einer brisanten Recherche preiszugeben. Es ging um die Frage, wer im Regierungsapparat des US-Präsidenten George W. Bush vor zwei Jahren Valerie Plame, die Frau des früheren US-Botschafters Joseph Wilson, als CIA-Agent enttarnt hatte. Wilson war während des Irak-Krieges als scharfer Kritiker des Präsidenten aufgefallen. Vergeblich berief sich Judith Miller darauf, dass ohne Quellenschutz eine freie Presse nicht möglich sei. Doch der Richter ignorierte das Zeugnisverweigerungsrecht, das ebenso wie insgesamt die freie Presse im Amerika Bushs nicht mehr viel gilt. Der ebenfalls von Beugehaft bedrohte Journalist Matthew Cooper vom Magazin Time konnte den Gerichtssaal nur als freier Mann verlassen, weil er – wie von ihm gefordert – seinen Informanten, einen der engsten Berater des US-Präsidenten, Karl Rove, preisgab. Er habe dessen ausdrückliche Zustimmung erhalten: »Daher bin ich bereit auszusagen. Das ist ein trauriger Tag.«

Der Fall Miller versinnbildlicht die schwere Krise zwischen unabhängigen Medien und konservativer Regierung. In Manhattan gab es vor dem Verlagshaus der New York Times Proteste; im ganzen Land demonstrierte die Newspaper Guild mit Mahnwachen. Die Inhaftierung sei »eine Bedrohung unseres ganzen Berufsstandes«, meinte Star Tribune aus Minneapolis, »ein harter Schlag gegen die Pressefreiheit«, assistiert Michael Konken, Chef des Deutschen Journalisten-Verbandes. Mit Judith Miller erwischte es eine Reporterin, die im eigenen Blatt umstritten ist. Sie hatte breit über die Massenvernichtungswaffen im Irak geschrieben, offenbar gefüttert von der Bush-Regierung. Miller gilt bei manchen Kollegen als überehrgeizig; selbst ihr Chefredakteur spricht von »spitzen Ellenbogen«. Nun lobte ihr Verleger Arthur Sulzberger jr. die Haft als »Akt des Gewissens«. Ziviler Ungehorsam habe in den USA eine lange Tradition – von der Boston Tea Party bis Martin Luther King.

In den USA sind Enttarnungen von Agenten strafbar. Sonderermittler Patrick Fitzgerald hatte den recherchierenden Reportern verbissen nachgesetzt. Die New-York-Times-Journalistin hatte keine Zeile über die Plame-Affäre geschrieben; ihre Quelle war den Ermittlern offenbar längst bekannt. Auch der dem Weißen Haus nahe stehende Kolumnist Robert Novak, der erstmals unter Berufung auf »zwei hochrangige Regierungsmitarbeiter« den Namen Plames genannt hatte, wird offenbar von Chefermittler Fitzgerald geschont. Dessen Aktivitäten richten sich vielmehr vor allem offenbar gegen die undichten »Quellen«. Auch in den USA sind Skandale oft mit Hilfe anonymer Informanten aufgeflogen. Populärstes Beispiel ist die Watergate-Affäre. Ein Insider (»Deep Throat«) hatte den Washington Post-Reportern Carl Bernstein und Bob Woodward Hinweise gegeben, die letztendlich zum Sturz von Richard Nixon führten. Erst vor Kurzem enthüllte sich der frühere FBI-Vizechef Mark Felt selbst als »Deep Throat«.

Der Fall Miller ermuntert die Staatsanwälte geradezu zur Jagd nach journalistischen Materialien. Insgesamt wurden im Jahr 2004 mehr als zwei Dutzend Reporter mit Vorladungen zur Preisgabe ihrer Quellen gedrängt. Betroffen sind davon vor allem sog Whistle-Blower, also Menschen, die in ihren Unternehmen oder Behörden Missstände erkennen und an die Medien weitergeben. Aus kritischen Kreisen wird die Meinung kolportiert, die Presse sei nicht ganz unschuldig an ihrer eigenen Entmündigung und Gängelung. Nach dem 11.09.2001 habe sie nicht mehr gewusst, ob sie einer patriotischen Pflicht erliegen oder besser Distanz zu den Herrschenden pflegen soll. Die meisten haben sich für die erste Alternative entscheiden mit der Folge, dass das Niveau und Qualität des US-Journalismus litten. Die Presse wird wenig ernst genommen. Zugleich zeigt der Fall, wie unkontrolliert politisiert die US-Justiz im Interesse der Regierung agiert. Die Regierung mag keine Verräter in den eigenen Reihen: Wer quatscht, wird enttarnt und bestraft. Derweil diskutieren die Abgeordneten im Kapitol über ein Zeugnisverweigerungsrecht, wie es z.B. in Deutschland existiert. In den USA haben es 49 Bundesstaaten eingeführt; aber das schützt nicht vor Verfahren der Bundesjustiz. Der »Newsweek«-Kolumnist Jonathan Alter schlug vor, mit niemandem im Kongress oder im Weißen Haus mehr Hintergrundgespräche zu führen, bis das Gesetz verabschiedet ist: »Wir sagen ihnen einfach: Wenn Ihr uns nicht beschützt, beschützen wir euch nicht« (Klüver SZ 19.07.2005, 8; Baden SZ 08.07.2005, 17; Kornelius SZ 02./03.07.2005, 4; Mascolo, Der Spiegel 28/2005, 116 f.; Hornig/Mascolo/Ter Haseborg, Der Spiegel 11/2005, 100 ff.).

USA
Mit Internet-Pranger gegen die Prostitution

Wer in Chicago die Prostitution fördert, muss damit rechnen, dass die Polizei seinen Namen und sein Foto auf ihrer Internet-Seite veröffentlicht. Dies trifft nicht nur Zuhälter, sondern auch Freier. Der Bürgermeister der Stadt, Richard Daley meinte anlässlich der Einweihung der Seite: »Wer nach Chicago kommt, sollte wissen: Wenn Sie eine Prostituierte ansprechen, werden Sie verhaftet. Und dann erfahren es Ihre Partnerin, Ihre Kinder, die Familie und der Arbeitgeber.« Die ersten 200 Verdächtigen waren schon online. Erwischten Freiern droht eine Geldbuße von 1000 Dollar und die Beschlagnahme ihres Autos. Dass Straftäter öffentlich zur Schau gestellt werden, ist in den USA nicht ungewöhnlich. Auch andere Gemeinden veröffentlichen regelmäßig Namenslisten und Fotos. Dabei geht es aber meist um schwere Sexualstraftaten wie Vergewaltigung (s.o.). Ähnlich wie in Chicago läuft in der Stadt Oakland seit Februar 2005 die »Operation Schande« gegen die Kunden von Prostituierten. Die Behörden der kalifornischen Gemeinde veröffentlichen die Bilder der Freier allerdings

nicht im Internet, sondern großformatig auf städtischen Reklametafeln (Der Spiegel 26/2005, 60).

USA

Röntgendurchleuchtung von Flugpassagieren geplant

Die zum US-Department for Homeland Security (DHS) gehörende Flugaufsichtsbehörde Transportation Security Administration (TSA) will noch im Jahr 2005 die ersten umfassenden öffentlichen Tests mit der sog. Backscatter-Röntgentechnik starten. Die etwa kühlschrankgroßen Geräte nutzen die Compton-Streuung normaler Röntgenstrahlen an Oberflächen. Dadurch wird nicht nur präzise sichtbar, was jemand unter der Kleidung oder Unterwäsche verbirgt, sondern seine Gestalt erscheint auch nackt auf dem Prüfbildschirm. Der neu ernannte DHS-Chef Michael Chertoff präsentierte den Plan zur Durchleuchtung aller Flugpassagiere im Frühjahr 2005 vor dem Sicherheitsausschuss des US-Kongresses. Darauf erhoben BürgerrechtlerInnen und SicherheitsexpertInnen schwere Bedenken gegen diesen Eingriff in die Privatsphäre der Flugreisenden. Zahlreiche US-Medien prangerten die Verletzung des Schamgefühls unbescholtener Passagiere an, die vor den Sicherheitskräften gleichsam nackt auf dem Präsentierteller landen. Ungeklärt ist bisher auch, was mit den gespeicherten Bildern geschieht.

Chertoff signalisierte, dass er »keine endlosen Debatten« über Datenschutzfragen wünsche. Die Regierung hält die Röntgenmethode für unverzichtbar, um endlich mehr Sicherheit an den Flughäfen zu erlangen. Testfälle mit verdeckten Agenten hätten gezeigt, dass die bisher eingesetzten Metalldetektoren zum Auffinden versteckter Waffen und Sprengstoffe zu unzuverlässig seien. Bedenken wegen des Eingriffs in die Intimsphäre – so die TSA – seien unbegründet. Als »Beweis« ließ sich Susan Hallowell, Leiterin des TSA-Sicherheitslabors, selbst röntgen und verschickte die Aufnahme zusammen mit Informationsmaterial an die Presse. Bereits die zunehmenden Leibesvisitationen an US-Flughäfen in der jüngsten Zeit provozieren in der Öffentlichkeit Unmut. Bisher werden Backscatter-Apparate nach freiwilligen Tests zur Durchsuchung von Verdächtigen eingesetzt. Künftig sollen sie im Routineverfahren jährlich bei mehreren Millionen Passagieren angewendet werden (Bonnert, www.heise.de 17.06.2005).

USA

Lebenslange GPS-Überwachung entlassener Sexualstraftäter

Nachdem in den vergangenen Monaten die US-Bundesstaaten Florida, Missouri, Ohio und Oklahoma Gesetze zur lebenslangen GPS-Überwachung von verurteilten Sexualstraftätern verabschiedet haben, folgten jüngst North Dakota und Alabama. Die Gesetzgebungswelle geht auf den Mord eines neunjährigen Mädchens durch einen vorbestraften Sexualstraftäter in Florida im Frühjahr 2005 zurück. Florida zwingt nun Kinderschänder, die elektronischen Ortungsgeräte lebenslang zu tragen, ebenso Ohio und Oklahoma. In Missouri müssen auch Exhibitionisten damit rechnen, bis ans Lebensende geortet zu werden. Die Technik soll es möglich machen, dass die Geräte automatisch Alarm schlagen, wenn der Träger sich einer Schule oder einem anderen verbotenen Gebäude nähert (Der Spiegel 32/2005, 56).

USA

Häftlingsüberwachung per RFID

In einem kalifornischen Gefängnis sollen Häftlinge im Rahmen eines Pilotprojektes mit RFID-Technik überwacht werden. Die Technik mit dem Namen TSI PRISM soll im Auftrag des Los Angeles County Sheriff´s Department (LASD) von Alanco Technologies geliefert werden. Dabei handelt es sich nach Herstellerangaben um ein drahtloses Überwachungssystem auf RFID-Basis. Die Häftlinge erhalten einen armbanduhrartigen Sender; die Wärter haben einen am Gürtel befestigten Empfänger. Alle zwei Sekunden wird ein Signal zwischen Handgelenk und Gürtel ausgetauscht, so dass der Aufenthaltsort der Überwachten in Echtzeit verfolgt werden kann. Das System zeigt auch an, wenn ein Wärter gewaltsam zu Boden geschlagen wird. Das System soll so die Sicherheit für die Angestellten und Insassen erhöhen und die Gewalt durch Häftlinge reduzieren. Die Kosten für die Anwendung bei 1800 Insassen wird auf 1,5 Mio. Dollar geschätzt. Bei positiven Ergebnissen hofft das Unternehmen auf zusätzliche Mittel, um weitere Gefängnisse ausstatten zu können. Nach Ansicht von Alanco besteht ein Marktpotenzial für Sicherheitssysteme in Gefängnissen in Höhe von 1,4 Mrd. US-Dollar (http://www.alanco.com).

Derweil plant der kalifornische Senat in einem »Information Protection Act 2005« ein eingeschränktes Verbot von kontaktlosen Datenspeichern in staatlichen ID-Karten. Ausnahmen von dem Verbot sind danach erlaubt, wenn dies »notwendig ist, um ein zwingendes Staatsinteresse zu erfüllen und es kein weniger stark in die Privatsphäre eingreifendes Mittel gibt, um dieses zu erreichen.« Als Beispiele für solche Ausnahmen werden genannt: Mauterfassung auf Straßen und Brücken, die Überwachung von Gefängnisinsassen und der Einsatz bei stationär in Krankenhäusern behandelten Kindern bis zum Alter von vier Jahren. Hintergrund und Auslöser des Gesetzesentwurfs, der dem Parlament vorgelegt werden muss (California State Assembly), war ein Projekt zur Überwachung von Kindern in der Schule mittels RFID-Technik (vgl. DANA 2/2005, 43; Omnicard-Newsletter 02.06.2005).

USA

FBI beobachtet Bürgerrechtler

Die amerikanische Bundespolizei FBI hat, wie das US-Justizministerium betätigte, in ihren Akten Tausende Seiten über Bürgerrechts- und Umweltgruppen gesammelt. Die Organisationen, darunter die Amerikanische Bürgerrechtsorganisation (ACLU) und Greenpeace, klagen nun auf Veröffentlichung der Dokumente. FBI speichert nach eigenen Angaben 1173 Seiten zur ACLU und 2383 Seiten zu Greenpeace. Es benötige noch mindestens bis Februar 2006, um die ACLU-Akten zu prüfen. Bis Juni 2006 soll die Durchsicht der Greenpeace-Dokumente dauern. Die Gruppen befürchten, dass sie vom FBI im Rahmen des Kampfes gegen den Terror überwacht werden. Die ACLU sieht diese Bedenken durch ein von der Regierung schon veröffentlichtes Dokument bestätigt. Dabei handelt es sich um ein an Antiterroreinheiten in

Boston, Los Angeles und New York adressiertes Memo über einen Aufruf zu Protesten gegen den Parteitag der Republikaner 2004. Anthony Romero, ACLU-Vorsitzender, kritisiert, hier würden Proteste gegen eine politische Versammlung mit dem Kampf gegen den Terrorismus in Verbindung gebracht (SZ 19.07.2005, 8).

USA

Hacker beschaffen sich Millionen Kreditkartendaten

40 Millionen Nutzende von Kreditkarten, davon allein 14 Mio. MasterCard-KundInnen müssen um ihr Geld fürchten: Unbekannte Betrüger haben sich offenbar in den Besitz der Kreditkartendaten mit Hilfe eines virusähnlichen Skriptes beschafft, mit dem sie in das Informationssystem der Fa. CardSystems Solution eingedrungen sind. Beschafft wurden Namen, Bankangaben und Kreditkartennummern. CardSystems ist eine von mehreren Firmen, über die Transaktionen zwischen Einzelhandel, Käufern und Kreditkartenunternehmen abgewickelt werden. CardSystems Solutions hat zugegeben, dass das Fehlverhalten von Mitarbeitern zum Diebstahl von mindestens 200.000 vertraulichen Datensätzen von VisaCard und MasterCard-Kunden geführt habe. CEO John Perry erklärte, Mitarbeiter hätten Transaktionsdaten im eigenen Firmennetz abgespeichert, obwohl dies ausdrücklich verboten sei. Die unverschlüsselten Kreditkarten-Daten inklusive persönlicher Geheimzahl habe die Firma für Nachforschungszwecke nutzen wollen, z.B. um herauszufinden, warum bestimmte Transaktionen nicht abgewickelt wurden.

Insgesamt sind in den USA etwa 1,1 Mrd. Kreditkarten im Umlauf. Der rekordträchtige Angriff ist bekannt geworden, als Sicherheitsexperten von MasterCard Abrechnungen routinemäßig auf Verdachtsmomente hin überprüften und Unregelmäßigkeiten auffielen. Das in Arizona ansässige Unternehmen bearbeitet jährlich Transaktionen im Wert von mehr als 15 Mrd. Dollar. Mit der Abspeicherung der Kundendaten für »Forschungszwecke« habe, so die beiden großen Kreditkartenfirmen MasterCard und Visa, die Firma CardSystems gegen die geltenden Sicherheitsbestimmungen verstoßen. Die Bundespolizei FBI wurde in die Ermittlungen eingeschaltet. Banken und KundInnen seien von dem Sicherheitsleck informiert worden, hieß es bei MasterCard. Die Sicherheitslücke sei inzwischen geschlossen. Mit den gestohlenen Daten lässt sich die fremde Identität vortäuschen und unter dieser Geld abheben.

Nach Angaben von MasterCard sind von dem Datenklau deutsche KundInnen nicht betroffen. Dies sah die Postbank anders. Diese tauschte die Kreditkarten aller gefährdeten deutschen Kunden aus. Betroffen sind mehrere Tausend Personen, die in den vorangegangenen Monaten bei Reisen in den USA ihre Kreditkarten genutzt oder via Internet in US-Shops eingekauft haben. Die anderen deutschen Banken und Sparkassen hielten eine solchen Schritt nicht für notwendig. Ein Sprecher der Deutschen Bank erklärte, alle gefährdeten Karten würden von der Gesellschaft für Zahlungssysteme (GZS) auf einen möglichen Missbrauch geprüft. Dieses Überwachungssystem werde jeder Buchung vorgeschaltet und könne etwa erkennen, ob eine Karte gleichzeitig in Frankfurt und New York eingesetzt worden ist. Einen Schadensfall hat es nach eigenen Angaben von Deutscher Bank, HypoVereinsbank, Dresdner und Commerzbank nicht gegeben. Die Sparkassen sehen zwar ein Risiko, doch sei das Risiko zu gering, um sich dem Beispiel der Postbank anzuschließen. Alle verdächtigen Transaktionen würden von den Präventionssystemen erkannt, sagte eine Sprecherin. Ein Kunde müsse nicht für nicht von ihm veranlasste oder autorisierte Transaktionen haften. Nachweislich missbräuchliche Buchungen würden selbstverständlich erstattet. Ein Sprecher des Bundesverbandes der Volks- und Raiffeisenbanken (VR) wies darauf hin, dass nur 0,1 % aller von dieser Bankengruppe ausgegebenen Karten – dies entspräche ca. 2000 Stück – in den USA in den vergangenen Monaten eingesetzt worden seien. Auf Wunsch könne dort, ebenso wie bei der Commerzbank, jedoch ein Kunde eine neue Karte beantragen.

Kurz vor dem oben genannten Vorfall war bekannt geworden, dass bei der weltgrößten Bank Citigroup im Computer gespeicherte Bankdaten von 3,9 Mio. KundInnen verloren gegangen seien. Computerbänder der Citi-Financial waren auf dem Weg zu einer Kreditbüro-Firma verschwunden mit Daten über Sozialversicherungs- und Kontonummern sowie Abzahlungsdaten der Betroffenen. Diese Informationen werden von Citi-Financial und anderen Kreditgebern monatlich an Kreditbüros weitergegeben. Es ist nicht das erste Mal, dass bei der Citigroup Kundendaten verschwinden. Gut ein Jahr zuvor verlor eine japanische Niederlassung der Großbank Informationen zu 120.000 Konten. Mai 2005 hatte die US-Polizei Verdächtige festgenommen, die die Daten von 700.000 KontoinhaberInnen von vier weiteren Banken, darunter die Bank of America und Wachovia gestohlen haben sollen. Nach amerikanischem Recht haften Kreditkartenbesitzer mit höchstens 50 Dollar für einen entstandenen Schaden. Nach Schätzungen der Federal Trade Commission (FTC) waren zuvor im Zeitraum 1998 bis 2003 mehr als 27 Mio. AmerikanerInnen Daten gestohlen worden. Der besonders betroffenen Finanzbranche sei dadurch ein Schaden von 48 Mrd. Dollar entstanden. Das Electronic Privacy Center (EPIC) forderte aus Anlass der aktuellen Sicherheitspannen eine strenge Regulierung der Branche. Der Verbraucher werde in seiner Vorstellung getäuscht, dass seine Zahlung direkt von der Kreditkartenfirma abgewickelt werde, sagte EPIC-Rechtsanwalt David Sobel: »Das ist eine Schattenwirtschaft, in der der Verbraucher niemals genau weiß, wer mit seinen persönlichen Daten umgeht« (SZ 08.06.2005, 30; Oldag SZ 20.06.2005, 1; SZ 22.06.2005, 32; OMNICARD-Newsletter Juni 2005).

USA

Pentagon muss Soldatensarg-Bilder veröffentlichen

Die US-Regierung verbot im jüngsten Krieg gegen den Irak und der anschließenden Besatzungszeit, wo es viele getötete US-Soldaten gab und gibt, die Veröffentlichung von Fotos der überführten Särge. Seit März 2003, dem Monat des Einmarsches in den Irak, kämpften verschiedene US-Bürgerrechtsorganisationen mit Verweis auf den Freedom of Information Act, das amerikanische Informationsfreiheitsgesetz, für deren Veröffentlichung (DANA 2/2004, 31). In einer außergerichtlichen Einigung gestand nun das amerikanische Verteidigungsministerium die Freigabe von Bildern, Videos

und Filmen von Soldatensärgen zu. Das Pentagon hatte mit seinem bisherigen Bilderverbot eine Direktive angewendet, die es seit dem ersten Golfkrieg 2001 gab. Nur hatte sich Präsident Bill Clinton im Gegensatz zu George W. Bush, nicht strikt daran gehalten. Die Leichensäcke wurden nicht nur versteckt, sondern auch begrifflich verschleiert: Sie hießen zunächst »human remains pouches« (Beutel für sterbliche Überreste) und später »transfer tubes« (Überführungsschläuche). Das Pentagon begründete die Geheimhaltung mit der Sorge um die Privatsphäre der Angehörigen und um die operative Sicherheit (Steinberger, SZ 06./07.08.2005, 13).

USA

Verkehrssicherheitsbehörde sammelt illegal Daten

Die US-Behörde für Verkehrssicherheit (TSA) hat, so ein Bericht des Kongresses illegal die Daten von mindestens 250.000 Menschen gesammelt. Die Daten wurden gesammelt, als die Behörde ein Programm testete, mit dem die Daten von Flugpassagieren mit denen steckbrieflich gesuchter Terroristen abgeglichen werden sollten (SZ 25.07.2005, 7).

USA

RFID-Einsatz im Krankenhaus

Im Jacobi Medical Center in New York soll mit Hilfe von RFID die Gefahr von Fehlbehandlungen reduziert und die Medikamenten- und Dosierungssicherheit verbessert werden. PatientInnen erhalten gleich bei der Aufnahme ein Funkarmband mit RFID-Chip, auf dem Name, Aufnahmedatum und Identifikationsnummer gespeichert sind. ÄrztInnen und Pflegepersonal lesen mittels eines TabletPCs oder Personal Digital Assistant (PDA) die Daten aus, identifizieren damit die PatientIn und erhalten Zugriff auf eine Datenbank, in der die Krankheitsgeschichte sowie Details zu den zu verabreichenden Medikamenten gespeichert sind. Es erfolgen auch elektronische Messungen an den PatientInnen: Spezielle Sensoren an der Brust messen z.B. die Herzwerte und senden diese an eine RFID-Uhr, welche die Daten an den Arzt funkt. Um die Position des Trägers auf 2 Meter genau ermitteln zu können, befinden sich auf dem Klinikareal mehrere Antennen. Sobald sich der Zustand der PatientIn verschlechtert, können sich die Mediziner sofort an den Aufenthaltsort begeben und eingreifen.

Das Projekt startete Sommer 2004 und ging Ende 2004 dauerhaft in Betrieb. Siemens Business Services wurde für seine technische Lösung 2005 auf dem Health Care Research & Innovations Congress (HCRIC) in Washington, DC, in der Kategorie »beste Innovation bei Patientensicherheit und Patientendaten« ausgezeichnet. Auch das Klinikum Saarbrücken hat Mitte April 2005 ein RFID-Pilotprojekt mit rund 1000 PatientInnen gestartet. Die Lösung ähnelt der im Jacobi Medical Center. Zur Erhöhung der Medikamenten- und Dosierungssicherheit wird dort ein Expertenprogramm eingesetzt, das die vorgeschlagene Verabreichung prüft und bei Gefahr auf Rot schaltet und zugleich erklärt, aus welchem Grund. Für mehr Patientennähe sollen Terminals im Aufenthaltsrum sorgen. Thomas Jell, Leiter für RFID-Technik bei Siemens Business Services: »Viele Unklarheiten und Fragen, die bei der Visite nicht beantwortet wurden, kann der Patient dort in aller Ruhe über sein Armband am Bildschirm abrufen«, z.B. Diagnose, Blutdruckwerte, Therapieformen, Behandlungsorte und -termine bis hin zum Entlassungsdatum (Franke, IT & Kommunikation Juli 2005).

Technik

ÖPNV-Fahrgast-Verhaltensdetektion

Australische Forschende arbeiten an einem Computerprogramm zum Erkennen von verdächtigem Verhalten in Bussen, U-Bahnen und auf Flughäfen. Das Überwachungssystem soll jene Fahrgäste aus der Masse herausfiltern, die sich merkwürdig benehmen, die Sitzplätze häufig wechseln oder mit auffälligem Gepäck unterwegs sind. Zwar räumen die Programmierer ein, dass die Detektion von Verhaltensmustern die Privatsphäre verletzen könnte. Doch in Zeiten wachsender Terrorismusgefahr halten sie den Preis für vertretbar. Barney Glover, Software-Experte an der Curtin University of Technology in Westaustralien: »Die notwendigen Daten für eine solche Überwachung werden ohnehin gesammelt, wir werten sie nur auf einem intelligenteren Level aus. Einfach nur schusselige oder nervöse Fahrgäste würden von dem System nicht erfasst. Roger Clarke, Computerspezialist an der Australian National University in Canberra kritisiert: »Man stelle sich nur einen Schulbus oder einen Touristenbus vor, in dem alle dauernd herumwuseln. Es ist einfach naiv, anzunehmen, dass ein solches System verwertbare Erkenntnisse liefern würde« (Der Spiegel 32/05, 114).

Virenschutz für Medizingeräte

Computerviren bedrohen die medizinische Apparatetechnik: Röntgengeräte, Ultraschallsysteme und andere medizinische Gerätschaften sind mittlerweile häufig mit dem hausinternen Krankenhausnetz verbunden, teilweise sogar mit dem Internet. Dadurch entstehen allerlei digitale Bedrohungen. Der Siemens-Konzern stellte mit »Siemens Virus Protection« nun das weltweit erste Virenschutzsystem vor, das die Diagnosegeräte vor Cyber-Attacken bewahren soll. Über eine geschützte Datenleitung wird die Virenschutz-Software direkt auf die Kliniksysteme übertragen und regelmäßig aktualisiert, um vor Ort die Daten aus Röntgen- und anderen Geräten nach digitalen Schädlingen zu durchforsten. Diese digitale Desinfektion dient – so Siemens – der Prophylaxe. Von durch Viren zum Absturz gebrachte Röntgengeräte seien bislang nicht bekannt. Nach Ansicht des Sicherheitsexperten Andreas Marx läuft das System jedoch Gefahr, zu spät zu kommen, da Virenschutz-Updates reaktiv sind: »Sie kommen erst, nachdem ein neuer Virus bereits unterwegs ist.« Am sichersten wäre es, medizinische Geräte mit empfindlichen Daten ganz vom Netz zu nehmen (Der Spiegel 26/2005, 116).

Hacker-Gegenangriff gegen Phising-Web-Seiten

Ein Hacker namens »Sickophish« greift Web-Seiten von Online-Betrügern an und versucht dadurch potenzielle Phising-Opfer davor zu bewahren, ihre Bankdaten preiszugeben. Die Betrüger verschicken Emails, angeblich von der Deutschen Bank, der Postbank und anderen als seriös geltende Instituten. Der Empfänger soll auf einen Link klicken und auf einer Web-Seite, die aussieht wie die einer realen Online-Bank, seine Daten eingeben. Sickophish und andere Hacker brechen nun in die Rechner der falschen Banken ein und hinterlegen dort, wo die KundInnen ihre Geheimnummern eingeben sollen, Botschaften wie: »Diese Seite war eine Fälschung. Sie wurde von Sickophish zerstört.« Angst vor dem Gesetz brauchen die Hacker kaum zu haben: Die Rechner der Betrüger befinden sich meist in Staaten der Karibik, wo man es mit der Strafverfolgung von unzulässigen Cyberangriffen, um die es sich hier wohl trotz aller Nothilferegelungen handeln dürfte, nicht so genau nimmt (Der Spiegel 24/2005, 62).

Email-Risiken im Wandel

Gemäß einem IBM-Report zur Computersicherheit, der die Erkenntnisse von ca. 3000 ExpertInnen aus der ganzen Welt zusammenfasst, wird Spam – der unerwünschte, meist harmlose Werbemüll in elektronischen Briefkästen – weniger. Zugleich steigt die Zahl schädlicher Angriffe mit virenverseuchten Emails stark an. Nach dem Report war Juni 2005 jede 28. Email verseucht; Ende 2004 galt das nur für eine von 52 Emails. Im ersten Halbjahr 2005 sind die Attacken auf Internet-Computer um 50 % angestiegen. Dabei konzentrierten sich die Internet-Kriminellen immer stärker auf Betrügereien, Erpressung und Ausforschung geheimer Daten. Fast 60 % der 237 Mio. registrierten Attacken im ersten Halbjahr 2005 waren gezielt gegen Behörden und Unternehmen gerichtet. Die meisten Angriffe, die bevorzugt freitags und sonntags starten, hatten ihren Ursprung in den USA, gefolgt von Neuseeland und China (Der Spiegel 32/2005, 64).

Gentechnik

Ernährungsberatung mit Genanalyse zunehmend beliebt - Nutzen zweifelhaft

Seit das menschliche Genom entschlüsselt ist, boomt die Erforschung des Wechselspiels zwischen Ernährung, genetischer Konstitution und Gesundheit. Die Europäische Kommission richtete kürzlich eine »NutriGenomics Organisation« (NuGO) ein, um diese Forschung voranzutreiben. Finanziert wird das Konsortium durch ein EU-Projekt, das in den nächsten sechs Jahren die Zusammenarbeit von 22 Partnern in zehn EU-Ländern mit ca. 17 Mio. Euro fördert. Zwar ist klar, dass bei ernährungsbedingten Erkrankungen auch genetische Ursachen eine Rolle spielen. Doch warnen Wissenschaftler, die Ernährungsgewohnheiten von Genanalysen abhängig zu machen.

Trotzdem schicken weltweit KundInnen jeden Alters ihre DNS-Proben an kommerzielle Labors, die nutrigenomische Tests anbieten. Der in Colorado/USA ansässige Hersteller Sciona verkaufte in den vergangenen zwei Jahren mehr als 10.000 Tests. Viele KäuferInnen haben Angehörige mit Diabetes und Herzerkrankungen und wollen diesen Krankheiten vorbeugen; andere wollen einfach möglichst gesund leben. Während das Infomaterial auf der Firmenwebseite von Sciona eher vage formuliert ist, wirbt die in Seattle ansässige Fa. Genelex, die Scionas Testkits vertreibt, offensiv: Wenn »Diät und Lebensstil erst einmal mit dem Genom harmonisiert« seien, winke »leichtere Gewichtskontrolle, optimierte Gesundheit und Haltbarkeit von Haut, Haar und Knochen sowie ein verringertes Risiko an einer der großen Drei – Herz-Kreislauf-Krankheiten, Krebs und Diabetes – zu erkranken.«

Die Entstehung dieser Krankheiten sind eine komplexe Angelegenheit, bei der viele Gene und sonstige Risikofaktoren eine wesentliche Rolle spielen. Rosalyn Gill-Garrison und Howard Coleman, Mitgründer von Genelux, nutzen aber nur ein einzelnes Gen als Beispiel dafür, wie und warum Gendiäten funktionieren sollen: Etwa 10 % aller Nord- und 15 % aller SüdeuropäerInnen besitzen eine Variante des Gens für das Enzym Methylentetrahydrofolat-Reduktase (MTHFR), welches die Aufnahme von Folsäure erschwert. Das führt bei folsäurearmer Ernährung zu einem moderaten Anstieg an Homocystein im Blut, was mit einem erhöhten Risiko für Herzkreislauf-Erkrankungen korreliert. Es gibt aber keine soliden Langzeitstudien, die einen klaren Zusammenhang zwischen einer erhöhten Folsäureaufnahme und einer Verringerung des Herzkreislauf-Risikos aufzeigen. MTHFR führt die Liste jener 19 Gene an, die Sciona als Teil des genetischen Ernährungsservices testet.

Die genetisch maßgeschneiderten Empfehlungen für eine passende Diät und das persönliche Gen-Profil kosten umgerechnet 300 Euro, einen Speichelabstrich und einen ausgefüllten Fragebogen. Die Ernährungsberaterin Carolyn Katzan offeriert Sciona-Tests unter dem Schlagwort »DNA-DiätTM« über ihre Webseite und in einem Wellnesscenter im kalifornischen Santa Monica. Ihre Preise bewegen sich zwischen 315 Euro für den Online-Service und 450 Euro inclusive persönlicher Ernährungsberatung in der Klinik. Dafür gibt es Ratschläge, wie man die Menge gesättigter Fettsäuren verringert (weniger Fleisch und Fertigprodukte), aber die an Antioxidantien ebenso steigert (mehr Obst und Gemüse) wie die an Folsäure (mehr dunkelgrünes Blattgemüse und Vollkornprodukte). Meist werden gleich die passenden Vitaminpillen dazu verkauft.

Die Tipps sind nicht revolutionär, sondern spiegeln die Richtlinien einer vernünftigen Ernährung wider. Die Zuordnung zu einem individuellen genetischen Profil hat allenfalls den Vorteil, dass die Person persönlich motiviert wird (Kirchweger, SZ 25./26.05.2005; vgl. DANA 2/2002, 36 f.).

Rechtsprechung

BVerfG

Keine willkürliche Datenbeschlagnahme bei Berufsgeheimnisträgern

Das Bundesverfassungsgericht hat entschieden, dass bei Ermittlungsverfahren gegen Berufsgeheimnisträger wie Anwälte und Steuerberater nicht willkürlich Daten beschlagnahmt werden dürfen. In einem Verfahren gegen den Angehörigen einer solchen Berufsgruppe kann die Beschlagnahme des gesamten Datenbestands und das Begehen von bewussten oder willkürlichen Verfahrensverstößen ein Beweisverwertungsverbot nach sich ziehen. Der zweite Senat des BVerfG gab damit der Verfassungsbeschwerde eines Rechtsanwalts und Steuerberaters auch wegen des damit verbundenen »erheblichen Eingriffs in das Recht auf informationelle Selbstbestimmung« statt, in dessen Kanzlei sämtliche Computerdateien beschlagnahmt worden waren (Az. 2 BvR 1027/02 v. 12.04.2005; Die Welt 05.06.2005, 4).

SächsVerfGH

Sächsischer großer Lauschangriff auch verfassungswidrig

Nachdem am 03.03.2004 das Bundesverfassungsgericht das Gesetz zur Zulassung der akustischen Wohnraumüberwachung auf Bundesebene für verfassungswidrig erklärt hatte (NJW 2004, 999 ff.; DANA 1/2004, 36), entschied der Sächsische Verfassungsgerichtshof (SächsVerfGH) am 21.07.2005, dass dieses Instrument zur Bekämpfung sog. organisierter Kriminalität in wesentlichen Teilen gegen die Sächsische Verfassung verstößt. Die April 2004 verabschiedete Änderung des Verfassungsschutzgesetzes missachtet nach Auffassung des Gerichtes das Trennungsgebot von polizeilicher und geheimdienstlicher Arbeit und die Grundrechte auf Menschenwürde und auf Unverletzlichkeit der Wohnung. Die Staatsregierung muss bis zum 30.06.2006 neue Regelungen für Polizei und Verfassungsschutz finden, die den »Kernbereich privater Lebensgestaltung« nicht antasten. Gegebenenfalls müssen bereits begonnene Abhörmaßnahmen beendet und deren Ergebnisse vernichtet werden. Um die Bekämpfung der organisierten Kriminalität nicht zu gefährden, wurden die Regelungen nicht für nichtig erklärt; vielmehr legt das Urteil Kriterien für die Ermittlungsarbeit fest. Bereits begonnene Abhörmaßnahmen müssen jetzt aber gegebenenfalls abgebrochen werden oder Aufzeichnungen vernichtet werden, wenn die Intimsphäre der Belauschten beeinträchtigt ist. Das Urteil stellt u.a. klar, dass der Verfassungsschutz nur solche Daten an die Polizei weitergeben darf, die diese ebenfalls hätte sammeln dürfen (U.v. 21.07.2005, Az. Vf. 67-II-04).

Gegen das Sächsische Verfassungsschutzgesetz geklagt hatten 29 PDS- und ein FDP-Abgeordneter des Sächsischen Landtags. Sie hatten bemängelt, dass dieses Gesetz die Arbeit von Polizei und Geheimdiensten unzulässig vermische. Der Sprecher der grünen Fraktion, Johannes Lichdi, sieht sich in der Auffassung bestärkt, dass das Trennungsgebot von Verfassungsschutz und Polizei nicht aufgeweicht werden dürfe. Dieses Trennungsgebot geht auf die Zeit der nationalsozialistischen Diktatur zurück, als diese Trennung in der Geheimen Staatspolizei (Gestapo) aufgehoben war. Trotz der Niederlage sieht sich die Sächsische Staatsregierung in ihrer Position bestätigt, da eine entscheidende Frage zu ihren Gunsten entschieden wurde, so Sicherheitsrechtler Dirk Heckmann: »Der Wohnraum darf beobachtet werden – nur die Gesetze müssen nachgebessert werden.« Für Innenminister Thomas de Maizière ist der wichtigste Aspekt des Urteils, dass es zu keiner Schwächung im Kampf gegen die organisierte Kriminalität führen werde. Die CDU-Fraktion im Landtag betonte, die erweiterte Zuständigkeit des Verfassungsschutzes müsse mit Blick auf den Terrorismus beibehalten werden (www.mdr.de 21.07.2005; SZ 22.07.2005, 7).

BGH

Abgehörte Selbstgespräche verletzen Kernbereich

Der Bundesgerichtshof (BGH) in Karlsruhe hat die Verwertung abgehörter Selbstgespräche im Strafprozess untersagt. Die Verurteilung eines Angeklagten wegen Mordes wurde aufgehoben, dem vorgeworfen wird, im Oktober 1998 im Landkreis Fürstenfeldbruck einen Landwirt mit einem massiven kantigen Werkzeug erschlagen zu haben. Das konnte dem tatverdächtigen alkoholkranken 46jährigen Maler aber zuerst nicht nachgewiesen werden. Nach neuen Verdachtsmomenten wurde der Verdächtige viereinhalb Jahre später während eines Krankenhausaufenthalts mit Wanzen überwacht. In einem dabei abgehörten Selbstgespräch fragte sich der betrunkene Angeklagte, ob er sein Opfer nicht besser erschossen hätte. Diese aufgezeichnete Bemerkung legte das Münchner Landgericht am 13.12.2004 einer Verurteilung wegen Mordes zur einer lebenslangen Freiheitsstrafe zu Grunde. Die Bundesrichter bezogen sich in ihrer Entscheidung auf das neue Gesetz zum großen Lauschangriff, das den Kernbereich privater Lebensführung absolut schützen will. Auch zur Aufklärung von Schwerkriminalität dürften »Erkenntnisse aus einem Eingriff in den absolut geschützten Kernbereich privater Lebensgestaltung« in Strafprozessen nicht verwertet werden. Anders als etwa bei einem Tagebuch oder einem Zwiegespräch habe der Beschuldigte nicht damit rechnen müssen, dass seine Äußerungen Dritten zugänglich sein könnten. Die Bemerkungen seien zudem »interpretationsbedürftig« gewesen. Bei einem »eindeutigen Bezug zu einer Straftat« könnte die Beurteilung anders ausfallen, sagte der BGH-Richter Armin Nack. Selbstgespräche müssten anders behandelt werden als Gespräche. Der Fall wurde an das LG München zurückverwiesen. Der BGH erwartet – so Richter Nack – nach dieser Entscheidung weitere Verfahren zum großen Lauschangriff. Der 1. Strafsenat habe sich hier

auf die Besonderheiten des konkreten Falls beschränkt und dabei mehrere Rechtsfragen offen gelassen. So habe der BGH nicht entschieden, ob das Abhören in einem Krankenzimmer eventuell abgebrochen werden muss oder ob ein Gespräch mit einem Angehörigen über eine Tat verwertet werden darf. Maßgebend sei in diesem Verfahren eine »Kumulation mehrerer Umstände« gewesen (U.v. 10.08.2005, Az. 1 SstR 140/05, Kerscher SZ 11.08.2005, 1).

OVG Saarlouis

Scientology darf nicht mehr observiert werden

In einem schon seit sechs Jahren anhängigen Streitverfahren entschied das Oberverwaltungsgericht (OVG) Saarlouis, dass die in Deutschland umstrittene Scientology-Organisation nicht mehr vom Landesamt für Verfassungsschutz (LfV) mit nachrichtendienstlichen Mitteln beobachtet werden darf. In erster Instanz hatte das Verwaltungsgericht Saarlouis im Jahr 2001 zugunsten des LfV entschieden. Das Gericht begründete seine Entscheidung damit, dass die mehr als siebenjährige Beobachtung »keine die Fortsetzung rechtfertigenden Ergebnisse erbracht« habe (Az. 2 R 14/03; SZ 28.04.2005, 6).

SG Augsburg

Kassenvorstände müssen Gehälter offenlegen

Das Sozialgericht (SG) Augsburg hat in einem bundesweiten Musterprozess am 20.04.2005 festgestellt, dass Krankenkassen die Gehälter ihrer Vorstände offen legen müssen. Das Bundesversicherungsamt (BVA) hatte gegenüber der Betriebskrankenkasse Essanelle (BKK) verfügt, diese müsse die Einkünfte ihrer Chefs in der Mitgliederzeitung und im Bundesanzeiger veröffentlichen und hatte nach entsprechender Weigerung geklagt. Seit 2004 besteht eine entsprechende gesetzlichen Verpflichtung im Sozialgesetzbuch IV für Krankenkassen und Kassenärztliche Vereinigungen. Die BKK hatte sich gegen eine Veröffentlichung gewehrt und Persönlichkeitsrechte ihrer Vorstände geltend gemacht. Das SG Augsburg stellte fest, die Bekanntgabe der Gehälter sei im »überwiegenden Allgemeininteresse zulässig« und ein geeigneter Beitrag zur Kostendämpfung. Die Transparenz werde durch das Solidarprinzip im Sozialstaat legitimiert, zumal die Gehälter paritätisch von Arbeitgebern und Arbeitnehmern finanziert werden. Das SG Augsburg verglich die Situation der Kassenmanager mit der von Spitzenpolitikern oder Richtern, deren Einkünfte auch bekannt sind. Bundesweit sind mehr als 20 Verfahren gegen weitere Krankenkassen wegen des Verstoßes gegen die Offenlegungspflicht anhängig. Die Wirkung der Veröffentlichungspflicht ist beachtlich: Seit die Spitzengehälter – zwischen 150.000 und 260.000 Euro – bekannt sind, kann sich die Gesundheitslobby die Gehälter nicht mehr erhöhen, ohne öffentlichen Unmut auszulösen (Az. S 10 KR 320/04; Graupner, SZ 18.05.2005, 2, 17).

AG Darmstadt

IP-Adressen-Speicherung bei T-Online rechtswidrig

Das Amtsgericht (AG) Darmstadt hat die Praxis der Speicherung von IP-Adressen bei T-Online für rechtswidrig erklärt. Die Aufbewahrung von Verbindungsdaten dynamischer IP-Adressen bis 80 Tage nach Rechnungsstellung verstoße gegen geltende Datenschutzbestimmungen (§ 6 Abs. 1 TDDSG). Geklagt hatte Holger Voss, der vor zwei Jahren wegen eines satirischen Beitrags in einem Telepolis-Forum angeklagt und freigesprochen worden war. Hierbei wurde ihm die Speicherpraxis von T-Online bewusst und er klagte als Flatrate-Kunde gegen die Speicherung. Der Anwalt von T-Online hatte versucht, den Richter davon zu überzeugen, dass die Aufbewahrung für Abrechnungszwecke erforderlich sei. Dem hatte Voss widersprochen. Auch für die Aufrechterhaltung des technischen Betriebs würde T-Online – ebenso wie andere Provider – die Verbindungsdaten nicht benötigen. So hatte z.B. der Provider Lycos Europe Mitte Mai 2005 erklärt, er verzichte vollständig auf die Speicherung der dynamisch zugewiesenen IP-Adressen seiner KundInnen. Unabhängig vom gewählten Tarif seien die IP-Adressen nicht abrechnungsrelevant. Voss hatte nicht bestritten, dass die IP-Adressen für Missbrauchs- und Störungsfällen im Einzelfall benötigt werden könnten. Eine Vorratsdatenspeicherung werde aber von § 6 Abs. 8 TDDSG nicht erlaubt. Dem schloss sich das Gericht an.

Abgelehnt wurde das Begehren von Voss, auch Zeiten und Datenmengen für seine Internetverbindung nicht mehr zu speichern. Zwar seien diese Daten für die Abrechnung einer Flatrate nicht direkt notwendig; für eventuelle Rechtsstreitigkeiten über eine Rechnung könnten diese Daten aber u.U. wichtig werden. Diese Speicherung sei von der Erlaubnis der Verarbeitung für Abrechnungszwecke gedeckt. T-Online-Anwalt Ulrich Wuermeling von der Anwaltssozietät Latham&Watkins ließ durchblicken, dass man im Fall einer Berufung darauf setzen werde, das Vosssche Verfahren erst einmal auszusetzen und eine Entscheidung in einem zweiten, bereits anhängigen Verfahren abzuwarten. In diesem Verfahren wird für September 2005 eine Gutachten vorgelegt werden. Kommentar des stellv. Datenschutzbeauftragten von Schleswig-Holstein, Johann Bizer: »Wir vom ULD und andere Datenschutzkollegen haben immer gesagt, dass das so sein muss«. Das Regierungspräsidium Darmstadt als die für T-Online zuständige Aufsichtsbehörde hatte dagegen behauptet, die IP-Adressspeicherung bei Flatrate-KundInnen sei korrekt (U.v. 30.06.2005, Az. 300 C 397/04; www.heise.de 01.07.2005).

SG Düsseldorf

Doppelbett beweist nicht eheähnliche Gemeinschaft

Nachdem bei einer Antragstellerin auf Arbeitslosengeld II ein Doppelbett sowie Herrenpflegeartikel im Bad festgestellt und ein männlichen Mitbewohner angetroffen wurde, unterstellte ihr eine Arbeitsagentur eine eheähnliche Gemeinschaft und versagte das Arbeitslosengeld.

Das Sozialgericht Düsseldorf erkannte nur eine Haushalts- und Wirtschaftsgemeinschaft. Es bedürfe sicherer und nachvollziehbarer Kriterien wie eine tatsächliche Unterhaltsleistung für die Feststellung einer von Einstandspflichten geprägten eheähnliche Gemeinschaft (SG Düsseldorf, S 35 AS 119/05 ER, 22.04.2005; AP 06.06.2005).

Buchbesprechungen

Hempel, Leon; Metelmann, Jörg (Hrsg.)
Bild – Raum – Kontrolle
Videoüberwachung als Zeichen gesellschaftlichen Wandels
suhrkamp taschenbuch wissenschaft, Frankfurt am Main 2005, 403 S., 14 €, ISBN 3-518-29338-9.

(tw) Zum Thema Videoüberwachung gibt es viele, auch kritische Veröffentlichungen. Der vorliegende Sammelband führt im handlichen Taschenbuchformat eine Bandbreite dieser kritischen Stellungnahmen zur optisch-elektronischen Kontrolle zusammen. Sein Schwerpunkt liegt bei den Sozialwissenschaften – von den Medien- über die Politik- bis hin zu den Geschichtswissenschaften – flankiert von etwas Psychologie und Recht. Die Videoüberwachung wird in ihren unterschiedlichen Anwendungen – vom Kindergarten bis zum Kriegseinsatz – beleuchtet; die verunsichernden wie auch versichernde Wirkweisen werden dargestellt, ihr Einsatz für Kommerz und für Sicherheit. Das Buch liefert die Grundlagen für eine Soziologie der Kameraüberwachung. In durchgängig gut lesbaren Beiträgen tauchen dabei aber immer wieder ähnliche Präsentationsmuster auf: die Bezugnahme auf Benthams »Panopticum«, Foucaults »Überwachen und Strafen« und George Orwells »1984«. Thematisiert werden die gesellschaftlichen, die wirtschaftlichen und psychologischen Rahmenbedingungen, die die Videoüberwachung hervorbringen und die von ihr hervorgebracht werden. Mancher Schluss – etwa die Bezugnahme zwischen Big-Brother-Medienspektakel und Big-Brother-Überwachungsrealität – klingt zwar plausibel, ist aber nicht weiter erkenntnisfördernd. Andere dargestellte Zusammenhänge sind dagegen wieder hoch spannend und von grundlegender Bedeutung.

Das Los eines Sammelbandes ist es, dass bei einem relativ engen, wenn auch schillernden Thema Argumentationsmuster immer wieder auftauchen. Zwar basieren praktisch sämtliche Darstellungen auf den modernsten technischen Standards – Digitalisierung, Vernetzung, Mustererkennung, Koppelung mit Datenbanken – doch fehlt in dem Band eine Darstellung des technischen »State of the Art«, die das Werk runder gemacht hätte. Instruktiv sind die Präsentationen verschiedener nationaler Überwachungskulturen. Eher beiläufig behandelt werden rechtliche Fragen. Damit wird ein weit verbreitetes Soziologendefizit kultiviert, was angesichts der zumindest teilweise bestehenden Herrschaft des Rechts in zivilisierten Gesellschaft schade ist. Ein weiteres Defizit liegt darin, dass vor lauter Deskription und Analyse – trotz mancher ethischen Grundierung – die Handlungsperspektive zu kurz kommt. Wer sich kritisch mit Videoüberwachung beschäftigen will, der kommt aber an diesem Bändchen definitiv nicht vorbei.

Absage an schrankenlose Kommunikationsüberwachung

Presseerklärung der DVD vom 27.07.2005

Mit einem Urteil vom 27.07.2005 hat das Bundesverfassungsgericht die 2003 in das Niedersächsische Gefahrenabwehrgesetz aufgenommene Befugnis zur Überwachung der Telekommunikation zwecks Gefahrenabwehr und zwecks Vorsorge für die künftige Strafverfolgung für nichtig erklärt. Dazu erklärt Sönke Hilbrans, Vorsitzender der Deutschen Vereinigung für Datenschutz:

»Das Urteil ist uneingeschränkt zu begrüßen. Es setzt die Linie der Entscheidungen vom 3. März 2004 fort, mit denen das Gericht den so genannten ›Großen Lauschangriff‹ an strenge verfassungsrechtliche Vorgaben gebunden und die Abhörbefugnisse des Zollkriminalamts an strengen Bestimmtheitsanforderungen gemessen hat. Auch der niedersächsische Gesetzgeber hat in dem Eifer, der Polizei neue Befugnisse zu geben, tragende Verfassungsprinzipien wie den Grundsatz der Verhältnismäßigkeit und das Gebot klarer und in ihrer Anwendung vorhersehbarer Gesetze übergangen.

Es sollte zu denken geben, dass sich das Bundesverfassungsgericht mit der jüngsten Entscheidung erheblich kürzer fassen konnte als noch im März 2004, da sich in seiner Rechtsprechung inzwischen ein klarer Katalog an Bedingungen für staatliche Überwachungsmaßnahmen herauskristallisiert hat.

Es ist jetzt an den Gesetzgebern nicht nur in Niedersachsen, sondern auch in anderen Bundesländern und im Bund, eine Trendwende in der Gesetzgebung zu vollziehen und anzuerkennen, dass Grundrechtsschutz etwas anderes ist als die permanente Aufrüstung von Polizei und Nachrichtendiensten mit neuen oder weitergehenden Eingriffsbefugnissen.

Das Bundesverfassungsgericht gibt in seiner Entscheidung zugleich dem Bundesbeauftragten für den Datenschutz Recht, dem zuletzt für seine offensiv grundrechtsfreundlichen Positionen von dem Bundesminister des Innern vorgeworfen wurde, dass er seine Kompetenzen überschreiten würde.«

TK-Vorratsdatenspeicherung ist keine Lösung – und zudem verfassungswidrig

Internationale Petition gegen Vorratsdatenspeicherung

Gemeinsame Pressemitteilung der Deutschen Vereinigung für Datenschutz (DVD) e.V., des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. und STOP1984 vom 01.08.2005

European Digital Rights (EDRi) hat gemeinsam mit dem Internetserviceprovider XS4ALL aus den Niederlanden eine internationale Petition gegen die Pläne einer europäischen Vorratsdatenspeicherung gestartet (www.dataretentionisnosolution. com/ index.php?lang=de).
Internetnutzer aller europäischen Staaten und weltweit sind aufgefordert, ihren Protest zu bekunden, indem sie die Petition an die Europäische Kommission sowie die Mitglieder des Europäischen Parlamentes unterzeichnen.

Der Vorschlag von Justizministern und EU-Kommission zur Vorratsdatenspeicherung beinhaltet eine Verpflichtung von Telefongesellschaften und Internetprovidern, die Verbindungsdaten von Telefonaten, SMS, Internet- und E-Mailverkehr ihrer Kunden langfristig zu speichern. Eine solche Vorratsdatenspeicherung würde zeigen, wer mit wem telefoniert, wem er E-Mails oder SMS gesandt, welche Webseiten er besucht und sogar von wo aus er mit seinem Handy telefoniert hat.

Dadurch würden die Überwachungsbefugnisse unverhältnismäßig erweitert, denn zu Überwachungsobjekten würden nicht nur verdächtige Kriminelle bzw. Terroristen, sondern alle Internetnutzer/innen.

Das Bundesverfassungsgericht hat im seinem jüngsten Urteil zur »vorbeugenden Kriminalitätsbekämpfung« deutlich gemacht, dass eine solche Vorratsdatenspeicherung nicht mit dem Grundgesetz der Bundesrepublik Deutschland zu vereinbaren ist (vgl. hierzu auch die Presseerklärung der DVD vom 27.05.2005). DVD- und FIfF-Vorstandsmitglied Werner Hülsmann erklärt hierzu:

»Das Bundesverfassungsgericht hat in seinem Urteil zur Telefonüberwachung zur vorbeugenden Verbrechensbekämpfung die Chance genutzt, dem Fernmeldegeheimnis wieder die ihm zustehende Bedeutung zu geben. In dem Urteil wurde unmissverständlich zum Ausdruck gebracht, dass auch die Umstände der Telekommunikation, also ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist, dem Schutz des Fernmeldegeheimnisses unterliegen und ausdrücklich dargestellt, dass jegliche Informationen, die mit Hilfe der Fernmeldetechnik übertragen werden – also auch E-Mails – hierunter fallen.

Es ist nicht zu übersehen, dass das Bundesverfassungsgericht in der aktuellen Diskussion einen verfassungsrechtlichen Pflock einschlagen und deutlich machen wollte, dass eine Vorratsdatenspeicherung der Verkehrsdaten verfassungsrechtlich nicht in Frage kommt.«

Die Deutsche Vereinigung für Datenschutz (DVD) e.V., das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, STOP1984 und andere Bürgerrechtsorganisationen teilen die Einschätzung der Initiatoren der Petitionskampagne EDRI und XS4ALL:

1. Die Vorratsdatenspeicherung in der geplanten Art stellt eine Maßnahme dar, die in unzulässiger Weise in die Privatsphäre von 450 Mio. Menschen allein in der Europäischen Gemeinschaft eingreift.
2. Diese Vorratsdatenspeicherung ist unverhältnismäßig und daher nicht mit dem Artikel 8 der Europäischen Menschenrechtskonvention vereinbar – in der Folge also illegal.
3. Die vorgebliche Sicherheit, die durch die Vorratsdatenspeicherung erzielt werden soll, stellt eine Illusion dar: Mit den derzeit verfügbaren technischen Möglichkeiten würden gezielte Suchläufe auf Personen Jahre dauern und die Ergebnisse leicht zu falschen Betroffenen führen.
4. Die Art und Weise, wie die Politiker einiger EU-Staaten nun versuchen, die EU zu instrumentalisieren, um die in ihren nationalen Parlamenten bereits abgelehnten Speicherungsvorhaben doch noch durch die Hintertüre durchzusetzen, stellt einen Missbrauch europäischer Gremien dar.

Bettina Winsemann von STOP1984: »Wir stellen uns vehement gegen die Vorratsdatenspeicherung, die ein unverhältnismäßiges Mittel der staatlichen Überwachung darstellt und fordern, dass die Datenspeicherung nur durch geeignete Behörden und nur in Ausnahmefällen nach richterlicher Anordnung genutzt werden darf.

Vorratsdatenspeicherung bedeutet auch, das Recht auf Rede- und Meinungsfreiheit einzuschränken, die Unschuldsvermutung nach Artikel 11 der UN-Menschenrechtscharta zu unterwandern und den Schutz des Privatlebens nach Artikel 12 der UN-Menschenrechtscharta fallen zu lassen.«

In den nächsten zwei Monaten hoffen die Initiatoren EDRI und XS4ALL und die unterstützenden Organisationen, eine möglichst beeindruckend Zahl von Unterzeichnern auf der Website www.dataretentionisnosolution .com/index.php?lang=de sammeln zu können, um die Kommission und das Parlament davon zu überzeugen, dass die angestrebte Vorratsdatenspeicherung keine Lösung ist, um Kriminalität und Terror zu bekämpfen. Unterstützer werden gebeten, die Information über die Petition zu verbreiten. Dies kann durch Platzierung eines Banners auf den eigenen Webseiten oder Homepages geschehen oder indem in Mailinglisten über die Petition informiert wird.