4/2005

Datenschutz Nachrichten

28. Jahrgang
ISSN 0137-7767
9,00 Euro

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

Big Brother Awards 2005

BBA Deutschland ■ BBA Schweiz ■ BBA Österreich ■ Datenschutznachrichten ■ Technik ■ Gentechnik ■ Rechtsprechung ■ Buchbesprechungen ■ Betriebliche Datenschutzbeauftragte ■ Vorratsdatenspeicherung ■ Koalitionspläne ■ Prime Projekt ■ Datenschutzaufsicht ■ Gesundheitskarte

Die neue Webseite der DVD in modernem übersichtlichen Design: www.datenschutzverein.de

Termine

21.01.2006
DVD-Vorstandssitzung in Frankfurt*

07.02.2006
Redaktionsschluss DANA 1/2006
Datenschutz in Europa

09.04.2006
DVD-Vorstandssitzung in Berlin*

07.05.2006
Redaktionsschluss DANA 2/2006
Vorratsdatenspeicherung

02.07.2006
DVD-Vorstandssitzung in Bonn*

07.08.2006
Redaktionsschluss DANA 3/2006
Arbeitnehmer-Datenschutz

07.11.2006
Redaktionsschluss DANA 4/2006
Big Brother Awards 2005

* (interessierte DVD-Mitglieder können gerne teilnehmen, bitte in der Geschäftsstelle melden)

Mitgliederversammlung der DVD in Bonn

Am Sonntag, den 23.10.2005 fand in Bonn die jährliche Mitgliederversammlung der DVD statt.

Der Vorstand unter Führung von Sönke Hilbrans konnte über ein erfolgreiches Jahr 2005 berichten. Die stetig steigenden Mitgliederzahlen belegen ein zunehmendes Bewusstsein für den Datenschutz in der Bevölkerung. Aufgrund der umsichtigen Haushaltsführung ist die finanzielle Situation weiterhin entspannt.

Das neue Layout der DANA ist bei Mitgliedern und Abonnenten sehr gut angekommen. Die DVD präsentiert sich seit Ende Oktober nun auch mit einer neu gestalteten Webseite. Noch im alten Design hatten im Laufe des Jahres die Besuche stetig zugenommen, der neue Auftritt dürfte die Bekanntheit der DVD im Internet weiter verbessern.

Die Presseerklärungen der DVD stießen auf gewohnt hohe Resonanz in den Medien; die weiter steigende Nutzung des Presseverteilers bestätigt das Interesse an Datenschutzthemen. Durch zahlreiche Vorträge und Schulungen konnten die Vorstandsmitglieder erfolgreich Datenschutzwissen vermitteln.

Beim BigBrotherAward, in dessen Jury die DVD durch Karin Schuler vertreten ist, nahm die Zahl der Meldungen dieses Jahr erneut zu.

Roland Schäfer, dessen Amtszeit als stellvertretender Vorsitzender ablief, wurde ohne Gegenstimmen für weitere drei Jahre wiedergewählt.

DANA
Datenschutz Nachrichten
ISSN 0137-7767
28. Jahrgang, Heft 4

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.

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

Abbildungen
Titelbild: Frans Jozef Valenta
S. 6, 9, 13, 14 Frans Jozef Valenta

Bürger voll unter Kontrolle

Die neue Regierungskoalition zeigt, wie es geht: Zuerst wurde die Mauterhebungs-Infrastruktur aufgebaut, selbstverständlich für einen berechtigten Zweck und gesetzlich garantiert nicht zur Überwachung der Bürger. Man wartet ab und schließlich gibt es einen einzelnen Vorfall, den man zum Anlass nimmt, alle bisherigen Versprechen zu vergessen und per Gesetzesänderung das Maut-System zum Überwachungssystem umzufunktionieren. Zunächst natürlich nur für die Verfolgung besonders scheußlicher Verbrechen – wer wollte sich dagegen aussprechen? Mit der Zeit wird dann der Straftaten-Katalog nach und nach erweitert, bis es fast keine Einschränkungen mehr gibt. Erstmal weiter nur für LKW-Fahrer, aber es ist ebenfalls nur eine Frage der Zeit, bis der geldhungrige Staat auch die PKW-Fahrer abkassieren und überwachen wird, nicht nur auf der Autobahn. Grenzen setzen wird – wie in der letzten Zeit üblich – erst das Bundesverfassungsgericht.
Dennoch ist die geplante Zweckänderung der Mautdatenerhebung vergleichsweise harmlos. Mit der anstehenden Vorratsdatenspeicherung von Telekommunikationsdaten wird der Staat nicht nur die Autofahrer, sondern alle handynutzenden Bürger permanent lokalisieren können, er wird auf einfachste Weise die elektronische Kommunikation der Bürger belauschen und über die Kontrolle der Webzugriffe ihre Interessen überwachen. Heute gibt man sich noch kompromissbereit, was den Umfang der Datenerhebung und die Möglichkeit des Zugriffs anbelangt. Die Erfassung sämtlicher anfallenden Daten ist schon öffentlich gefordert und der heimliche Direktzugriff auf die bei den Telekommunikationsunternehmen gespeicherten Daten analog zum Kontodatenabruf sicher auch schon geplant. Werden die Daten dann auch noch auf europäischer Ebene ausgetauscht, wird nicht mehr zu kontrollieren sein, was damit geschieht.
Die Bürger haben kaum Chancen, sich zu schützen. Das Handy könnte man auch mal abschalten, E-Mails verschlüsseln, auf Webseiten nur per anonymisierendem Proxy zugreifen. Für die meisten Menschen ist das technisch zu aufwendig und sind die damit verbundenen Einschränkungen nicht akzeptabel. Der Staat wird aber auch versuchen, vorhandene Schutzmaßnahmen einzuschränken; letztlich wird in einer zunehmend technisierten Welt, in der praktisch alles elektronisch registriert wird, auch bei einer Bereitschaft zu Einschränkungen und Verzicht ein erträgliches Leben nicht mehr möglich sein, ohne die permanente Datenerfassung hinzunehmen.
Wenn die Bürger auf die durchaus wahrgenommenen Gefahren weiter gleichgültig reagieren, wird Orwell Realität werden.

Rainer Scholl

Inhalt

BigBrotherAwards Deutschland 2005

Am Freitag, den 28.10.2005 wurden in Bielefeld in der Ravensburger Spinnerei zum sechsten Mal die BigBrotherAwards verliehen. Diese Auszeichnung wird jährlich an Personen, Firmen, Behörden und Verbände verliehen, die das informationelle Selbstbestimmungsrecht der Menschen in Deutschland mit Füßen getreten haben. Verantwortlich für die Organisation ist der Verein FoeBuD, in der Jury sind Menschen aus acht verschiedenen deutschen Bürgerrechtsgruppen vertreten.
Die Anzahl der Nominierungen für die acht Kategorien war auch 2005 wieder gestiegen. Für die meisten Zuschauer nicht überraschend, erhielten Otto Schily als ehemaliger Bundesinnenminister sowie Franz Beckenbauer mit dem Organisationskomitee für die Fußball-WM die meisten Nominierungen.

Kategorie Lifetime
Otto Schily, Bundesinnenminister a.D.

Laudator: Dr. Rolf Gössner, ILMR

Der Big Brother Award 2005 in der Kategorie »Lifetime« geht an Bundesinnenminister (a.D.) Otto Schily (SPD).

Otto Schily erhielt in diesem Jahr mit Abstand die meisten Nominierungen – wie übrigens schon im Jahr 2001, als er für seine »Otto-Kataloge« den »BigBrotherAward« in der Kategorie »Politik« verliehen bekam. In der Jury bestand große Einigkeit, dass Schily in diesem Jahr, zum mutmaßlichen Ende seiner politischen Karriere, der »Lifetime-Award« für langjährige »Verdienste« gebührt – wohlwissend, dass wir mit unserer Würdigung im Rahmen der Verleihung eines Negativpreises einer so schillernden Persönlichkeit wie Otto Schily und seiner gesamten Lebensleistung bei Weitem nicht gerecht werden können. Leider können wir hier und heute nur eine Auswahl aus der Fülle seiner beeindruckendsten Projekte und Initiativen würdigen.

Otto Schily erhält den BigBrother-Lifetime-Award 2005

- für die übereilte Einführung des biometrischen ePasses mit unausgereifter Technologie und ohne parlamentarische Legitimation,
- für seine »Verdienste« um den Ausbau des deutschen und europäischen Überwachungssystems auf Kosten der Bürger- und Freiheitsrechte,
- für seine hartnäckigen Bemühungen um die Aushöhlung des Datenschutzes und der informationellen Selbstbestimmung unter dem Deckmantel von Sicherheit und Terrorbekämpfung – Stichwort: »Antiterror«-Gesetze, auch »Otto-Kataloge« genannt,
- für seine maßgebliche Mitwirkung am Großen Lauschangriff sowie
- für seine Angriffe auf die Unabhängigkeit des Bundesdatenschutzbeauftragten.

Zu den großen Obsessionen unseres Preisträgers gehört die digitale Erfassung von biometrischen Merkmalen in Ausweispapieren. Schon ab 1. November 2005, also in wenigen Tagen, wird in der Bundesrepublik als erstem EU-Land der Reisepass mit solchen Merkmalen ausgerüstet. Auf einem kontaktlos per Funk auslesbaren RFID-Mikrochip wird neben den Personalien zunächst ein digitalisiertes Gesichtsbild gespeichert, ab März 2007 kommen zwei digitale Fingerabdrücke hinzu. Die Speicherung weiterer Merkmale, etwa Irisscan oder genetischer Fingerabdruck, ist möglich. Der nächste Schritt wird die Einführung des biometrischen Personalausweises sein.

Unter souveräner Missachtung von Parlamenten und Datenschützern und ohne gesellschaftliche Debatte boxte Schily sein Lieblingsprojekt auf EU-Ebene durch – am Bundestag vorbei, ohne demokratische Legitimation. Statt das Parlament über die Folgen für Datenschutz und Bürgerrechte entscheiden zu lassen, forcierte er eine EU-Verordnung, die unmittelbare Gesetzeswirkung in allen EU-Ländern hat. So brachte es Schily fertig, das Pass-Gesetz (§ 4) zu umgehen, das zur Festlegung der biometrischen Daten ein neues, vom Bundestag zu beschließendes Gesetz fordert.

Nicht nur wir halten Schilys selbstherrlichen Akt für zutiefst undemokratisch. Als der Bundesdatenschutzbeauftragte Peter Schaar (Grüne) diese übereilte Einführung des ePasses durch die europäische Hintertür kritisierte und ein umfassendes sicherheitstechnisches Konzept zum Schutz der Daten forderte, bezichtigte ihn Otto Schily des Amtsmissbrauchs. Es liege nicht in Schaars Kompetenz, über Sinn und Zeitpunkt der Einführung biometrischer Merkmale zu befinden, wies ihn Schily via Deutschlandfunk zurecht und empfahl ihm gebieterisch »mehr Zurückhaltung«, auf dass er mit seinen Einwänden sein Amt nicht mehr missbrauche.

Mit diesem selbstgerechten Angriff auf die Unabhängigkeit des Datenschutzbeauftragten wollte der beratungsresistente Schily offenbar einen fachkundigen Kritiker in seinem eigenen Verantwortungsbereich zum Schweigen bringen. Doch es gehört zu den Pflichten eines Datenschutzbeauftragten, die betroffene Bevölkerung darauf aufmerksam zu machen, dass bis heute keine transparente Risikoanalyse existiert, um Missbrauch und Systemanfälligkeiten der Biometrie in Ausweisen überhaupt einschätzen zu können. Nach einer Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die neue Technologie weder praxistauglich noch ausgereift. So ist die Gesichtserkennung stark fehlerbehaftet, allein schon, weil sich Gesichter im Laufe der Jahre erheblich verändern. Es steht zu befürchten, dass täglich Tausende Menschen an Flughäfen zurückgewiesen und in ihrer Reisefrei-

Preisträger der Big Brother Awards 2006 in Deutschland

Kategorie	Preisträger	Begründung
Lifetime	Otto Schily, Bundesinnenminister a.D.	Aktuell für die Einführung des biometrischen Reisepasses mit unsicherer Technik, die zu einer erkennungsdienstlichen Behandlung der gesamten Bevölkerung führt. Für sein Lebenswerk, den Ausbau des deutschen und europäischen Überwachungssystems und die Aushöhlung des Datenschutzes auf Kosten der Bürger- und Freiheitsrechte.
Wirtschaft	Dirk Otten, Saatgut Treuhand Verwaltungs GmbH	Für den Aufbau einer Kontrollstruktur zum Eintreiben von Nachbaugebühren in der Landwirtschaft. Die Saatgut Treuhand beschaffte sich Daten von Genossenschaften, verklagte auskunftsunwillige Bauern und führte verdeckte Testeinkäufe durch.
Behörden & Verwaltung	Christian Wulf, Regierung des Landes Niedersachsen	Unter Verstoß gegen die EU-Datenschutzrichtlinie soll die Aufsicht über den Datenschutz in der Wirtschaft dem Innenministerium zugeordnet werden. Die EU hat wegen dieser Praxis in anderen Bundesländern bereits ein Vertragsverletzungsverfahren eingeleitet.
Kommunikation	Erhard Rex, Generalstaatsanwaltschaft Schleswig-Holstein	Für die großflächige Fahndung nach Zeugen mittels Handy-Ortung. Mehrere tausend Personen wurden anschließend ohne konkreten Tatverdacht als mögliche Verdächtige behandelt. Die Staatsanwaltschaft verweigerte die Aktenherausgabe gegenüber der Datenschutzaufsicht.
Technik	Diverse Kandidaten	Für die schleichende Degradierung von Menschen zu überwachten Objekten und der Verharmlosung der Folgen von flächendeckender Überwachung an alle »Überwachungsfetischisten«.
Verbraucherschutz	Franz Beckenbauer, WM-Organisationskomitee	Für die inquisitorischen Fragebögen zur Bestellung von WM-Tickets, die geplante Weitergabe der Adressen an FIFA und Sponsoren sowie der Nutzung von RFID-Chips in den Eintrittskarten, um im Interesse eines Sponsors eine Kontroll- und Überwachungstechnik salonfähig zu machen.
Politik	Volker Bouffier, Innenmister Hessen	Für das »präventive« Orten von Mobiltelefonen, die DNA-Analyse bei Kindern unter 14 Jahren, für die Einführung des Scannens von KFZ-Kennzeichen auch ohne Straftatverdacht sowie den Einsatz von Videoüberwachung bei Personenkontrollen.
Regionalpreis	Grundschule Ennigloh, Volksbank Oeynhausen Herford, Sparkasse Herford	Für die Weitergabe der Namen von Schulanfängern an diverse Geldinstitute zum Zwecke der Werbung.

heit beschränkt werden, weil ihre digitalen Fotos oder Fingerabdrücke von der Software nicht akzeptiert werden oder einem Vergleich mit dem leibhaftigen Original nicht Stand halten. Solche Personen kommen in Rechtfertigungszwang, schlimmstenfalls geraten sie in einen bösen Verdacht. Schily nimmt das wissentlich in Kauf.

Elektronische Ausweise sind zudem missbrauchsanfällig: Die biometrischen Daten können an allen Kontrollstellen im In- und Ausland ausgelesen und in Datenbanken gespeichert werden – ohne dass die Betroffenen wissen, wer auf die sensiblen Daten Zugriff hat und was anschließend mit ihnen passiert. Selbst das kontaktlose und daher unbemerkte Auslesen der RFID-Chips per Funk ist nicht wirklich auszuschließen, so dass nicht nur Grenzkontrollstellen, sondern auch unbefugte Dritte Bewegungsprofile von arglosen Passinhabern anfertigen könnten.

Zwar konnten die Grünen im Bundestag Schilys ursprünglichen Plan, alle biometrischen Daten in einer Zentraldatei zu speichern, bislang noch verhindern. Doch auch dezentrale Speicherungen würden Risiken bergen: Mit geringem Mehraufwand könnten biometrische Passdaten aus dezentralen Dateien automatisch mit Fahndungsdateien und Fingerabdrücken von Straftätern und Verdächtigen abgeglichen werden, aber auch mit Fingerabdrücken, die an Tatorten gefunden werden. Und die digitalisierten Gesichtsbilder könnten etwa mit Video-Aufnahmen aus dem öffentlichen Raum abgeglichen werden, um eine verdächtige oder gesuchte Person herauszufiltern. Ein großer Schritt zum Generalverdacht gegen alle Bürgerinnen und Bürger dieses Landes – oder gleich ganz Europas, denn auf EU-Ebene gibt es bereits Pläne für eine biometrische Zentraldatei.

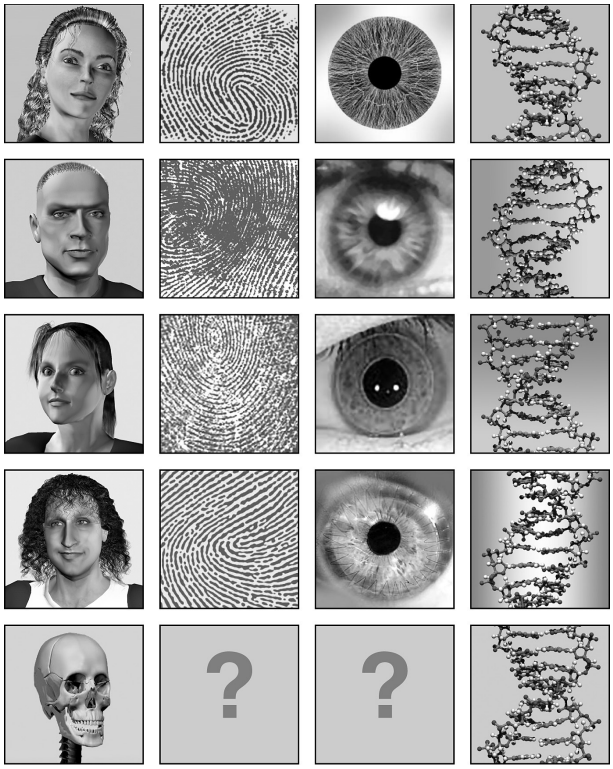
Im Zusammenhang mit elektronischen Ausweispapieren wird eine milliardenteure Überwachungsinfrastruktur mit hohem Missbrauchspotential aufgebaut. Für die Bürger steigen die Kosten eines Reisepasses um mehr als das Doppelte von 26 auf 59 Euro – wie hoch die staatlichen Subventionen pro ePass liegen, wagen wir nicht zu schätzen. Doch der riesige Kostenaufwand steht in keinem vernünftigen Verhältnis zum angeblichen Sicherheitsgewinn. Denn auch der ePass mit seinen biometrischen Merkmalen kann manipuliert werden. Im Übrigen gelten die bisherigen bundesdeutschen Ausweispapiere schon jetzt als die fälschungssichersten der Welt. Gleichwohl verkaufte Otto Schily sein biometrisches Projekt als großen Fortschritt für die Sicherheit und als wichtigen Baustein im Kampf gegen organisierte Kriminalität und internationalen Terrorismus. Mit dieser Behauptung nährt Schily allenfalls eine riskante Sicherheitsillusion, denn der ePass führt keineswegs automatisch zu mehr Sicherheit. Weder die Selbstmord-Anschläge in New York, noch diejenigen von Madrid oder London hätten mit der neuen Technologie verhindert werden können. Schließlich gibt es kein

biometrisches Merkmal, das signalisiert: »Dieser Pass gehört einem potentiellen Terroristen – bitte vor jedem Anschlagsversuch kontrollieren«.

Otto Schily nötigte uns den ePass nicht nur als vermeintliches Sicherheitsinstrument auf, sondern auch als Innovationsprojekt zur Sicherung nationaler Standortvorteile: Die rasche Einführung der biometrischen Verfahren vor allen anderen EU-Staaten liege im ureigenen deutschen Interesse. Damit »bringen wir den Beweis«, so Schily in einer Rede am 2. Juni 2005, »wie rasch sich deutsche Firmen auf die neue Sicherheitstechnik und auf den zukunftsorientierten Wachstumsmarkt der Biometrie eingestellt haben«. Deutschland nehme so in Sachen Sicherheit eine Führungsrolle in der EU ein. Wir sehen darin allerdings eine verdeckte Wirtschaftsförderung, etwa zugunsten der Bundesdruckerei GmbH und der Chiphersteller Philips und Infineon, aber auch vorauseilenden Gehorsam gegenüber den USA, die in Sachen Biometrie auf die europäischen Regierungen massiven Druck ausgeübt hatten.

Die biometrisch-digitale Erfassung der gesamten Bevölkerung ist nicht nur ein unverhältnismäßiger Eingriff in die informationelle Selbstbestimmung, sondern auch eine Misstrauenserklärung an die Bevölkerung. Sie muss sich behandeln lassen, wie bislang nur Tatverdächtige oder Kriminelle im Zuge einer Erkennungsdienstlichen Behandlung. Mit Schilys biometrischer Obsession werden Menschen im Namen vermeintlicher Sicherheit zu bloßen Objekten staatlicher Macht degradiert – ohne dass dies auch nur durch »Gefahrennähe« des Einzelnen gerechtfertigt wäre. Otto Schily kontert mit dem zynischen Argument, dass »die Würde des Fingers« auch nicht größer sei als die des Gesichts (lt. SZ 24.8.04). Im Übrigen beruft er sich gerne auf spanische Ausweise, die bereits nicht-digitalisierte Fingerabdrücke enthalten. Allerdings verschweigt er, dass es sich dabei um ein Relikt aus faschistischen Franco-Zeiten handelt. Und er verschweigt, dass damit weder Anschläge der baskischen ETA noch die Anschläge von Madrid verhindert werden konnten.

Demnächst wird hierzulande selbst den hartnäckigsten Sicherheitsfanatikern das Lachen vergehen, denn ein solches wird auf den neuen Digitalfotos verboten sein – offene Münder oder blitzende Zähne könnten nämlich die Hightech-Lesegeräte irritieren. Lediglich ein leichtes Grinsen mit geschlossenen Lippen und bei ansonsten neutralem Gesichtsausdruck wird noch statthaft sein. Beim elektronischen Gesichtsabgleich werden wohl Vollbärte, dicke Brillen, aufgespritzte Lippen oder Nasenoperationen genauso zum Sicherheitsproblem, wie das unvermeidliche Älterwerden und deutlicher werdende Falten im Gesicht. Mit dem »BigBrother-Lifetime-Award« würdigen wir die Wandlung des anthroposophisch geprägten Preisträgers Otto Schily vom linksliberalen Anwalt über den realogrünen Oppositionspolitiker zum staatsautoritären SPD-Polizeiminister – eine Metamorphose, die viele Menschen nur schwer nachvollziehen können. Vor vielen, vielen Jahren stand sein Name als herausragender Strafverteidiger der außerparlamentarischen Linken und besonders im Stammheimer RAF-Prozess für den Kampf gegen Deformationen des Rechtsstaates, die dieser damals im Zuge der Terrorismusbekämpfung erleiden musste. Es war jene Zeit, in der Schily noch die mahnenden Worte einer Erklärung der »Humanistischen Union« unterschrieben hatte: »Man bekämpft die Feinde des demokratischen Rechtsstaats nicht mit dessen Abbau, und man verteidigt die Freiheit nicht mit deren Einschränkung« (1978).



Die biometrischen Zukunftspläne: Todsichere Identifikationen

So ändern sich die Zeiten – dennoch will Schily von biografischen Brüchen nichts wissen: Vom »Terroristenprozess« in Stammheim bis zu seinen »Antiterror«-Gesetzen – kontinuierlich wähnte er sich im Einsatz für den Rechtsstaat, wenn auch in unterschiedlichen Rollen. Doch Schily hat nicht nur die Rollen, sondern die Seiten gewechselt – und zwar kompromisslos: Aus dem eloquenten Strafverteidiger, der im Interesse seiner Mandanten rechtsstaatliche Prinzipien gegen staatsautoritäre Übergriffe verteidigte, wurde spätestens in seiner Funktion als Bundesinnenminister ein autoritärer Staats-Anwalt, der die Macht des Staates zu Lasten der individuellen Freiheitsrechte ausgebaut hat. Schily machte den Staat zu seinem Mandanten, für dessen Autorität und Stärke er sich auf geradezu fundamentalistische Weise eingesetzt hat. Schon länger hält er die Angst vor dem Leviathan, also vor einer entfesselten Staatsmacht, für ein Problem von vorgestern. Der Einzelne müsse heute nicht mehr vor dem Staat geschützt werden, nur noch vor Kriminalität und Terror. Jedes Misstrauen gegen staatliche Maßnahmen ist im Schily-Staat demnach unangebracht, ja verwerflich, zumindest verdächtig.

Schon als Oppositionspolitiker hatte der von den Grünen zur SPD konvertierte Schily die spätere rot-grüne Koalition mit schweren Hypotheken belastet – so mit dem Großen Lauschangriff. Schily, der in Stammheim selbst Opfer von Lauschangriffen geworden war, hatte an der dafür nötigen Verfassungsänderung, die ohne die SPD nicht zustande gekommen wäre, maßgeblich mitgewirkt – und damit an der Aushöhlung des Grundrechts auf Unverletzlichkeit der Wohnung. Jahre später hat das Bundesverfassungsgericht dieses Machwerk für weitgehend verfassungswidrig erklärt. Verfassungswidrige Betätigung – streng genommen ein Fall für den »Verfassungsschutz«, im Fall Schily offenbar eine höchst paradoxe Empfehlung für den Posten des In-

nenministers, der schließlich auch als Verfassungs(schutz)minister fungiert.

Als Geburtshelfer des Großen Lauschangriffs hatte Schily ursprünglich sogar für eine noch weit schärfere Fassung gefochten: Wäre es nach ihm gegangen, wären elektronische Wanzen auch gegen Berufsgeheimnisträger wie Journalisten oder Ärzte einsetzbar gewesen. Seit jener Zeit sind zumindest erhebliche Zweifel an seiner Verfassungstreue angebracht, zumal er zuvor schon die faktische Abschaffung des Asylgrundrechts betrieben hatte. Man muss sich seitdem fragen: Ist Schily bereit, jederzeit für die freiheitlich-demokratische Grundordnung einzutreten, wie es von jedem Beamten gefordert wird, oder neigt er dazu, diese vermehrt zugunsten der Staatsräson und zu Lasten der Bürgerrechte einzuschränken?

Unser Preisträger hat mit seiner Law-and-order-Politik einen gehörigen Beitrag dazu geleistet, dass bürgerrechtliche Grundwerte in der herrschenden Sicherheitspolitik mehr und mehr verdrängt worden sind – ganz besonders nach den Terroranschlägen vom 11.9.2001 in den USA. Damals verkündete Schily als Bundesinnenminister, die rot-grüne Koalition werde »alle polizeilichen und militärischen Mittel aufbieten, über die die freiheitlich-demokratische Staatsordnung, die wehrhafte Demokratie verfügt«. Mit dieser martialischen Androhung trat Schily einen fatalen Gesetzesaktionismus los, bediente den krankhaften Sicherheits-Wahn so mancher Bürger, und nutzte ihn zur Legitimierung lang gehegter Nachrüstungspläne, ließ sie aus den Schubladen der Macht kramen, zu voluminösen »Otto-Katalogen« schnüren und mit Antiterror-Etiketten bekleben. Anstatt der Bevölkerung die Wahrheit über Unsicherheitsfaktoren in einer Risikogesellschaft zuzumuten und deutlich zu machen, dass absolute Sicherheit leider nicht und nirgendwo zu erreichen ist, machen Schily und andere Regierungspolitiker mit symbolischer Politik bis heute unhaltbare Sicherheitsversprechen.

Mit den so genannten Antiterror-Gesetzen, für die Otto Schily wie kein anderer steht, haben Polizei und Geheimdienste erweiterte Aufgaben und Befugnisse erhalten. Damit wurde die ohnehin hohe Kontrolldichte in Staat und Gesellschaft noch weiter erhöht. Vermehrt können Beschäftigte in so genannte lebens- oder verteidigungswichtigen Einrichtungen geheimdienstlichen Sicherheitsüberprüfungen unterzogen werden – mitunter auch ihre Lebenspartner und ihr soziales Umfeld. Betroffen sind Einrichtungen und sicherheitsempfindliche Stellen, so heißt es im Gesetz wörtlich, »die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung entstehen lassen würde«. Gemeint sind Einrichtungen, die der Versorgung der Bevölkerung dienen, wie Energie-Unternehmen, Krankenhäuser, Chemie-Anlagen, Bahn, Post, Banken, Telekommunikationsbetriebe, aber auch Rundfunk- und Fernsehanstalten können betroffen sein.

Migrantinnen und Migranten, unter ihnen besonders Muslime, werden praktisch per Gesetz unter Generalverdacht gestellt, zu gesteigerten Sicherheitsrisiken erklärt und einem rigiden Überwachungssystem unterworfen – denken wir nur an die biometrische Erfassung von Fingerabdrücken und Stimmprofilen, an geheimdienstliche Regelanfragen, an erleichterte Auslieferungen und Abschiebungen. Ohne wirklichen Nachweis, dass von ihnen mehr Terror ausgehe als von Deutschen, werden Migranten oft – unter Verletzung des Gleichheitsgrundsatzes – einer entwürdigenden Sonderbehandlung unterzogen, die für viele existentielle Folgen haben kann.

Die »Antiterror«-Gesetze bewirken eine verhängnisvolle Lockerung des Datenschutzes, ganz im Sinne Otto Schilys, der den Datenschutz ohnehin für »übertrieben« hielt – gerade so, als könnten selbstmörderische Terroranschläge mit weniger Datenschutz und mehr Eingriffen in die Privatsphäre der Bürger verhindert werden. Doch die meisten Gesetzesverschärfungen taugen nur wenig zur Bekämpfung eines religiös-aufgeladenen, selbstmörderischen Terrors; sie schaffen kaum mehr Sicherheit, gefährden aber die Freiheitsrechte um so mehr. Etliche der Antiterror-Maßnahmen sind unverhältnismäßig, ja maßlos – sie zeigen Merkmale eines nicht erklärten Ausnahmezustands und eines autoritären Präventionsstaates, in dem letztlich Rechtssicherheit und Vertrauen verloren gehen. Die Unschuldsvermutung, eine der wichtigsten rechtsstaatlichen Errungenschaften, verliert in dieser Sicherheitskonzeption ihre machtbegrenzende Funktion. Der Mensch wird zum potentiellen Sicherheitsrisiko, der seine Harmlosigkeit und Unschuld nachweisen muss – während Otto Schily die vermeintliche Sicherheit zum Supergrundrecht erklärt, das die wirklichen Grundrechte der Bürger – als Abwehrrechte gegen Eingriffe des Staates – in den Schatten stellt.

In seinem missionarischen Eifer als Staatsschützer schreckte der Preisträger selbst vor extremistischen Forderungen aus dem Arsenal von Diktaturen nicht zurück: So würde er allzu gerne »gefährliche« Personen ohne konkreten Verdacht in präventive Sicherungshaft nehmen lassen. Otto Schilys zuweilen obrigkeitsstaatliche Interpretation des Rechtsstaats zeigt sich auch in seinen folgenden Staatsschutzprojekten:: Er hat mit einem gemeinsamen Antiterror-Lagezentrum und mit dem Plan einer zentralen »Islamistendatei« Grundsteine für einen Datenverbund aller Geheimdienste und des Bundeskriminalamts gelegt. Eine noch engere Vernetzung würde die Aufhebung des verfassungsmäßigen Gebots der Trennung von Polizei und Geheimdiensten be-

Die Big Brother Award Jury 2005

Rena Tangens & padeluun
Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)
www.foebud.de

Karin Schuler
Deutsche Vereinigung für Datenschutz e.V. (DVD)
www. datenschutzverein.de

Frank Rosengart
Chaos Computer Clulb e.V. (CCC)
www.ccc.de

Alvar C.H. Freude
Förderverein Informationstechnik und Gesellschaft e.V. (Fitug)
www.fitug.de

Werner Hülsmann
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FifF)
www.fiff.de

Dr. Fredrik Roggan
Humanistische Union e.V. (HU)
www.humanistische-union.de

Dr. Rolf Gössner
Internationale Liga für Menschenrechte (ILMR)
www.ilmr.org

deuten – immerhin eine Konsequenz aus den bitteren Erfahrungen mit der Gestapo im Nationalsozialismus. Damit nimmt Schily eine Machtkonzentration in Kauf, die kaum noch wirksam kontrollierbar sein wird.

Schily hat sich mit Vehemenz dafür eingesetzt, dass alle Telekommunikationskontakte – ob per Telefon, SMS, Email oder Internet – zur Terror- und Kriminalitätsbekämpfung deutschland- und europaweit für mindestens zwölf Monate auf Vorrat gespeichert werden. Also: Wer hat mit wem, wann, wie oft und wie lange von wo nach wo fernmündlich oder schriftlich kommuniziert, welche SMS- oder Internet-Verbindungen genutzt, welche Suchmaschinen mit welchen Begriffen benutzt, welche Websites besucht und mit welchen Email-Empfängern kommuniziert? Mit dieser beispiellosen Vorratsdatensammlung ließe sich das Kommunikations- und Konsumverhalten einzelner Telekommunikationsnutzer heimlich ablesen – Verhaltens- und Kontaktprofile inklusive.

Auch die Pressefreiheit ist vor Otto Schily keineswegs sicher: So rechtfertigt er undifferenziert und hartnäckig die höchst umstrittene Durchsuchung der Redaktionsräume des Monatsmagazins »Cicero« und der Privatwohnung eines Journalisten durch das Bundeskriminalamt (BKA), zu der Schily die Ermächtigung erteilt hatte. Der Journalist hatte zulässigerweise aus einem geheimen BKA-Papier zitiert. Weil die undichte Stelle im BKA, also der Lieferant des Geheimdossiers, nicht zu finden war, wurde gegen den Journalisten wegen »Beihilfe zum Geheimnisverrat« ermittelt – stundenlange Razzien und kistenweise Beschlagnahme von Recherchematerial inklusive. Das gesuchte Dokument wurde nicht gefunden, dafür »Zufallsfunde« zuhauf, die mit dem Durchsuchungsanlass nicht das Geringste zu tun haben, aber zu weiteren Ermittlungsverfahren führten. Mit dieser Verdächtigung, als Journalist am Verrat von Dienstgeheimnissen selbst beteiligt gewesen zu sein, lassen sich Informantenschutz und Zeugnisverweigerungsrecht praktisch aushebeln – und damit das hohe Gut der Pressefreiheit. Solche Praktiken können letztlich dazu führen, kritische Journalisten einzuschüchtern und von investigativen Recherchen abzuhalten.

So sehen die fatalen Folgen aus, wenn man, wie der Preisträger, die Sicherheit zum Grundrecht kürt, wenn man die Staatsräson zum Verfassungsgrundsatz erhebt, die alles andere dominiert: Dann herrscht partielle Willkür, dann werden Bürgerrechte zur Makulatur. Angesichts überzogener Antiterrormaßnahmen und einer eskalierenden Sicherheitsdebatte warnte der frühere Datenschutzbeauftragte und Vorsitzende des Nationalen Ethikrates, Spiros Simitis, eindringlich: »Jetzt ist der Punkt erreicht, wo wir am Grundbestand unserer verfassungsrechtlichen Vorgaben angelangt sind – der Übergang in eine totalitäre Gesellschaft ist fließend«. Und der Soziologe Ulrich Beck sieht mit der »Risikogesellschaft«, in der wir leben, ohnehin eine »Tendenz zu einem ›legitimen‹ Totalitarismus der Gefahrenabwehr« verbunden: Ausgestattet mit »dem Recht, das Schlimmste zu verhindern«, schaffe sie in »nur allzu bekannter Manier das andere Noch-Schlimmere«. Anstatt dieser fatalen Tendenz wirksam entgegenzutreten, betätigte sich Otto Schily als ihr missionarischer Vollstrecker. Selbst sein Ministerkollege Wolfgang Clement fand deutliche Worte für Otto Schilys freiheitsbegrenzendes Wirken, als er seine Zeit nach dem Ausstieg aus der Bundesregierung so skizzierte: »Ich bin ein freier Mensch und werde jetzt von meinen Freiheitsrechten Gebrauch machen, und zwar ausgiebig – natürlich nur in dem Rahmen, den Otto Schily mir noch zur Verfügung stellt ...« (WDR 10.10.2005).

Herzlichen Glückwunsch zum »Big-Brother-Lifetime-Award«, Herr Schily.

Kategorie Wirtschaft
Dirk Otten, Saatgut Treuhand Verwaltungs GmbH

Laudatorin: Rena Tangens, FoeBuD

Den Big Brother Award 2005 in der Kategorie »Wirtschaft« erhält die Saatgut-Treuhand Verwaltungs GmbH, Bonn, vertreten durch ihren Geschäftsführer Dirk Otten.

Bauern erhalten Post von Rechtsanwälten, Felder werden kontrolliert, die Kundendaten bei Genossenschaften ermittelt, über 2.500 Bauern, die die Auskunft verweigern, wurden bereits verklagt. Zusätzlich sind verdeckte Testkäufer der Saatgut-Treuhand unterwegs, kaufen auf Bauernhöfen Kartoffeln und stellen damit Beweismaterial sicher, um Täter zu überführen.

Was geht hier vor? Welcher Straftat werden die Bauern bezichtigt: Gefährliche Giftcocktails gespritzt? Das Grundwasser mit Gülle verunreinigt? Heimlich gentechnisch veränderte Pflanzen angebaut?

Nein – viel schlimmer – diese Bauern werden verdächtigt, Feldfrüchte aus eigenem Anbau aufzubewahren und für die Aussaat im nächsten Jahr zu verwenden – also ihre eigene Ernte auszusäen.

Wir stutzen: Genau das tun Bauern schon seit Jahrtausenden – die eigene Ernte wieder aussäen. Wo liegt das Problem? Nun, seit den 90er Jahren gibt es eine internationale Vereinbarung (die Neufassung der so genannten UPOV-Konvention), die erst ins EU-Recht und schließlich auch ins deutsche Recht eingegangen ist und die besagt: Für Saatgut muss eine Lizenzgebühr an die Saatgutfirma, die die Sorte angemeldet hat, bezahlt werden. Und zwar nicht nur einmal, wenn das Saatgut gekauft wird, sondern (seit der Änderung des deutschen Sortenschutzgesetzes von 1997) jedes Jahr wieder, auch wenn das Saatgut die eigene Ernte ist. Das sind die so genannten Nachbaugebühren. Und um diese von den Landwirten einzutreiben, wurde die Saatgut-Treuhand aktiv.

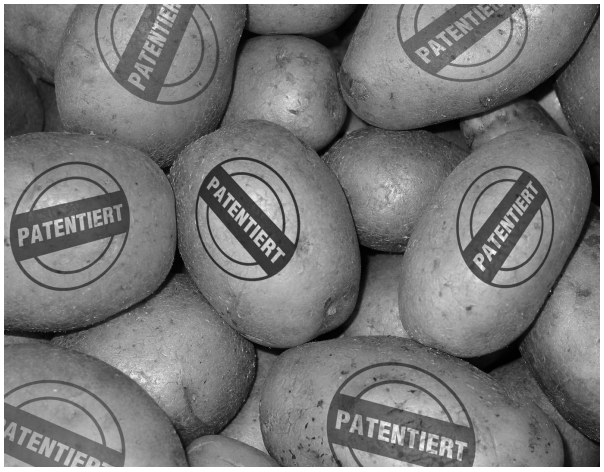
Eine beim deutschen Bundessortenamt angemeldete Sorte erhält Sortenschutz – bei Getreide 25 Jahre und bei Kartoffeln 30 Jahre. Damit erhalten die Züchter der Sorte das Recht, innerhalb dieser Zeit Lizenzgebühren beim Verkauf von Saatgut dieser Sorte zu erheben.

Exkurs: Linda – eine Kartoffelsorte wird »illegal«:

Welch absurde Blüten das Geschäft mit den Lizenz- und Nachbaugebühren treibt, wird an der Geschichte von »Linda« deutlich. Die Kartoffelsorte Linda war auf bestem Wege, ihren dreißigsten Geburtstag zu erreichen – und damit lizenzfrei zu werden. Die Saatzuchtfirma Böhm / Europlant fand das keinen Grund zum Feiern, sondern zog kurzerhand zum 31. Dezember 2004 die Zulassung von »Linda« von der Bun-

dessortenliste zurück. Das bedeutet, Linda darf nicht mehr als Pflanzkartoffel angebaut und vermehrt werden. Die Logik ist klar: Landwirte sollen gefälligst neue Sorten anbauen, an denen sich Lizenzgebühren verdienen lassen. Doch Lindas Beliebtheit, speziell im Norden Deutschlands, wurde von der Saatgutfirma unterschätzt: Ein Proteststurm von Verbrauchern brach los, rebellische Bauern bauten weiter Linda an, das Bundessortenamt verlängerte die Auslauffrist für Linda bis 2007 und ein engagierter Bauer bemüht sich um die Wiederanmeldung der Sorte.

Und auch allgemein wächst der Widerstand der Bauern, z.B. gegen die Nachbaugebühren. 16.000 Bauern verweigern mittlerweile die Auskunft an die Saatgut-Treuhand. Dabei geht es nicht darum, die Züchter um ein Honorar für ihre Leistung zu prellen. Die »IG Nachbau«, gegründet von Bauern in der Arbeitsgemeinschaft bäuerliche Landwirtschaft (AbL e.V.), hat ein alternatives Konzept für einen Saatgutfonds entwickelt, in den Bauern, Verbände, Züchter und der Staat einen Beitrag einzahlen. Aus diesem Fonds würden die Züchter bezahlt; Mitbestimmung würde helfen, die Vielfalt der Pflanzensorten zu erhalten, vom alleinigen Zuchtziel »Ertragssteigerung« Abstand zu nehmen und die Vielfalt der Pflanzensorten zu erhalten.



Saatgut Treuhand fahndet nach Patent-Kartoffeln

Was tut die Saatgut-Treuhand? Die Saatgut-Treuhand schreibt Briefe und will detailliert wissen, was wo angebaut wird. Mehr als 2.500 Bauern, die keine Auskunft geben, wurden bereits verklagt, und zwar durch alle Instanzen.

Doch die Bauern halten dagegen – mit Erfolg: der Europäische Gerichtshof hat im Frühjahr 2003 entschieden, dass es keine allgemeine Auskunftspflicht der Bauern gegenüber der Saatgut-Treuhand gibt. Im Herbst 2004 wurde auch die allgemeine Auskunftspflicht der Saatgutaufbereiter vom EuGH verneint. Ebenso urteilte der Bundesgerichtshof: Saatgutfirmen müssen Anhaltspunkte haben, dass ein Bauer über Saatgut der von ihr geschützten Sorte verfügt und damit Nachbau betreiben könnte, bevor sie Auskunft verlangen können. Ein Anhaltspunkt kann nach dem EuGH der Erwerb einer geschützten Sorte sein.

Doch die Saatgut-Treuhand fordert nach wie vor Auskunft (auch wenn sie mittlerweile formlose Meldungen akzeptiert), lässt auskunftsunwillige Bauern von Rechtsanwaltskanzleien mit Drohbriefen traktieren, zusätzlich schickt die Saatgut-Treuhand verdeckte Testkäufer auf Höfe, die gegen Quittung ein paar Zentner Kartoffeln kaufen und ganz nebenbei fragen, ob sich die Kartoffeln auch zu Pflanzzwecken eignen – wer da nicht unter Zeugen entschieden verneint, wird von der Saatgut-Treuhand verklagt.

Warum gibt es dafür einen BigBrotherAward?

Dafür gibt es zwei Gründe. Der erste: Woher die Saatgut Treuhand die Adressen der Bauern hat, bleibt ihr Geheimnis. Nach eigenen Angaben hat sie dafür Telefon-CDs nach Berufsbezeichnungen oder Angaben wie »Hof Soundso« durchsucht. Jedoch erhielten auch Bauern von der Saatgut Treuhand Post, die keine solche Angaben im Telefonbuch haben. In dem Jahrbuch »Kritischer Agrarbericht« wurde die Vermutung geäußert, dass der Deutsche Bauernverband der Saatgut Treuhand sein Mitgliederverzeichnis zur Verfügung gestellt habe. Sicher ist, dass Raiffeisen-Genossenschaften wie die BayWa in Süddeutschland nicht nur ihre Kundenadressen, sondern gleich auch Belege über deren kompletten Einkauf an die Saatgut-Treuhand weitergegeben haben.

Der zweite Grund: Hier wird eine neue zentrale Datensammlung angelegt, mit detaillierten Angaben wo, was, von wem, auf welcher Fläche, wie viel etc. angebaut wird. Die Saatgut Treuhand ist dabei keine neutrale Clearingstelle, sondern sie ist im Auftrag der Saatgutindustrie tätig – sie ist nicht zufällig auch im selben Gebäude wie der BDP (Bundesverband deutscher Pflanzenzüchter) und der ESA (European Seed Association) in Bonn angesiedelt.

Diese Informationen über Flächennutzung gelangen so in die Hände der Saatgutkonzerne, die ein großes kommerzielles Interesse am »gläsernen Landwirt« haben. Wer über die Anbauplanung von Bauern Bescheid weiß, kann durch gezielte Rabatte hier und Preiserhöhungen dort steuern, was hierzulande in Zukunft angebaut – und gegessen – wird. Die Erhebung von Nachbaugebühren ist dabei ein wichtiger Mosaikstein, um an die Daten zu kommen. Wissen ist Macht.

Die Saatgutindustrie konzentriert sich immer mehr, Chemiekonzerne kaufen sich ein – die Global Player Novartis, Bayer und Monsanto möchten gerne Saatgut, Pestizide und Dünger im Kombipack verkaufen. Ihr erklärtes Ziel ist, die gesamte »Nahrungskette« zu kontrollieren, vom Saatgut über Ernte und Verarbeitung zu normierten Nahrungsmitteln bis hin zum Teller der Verbraucher.
Das obrigkeitshörige Deutschland wurde ausgewählt, um die Durchsetzbarkeit von Nachbaugebühren in Europa zu testen – andere Länder schauen gespannt auf die Entwicklung hierzulande. In Entwicklungsländern werden über 90% der Felder mit selbst gezogenem Saatgut bestellt. Hier tut sich ein gigantischer Markt auf, wenn die Industrie schafft, all diese Bauern nach und nach dazu zu bringen, jedes Jahr Saatgut neu einzukaufen.

Doch wem gehört die Natur? Pflanzensorten sind Kulturgut. Sie sind von Bauern durch ständige Selektion und Anpassung an die regionalen Gegebenheiten über die Jahrtausende gezüchtet worden. Nun werden Nutzpflanzen nach geringen Änderungen von Firmen unter Sortenschutz gestellt oder patentiert, die damit ein Monopol auf deren Anbau erwerben.

Diese Entwicklung passt in einen Trend zur Privatisierung einer Vielzahl von Dingen, die vormals Allgemeingut waren. Auf die Privatisierung und Kommerzialisierung von Gütern, die vorher frei waren, wie z.B. Wissen oder Pflanzensorten, folgt stets die Einrichtung von Kontrollinstanzen und Überwachungsmaßnahmen, um Lizenzgebühren einzutreiben. Der Daten- und Vermarktungshunger wächst ständig.

Doch die Saatgut-Treuhand wird

möglicherweise in einigen Jahren überflüssig – denn für ihre Arbeit ist eine technologische Lösung in Sicht: Das so genannte »Terminator-Gen« macht die Samen der Pflanze unfruchtbar und zwingt Landwirte dazu, jedes Jahr neues Saatgut einzukaufen. Das Terminator-Gen ist sozusagen der Kopierschutz der Saatgutindustrie. Doch so dumm werden weder Bauern noch Verbraucher sein, solche Kartoffeln zu wollen – und seien sie noch so dick.

Liebe Saatgut-Treuhand, herzlichen Glückwunsch zum Big Brother Award!

Kategorie Behörden & Verwaltung
Christian Wulf, Regierung des Landes Niedersachsen

Laudator: Werner Hülsmann, FIfF

Der BigBrotherAward 2005 in der Kategorie »Behörden und Verwaltung« geht an den Ministerpräsidenten des Landes Niedersachsen, Herrn Christian Wulff, für die Zerschlagung der Datenschutzaufsicht in Niedersachsen.

Langsam, aber stetig geben immer mehr Landesregierungen die Datenschutzaufsicht über die Wirtschaft ab und legen sie in die Hände der unabhängigen Landesdatenschutzbeauftragten. Die Niedersächsische Landesregierung allerdings hat entschieden, die Datenschutzaufsicht über die Wirtschaft zu Beginn des kommenden Jahres vom Landesdatenschutzbeauftragten an das Ministerium für Inneres und Sport zu übergeben.

Bislang war in Niedersachsen die Datenschutzaufsicht für die Wirtschaft zweigeteilt: Das Innenministerium hatte die Rechtsaufsicht und der Landesdatenschutzbeauftragte die Fachaufsicht. Er verkörperte damit die eigentlich zuständige Aufsichtsbehörde. Diese Zweiteilung war spätestens seit der Verabschiedung der EU-Datenschutzrichtlinie vom Oktober 1995 nicht mehr zeitgemäß. Dort wird gefordert, dass die Datenschutzaufsicht – nicht nur für die öffentliche Verwaltung, sondern auch im Bereich der Wirtschaft – völlig unabhängig sein muss.

Und dies aus gutem Grund. Nicht selten lassen Entscheidungen von bei Regierungspräsidien und Innenministerien angesiedelten Datenschutzaufsichtsbehörden in verschiedenen Bundesländern vermuten, dass auch die Interessen der Sicherheitsbehörden – also z.B. Polizei oder Staatsanwaltschaft – bei der datenschutzrechtlichen Beurteilung mitentscheidend waren. Beispielhaft seien hier nur zwei Entscheidungen genannt: Erstens die des Regierungspräsidiums Darmstadt zur Erlaubnis der Verbindungsdatenspeicherung bei Internet-Flatrates für bis zu sechs Monate, die – wie auch das zuständige Amtsgericht inzwischen feststellte – gesetzwidrig ist, und zweitens die Entscheidung des Innenministeriums von Baden-Württemberg zur Zulässigkeit der Einführung eines Verfahrens, bei dem mit dem Fingerabdruck bezahlt wird. Hierzu müssen natürlich die digitalen Gegenstücke der Fingerabdrücke in der Kneipe oder auch in den Zentralen der Einzelhandelsketten wie z.B. bei EDEKA gespeichert werden. In beiden Fällen haben die Ermittler ein quasi »natürliches« Interesse an diesen Datenbeständen.

Eine Änderung der Datenschutzaufsicht in Niedersachsen war also 10 Jahre nach Erlass der EU-Datenschutzrichtlinie höchste Zeit. Nur hat Niedersachsen den Schritt in die falsche Richtung gemacht. Statt also auch die Rechtsaufsicht auf den unabhängigen Landesdatenschutzbeauftragten zu übertragen, wie dies bereits in einigen anderen Bundesländern seit Jahren erfolgreich praktiziert wird, richtet die niedersächsische Landesregierung beim Ministerium für Inneres und Sport eine neue Abteilung ein. Der Landesdatenschutzbeauftragte soll künftig nur noch für die Landes- und Kommunalverwaltungen in Niedersachsen zuständig sein, die Wirtschaft wird vom Innenministerium kontrolliert. Gleichzeitig spricht die Regierung von »Synergie-Effekten«. Diese wären aber sicherlich größer, wenn man alle Kompetenzen künftig in eine Hand, nämlich die des Landesdatenschutzbeauftragten, gegeben hätte.

Pikanterweise hat die EU-Kommission im Juli 2005 gegen Deutschland ein Vertragsverletzungsverfahren wegen Missachtung der EU-Datenschutzrichtlinie eingeleitet, da die in den einzelnen Bundesländern unterschiedlichen Formen von Fach-, Rechts- und Dienstaufsicht über den Datenschutz in der Wirtschaft nicht die Forderung nach »völliger Unabhängigkeit« der Aufsichtsbehörden erfüllen. Anstatt die Datenschutzbehörden unabhängiger zu organisieren, macht die Entscheidung der niedersächsischen Landesregierung die Datenschutzaufsicht jetzt erst Recht abhängig von den Interessen der Landesregierung.

Es ist doch Augenwischerei, wenn die Niedersächsische Staatskanzlei in einer Pressemitteilung erklärt, dass mit dieser Aufgabenverlagerung auch »Reibungsverluste« im »gesetzesvorbereitenden Bereich« vermieden würden. Es ist doch offensichtlich, dass die Regierung damit den Landesdatenschutzbeauftragten für seine kritischen Stellungnahmen zu manchem Gesetzesentwurf abstraft! Die Stellungnahme zur – inzwischen für verfassungswidrig erklärten – präventiven Telekommunikationsüberwachung, in der der niedersächsische Datenschutzbeauftragte einer Gesetzesbegründung widersprach, ist hierfür nur ein Beispiel.

Hier scheint die niedersächsische Landesregierung dem scheidenden Bundesinnenminister nacheifern zu wollen. Auch diesem gefallen die Stellungnahmen »seines« Datenschutzbeauftragten nicht und so forderte er vom Bundesbeauftragten für den Datenschutz mehr Zurückhaltung und warf ihm Kompetenzüberschreitung vor. Dabei gehört es zu den Aufgaben des Bundesdatenschutzbeauftragten, sich auch zu Regierungsvorhaben kritisch zu äußern. Und es kommt nicht darauf an, ob diese Stellungnahmen der Regierung und insbesondere dem Bundesinnenminister passen oder nicht.

Zynisch ist in der Presseerklärung der Niedersächsischen Staatskanzlei zur Aufgabenverlagerung auch ein Hinweis auf Baden-Württemberg und Bayern, in denen die Datenschutzaufsicht für die Wirtschaft im Innenministerium bzw. bei einer Bezirksregierung angesiedelt ist. Denn auch dort lässt die Datenschutzaufsicht zu Wünschen übrig. Aufgrund der sehr geringen personellen Ressourcen der dortigen Aufsichtsbehörden ist es kein Wunder, dass in diesen beiden Bundesländern die Wirtschaft und auch die betroffenen Bürgerinnen und Bürger von der Datenschutzaufsicht nahezu nichts merken. Inzwischen wird daher auch dort

über eine Herauslösung der Datenschutzaufsicht aus dem Bereich der Innenministerien zumindest nachgedacht.

Der Preis geht an den Ministerpräsidenten Christian Wulff als Stellvertreter für die Gremien der niedersächsischen Landesregierung, die die Zerschlagung der Datenschutzbehörde beschlossen haben. Mildernde Umstände kommen für Herrn Wulff nicht in Betracht, da das Land Niedersachsen nicht nur dem Niedersächsischen Landesdatenschutzbeauftragten die Datenschutzaufsicht über die Wirtschaft entzieht. Es hat vielmehr auch gemeinsam mit Hessen einen Gesetzentwurf in den Bundesrat eingebracht, der – wenn er vom Bundestag angenommen wird – dazu führen würde, dass bedeutend weniger Unternehmen einen betrieblichen Datenschutzbeauftragten bestellen müssten und damit die innerbetriebliche Datenschutzkontrolle durch die betrieblichen Datenschutzbeauftragten deutlich geschwächt würde. Eine abhängige staatliche Datenschutzaufsicht über die Wirtschaft, wie sie in Niedersachsen eingeführt wird, gepaart mit einer Schwächung der innerbetrieblichen Datenschutzkontrolle lässt für den Kunden- und Arbeitnehmerdatenschutz leider nichts Gutes erwarten!

Herzlichen Glückwunsch, Christian Wulff, Ministerpräsident des Landes Niedersachsen.

Kategorie Politik
Volker Bouffier, Innenminister des Landes Hessen

Laudator: Dr. Fredrik Roggan, HU

Der Big Brother Award 2005 in der Kategorie »Politik« geht an den Innenminister des Landes Hessen, Herrn Volker Bouffier.

Sie werden ausgezeichnet für das von Ihnen zu verantwortende neue Hessische Polizeigesetz, mit dem das Fernmeldegeheimnis weiter beschnitten, die informationelle Selbstbestimmung zunehmend ausgehöhlt und der öffentliche Raum fortschreitend zu einer komplett zu überwachenden Zone degradiert wird.

Alleine die Anzahl der neuen oder ergänzten Vorschriften macht es mir unmöglich, Ihnen, Herr Bouffier, eine komplette Liste Ihrer freiheitsfeindlichen Untaten vorzuhalten. Ich muss mich also beschränken auf diejenigen Eingriffsermächtigungen, bei denen die Verstöße gegen rechtsstaatliche Maßstäbe besonders eklatant sind.

Werfen wir zunächst einen Blick auf die neue Regelung über die Telekommunikationsüberwachung, kurz TKÜ. In Hessen haben Sie jetzt das Abhören von Telefonen und den Einsatz von so genannten IMSI-Catchern erlaubt. IMSI-Catcher sind Geräte, mit denen der Standort von Menschen mit Handys auch, wenn sie nicht telefonieren, schnell festgestellt werden kann. Die präventive TKÜ und der Einsatz des IMSI-Catchers sind erlaubt zur Abwehr von gegenwärtigen Gefahren für Leib, Leben oder Freiheit einer Person. Unsere Kritik: Entgegen den ausdrücklichen Vorgaben des Bundesverfassungsgerichts sieht Ihr Gesetz dabei keine Regelungen vor, die den absoluten Kernbereich privater Lebensgestaltung schützen. Zu diesem Kernbereich gehören zum Beispiel Gespräche zwischen Ehepartnern, nahen Angehörigen und sonstigen Personen des höchstpersönlichen Vertrauens.

Jetzt werden Sie, Herr Bouffier, einwenden, dass etwa ein Geiselnehmer kaum während eines Banküberfalls am Telefon mit seiner Frau über Details des Ehelebens plaudert. Dabei übersehen Sie allerdings, dass der Begriff der gegenwärtigen Gefahr für Leib und Leben nach dem 11. September 2001 schweren Schaden erlitten hat. Viele Gerichte meinten, dass schon die abstrakte Möglichkeit, dass irgendwann einmal irgendjemand irgendeinen Anschlag verüben könnte, ausreicht, um eine gegenwärtige Gefahr annehmen zu können. »Gegenwärtige Gefahren für Leib und Leben« scheinen in Zeiten des globalen Terrors überall und jederzeit zu lauern. Wer aber will im permanenten Ausnahmezustand noch ausschließen, dass durch Ihre neue Befugnis eben auch solche Telefonate mitgehört werden, die dem unantastbaren Kernbereich des TK-Geheimnisses zuzurechnen sind? Erst vor wenigen Monaten musste das Bundesverfassungsgericht dem niedersächsischen Gesetzgeber erklären, dass auch im Bereich der TKÜ der Kernbereich privater Lebensgestaltung unantastbar ist. Diese Vorgabe missachtet Ihre Regelung.

Auch sind Sie für eine Regelung verantwortlich, nach der auch bei Personen unter 14 Jahren, also Kindern, eine DNA-Analyse durchgeführt werden darf. Voraussetzung ist, dass die Kinder eine Straftat von erheblicher Bedeutung begangen haben und das auch in Zukunft von ihnen zu erwarten ist. Dem Nachwuchs können zu diesem Zweck Körperzellen entnommen werden; das auf diese Weise erlangte Material darf untersucht und das so gewonnene DNA-Muster gespeichert werden. Dabei übersehen Sie, Herr Bouffier, dass die Verfehlungen von Kindern das Gefühl der Rechtssicherheit der Bevölkerung in aller Regel nur wenig – wenn überhaupt – beeinträchtigen. Eine erhebliche Beeinträchtigung dieses Sicherheitsgefühls gehört aber nach verfassungsgerichtlichen Maßstäben zu einer erheblichen Straftat. Es stellt sich also grundsätzlich die Frage, ob die Kleinsten der Gesellschaft überhaupt »erhebliche Straftaten« im Sinne des Gesetzes begehen können. Über diese Zweifel hinaus missachten Sie das Prinzip, wonach frühzeitige Stigmatisierungen von jungen Menschen – etwa durch ihre Speicherung in einer »Verbrecher-Datei« – vermieden werden sollen. Und schließlich hätten Sie sich mit dem Einwand, dass Sie für DNA-Analysen zur Vorsorge für zukünftige Strafverfolgungen überhaupt keine Gesetzgebungskompetenz besitzen, etwas näher befassen sollen. Das wurde Ihnen bei der Sachverständigenanhörung im Hessischen Landtag auch ausdrücklich nahe gelegt. Genützt hat dieser Rat offenkundig wenig, denn das Gesetz wurde dennoch unverändert zur Abstimmung gebracht. Und deshalb werden Ihnen in naher Zukunft wohl die Gerichte die Kompetenzverteilung zwischen Bund und Ländern eingehender erläutern müssen.

Kommen wir zum öffentlichen Verkehrsraum, den Sie, Herr Bouffier, offenkundig in erster Linie als Überwachungsraum missverstehen. Als eines der ersten Bundesländer hat Hessen für eine Befugnis zum so genannten Kennzeichen-Scannen gesorgt. Mittels Ihrer Befugnis wird die Polizei ermächtigt, im Straßenverkehr einen Abgleich von Kfz-Kennzeichen mit Fahndungsdateien der Polizei durchzuführen. Dabei wird immer dann ein Personenbezug

hergestellt, wenn das Fahrzeug von seinem Halter geführt wird: Die Polizei weiß dann also, wer sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort befunden hat. Darin unterscheidet sich die Maßnahme von der »einfachen« Videoüberwachung des öffentlichen Raums durch die Polizei, bei der diese ja in der Regel nicht weiß, wen sie mit ihren Kamera-Augen auf Schritt und Tritt observiert. Dieser Personenbezug des Kennzeichen-Scannens lässt die Fahndungsmaßnahme folglich als besonders eingriffsintensiv erscheinen.

Auch in Sachen Videoüberwachung meinen Sie, neue Maßstäbe setzen zu müssen. Im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung steht inzwischen eine Ermächtigung, nach der die Polizei anlässlich von Personenkontrollen – etwa am Rande von Großveranstaltungen – Videoaufnahmen machen darf. Nicht nur, dass Sie damit einen weiteren Bereich des öffentlichen Lebens – wozu ja auch gelegentlich die Feststellung der Personalien von Personen gehört – einer Totalüberwachung unterwerfen. Nein, Sie differenzieren bei der Befugnis zur Speicherung der Videoaufnahmen auch noch zwischen den kontrollierten Personen und unvermeidbar betroffenen Dritten. Die Speicherung ist nur bei den Kontrollierten erlaubt, bei den übrigen Passanten aber nur die Datenerhebung, also die Vorstufe für eine Datenspeicherung. Wie aber, Herr Bouffier, wollen Sie eine Datenspeicherung der Passanten verhindern, wenn das Abbild der kontrollierten Personen gespeichert wird? Die Jury hält das, was nun im Gesetz steht, wirklich für legislativen Unfug, auf den Sie per Rechtsgutachten ebenfalls im Vorfeld der Verabschiedung des Gesetzes bereits hingewiesen worden waren.

Sie, Herr Bouffier, sind Wiederholungstäter im Sinne der BigBrotherAwards. Bereits im Jahr 2002 wurden Sie geehrt für eine Polizeirechtsnovelle, mit der die Voraussetzungen für die Rasterfahndung erheblich herabgesetzt wurden und damit gleichzeitig eine sehr sorgfältig begründete Entscheidung des Oberlandesgerichts Frankfurt konterkariert wurde. Wir haben das als Ihre erste, erhebliche Verletzung bürgerlicher Freiheit verstanden, durch die das sichere Gefühl, in einem freien Land zu leben, erheblich beeinträchtigt wurde. Das neue Hessische Polizeigesetz ist nun ein weiterer Beweis dafür, welch geringe Bedeutung Sie datenschutzrechtlichen Belangen zusprechen. Informationelle Selbstbestimmung, Herr Bouffier, ist ein Grundrecht. Irrtümlich gehen Sie offensichtlich immer noch davon aus, dass man Grundrechte fast beliebig einschränken kann, ohne irgendwann auch ihren Wesensgehalt anzutasten. Dieses abermalige Vergehen an einer freien Gesellschaft führt zu Ihrer unbefristeten Speicherung in der bei uns geführten Datei über Datenkraken.

Herzlichen Glückwunsch, Herr Bouffier.

Kategorie Technik
Diverse Kandidaten

Laudatorin: Karin Schuler, DVD

Der Big Brother Award 2005 in der Kategorie »Technik« geht stellvertretend an – tja, wen eigentlich? – für die schleichende Degradierung von Menschen zu überwachten Objekten Verharmlosung von Tendenzen zu flächendeckender Überwachung.

Popeln Sie manchmal in der Nase, wenn grad keiner guckt? Sitzen Sie bei langweiligen Vorträgen gerne schlafend in den hinteren Reihen? Überfallen Sie manchmal Tankstellen? »Wahrscheinlich guckt wieder kein Schwein!« – Dieser berühmte Seufzer von Friedrich K. Waechters Truthahn war schon im Cartoon unberechtigt (ein Schwein guckte und war begeistert). Und wir alle haben immer weniger Anlass zu dieser »Befürchtung«, denn alle möglichen Arten von »Schweinen« gucken uns in immer mehr Lebensbereichen zu – ohne dass wir sie sehen könnten. Allerdings verstecken sie sich heute hinter Bildschirmen, die von Videokameras gespeist werden – eine höchst einseitige Blickverbindung, bei der sie sich nicht als Betrachter offenbaren müssen. Dem Beobachteten ist der Blick auf den Beobachter verstellt: er mutiert zum bloßen Objekt der Betrachtung und weiß nicht, wer ihn wann, wie nah und zu welchem Zweck betrachtet, begafft, anstiert oder filmt.

Richter an deutschen Gerichten hingegen sprechen der anonymen Kamera als Vertreterin staatlicher Gewalt inzwischen quasi Persönlichkeitsrechte zu. Bereits im Jahr 2000 entschied das bayerische Oberlandesgericht, dass ein vor laufender Kamera gezeigter Stinkefinger als persönliche (!) Beleidigung der hinter dem Bildschirm spannenden Polizeibeamten anzusehen und ein Bußgeldverfahren berechtigt ist. Das Amtsgericht Stadtroda schrieb im Jahre 2004 einen fast gleich lautenden Fortsetzungsroman. Muss man demnächst befürchten, wegen Beleidigung des Finders verklagt zu werden, wenn man Urlaubsfotos von Menschen mit nackten Hintern auf der Straße verliert?

Da erscheint das folgende Szenario nur folgerichtig: Wenn Sie kurzsichtig sind, im U-Bahnhof Brandenburger Tor erst an Ihrer Freundin vorbeilaufen, mit der Sie verabredet sind, und wieder zurücklaufen, nachdem sie Ihnen nachruft – dann, ja dann sollten Sie sich schon mal auf einen kleinen Polizeiauflauf um sie herum einstellen – oder sich besser an einem anderen Ort verabreden. Denn genau dieses Verhalten (vorbeilaufen, anhalten, zurücklaufen und anschließend beieinander stehen) legen gemäß einer Analyse typischer Verhaltensmuster Drogendealer an den Tag – und werden damit in Zukunft sofort die Aufmerksamkeit der Mustererkennungssoftware erregen. Und wenn Sie Ihr Verhalten nicht ändern wollen – die Drogendealer werden es mit ziemlicher Sicherheit schnell schaffen. Weswegen man auf Dauer mit der Mustererkennung alleine nicht auskommt.

»Warum also nicht stets die neueste Technologie ausprobieren oder besser: ausprobieren lassen?«, dachte sich der Betriebsvorstand der Berliner Verkehrsbetriebe, Thomas Necker. Und deshalb hat er – vielleicht gab es ja auch ein paar zusätzliche Werbeeinnahmen dafür – gleich den ganzen U-Bahnhof Brandenburger Tor als Spielwiese für die Hersteller von Überwachungstechnologie frei gegeben. Die Spielgeräte werden von dankbaren Unternehmen gestellt, die notwendigen Utensilien, nämlich uns, gibt es gratis dazu.

Auch die Deutsche Bahn setzt seit langem, wie ja auch die Berliner Verkehrsbetriebe und mit ihr viele andere städtische Verkehrsbetriebe, auf die flächendeckende Videoüberwachung ihrer Bahnhöfe und Bahnsteige. Da muss man fast dankbar sein, dass man im ICE noch nicht unter Dauerbeobachtung durch ein Videoauge steht – wie

dies in vielen Bussen und Bahnen bereits fragwürdige Normalität ist. Aber: bis man in den ICE entkommt, steht man dafür unter besonders gründlicher Beobachtung. Da aber nichts so gut ist, dass man es nicht noch verbessern könnte, plant die Bahn jetzt eine zentrale Überwachungszentrale in Berlin. Hier sollen sowohl der bahneigene Sicherheitsdienst wie auch der Bundesgrenzschutz (der jetzt Bundespolizei heißt) Zugriff auf sämtliche Videokameras auf deutschen Bahnhöfen erhalten. Das angekündigte Ziel besteht in der Ausstattung jedes einzelnen Bahnhofs mit einer an die Berliner Zentrale angeschlossenen Kamera. Abgesehen von der fehlenden rechtlichen Grundlage für die Konstruktion (es gibt z.B. noch keinen Datenschutzvertrag zwischen Bahn und Bundespolizei, wie auch der Berliner Datenschutzbeauftragte säuerlich vermerkte), fragt man sich, wie sinnvoll es ist, wenn man in Berlin sieht, dass in München-Ost gerade jemand überfallen wird. Jedoch geht es vermutlich nicht um so unwichtige Dinge wie Pöbeleien, Vergewaltigungen oder Handtaschenraub, sondern um die ganz großen Gefahren: Terror, bestenfalls noch Raub und Mord, die man nun von Berlin aus zentral im Blick behalten will, wenn man sie schon nicht verhindern kann.

Perfekt ist an dieser Überwachung vor allem eines: Die weitgehende Erfassung großer Lebensbereiche vieler Menschen, die auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind, wie zum Beispiel Pendler oder Schülerinnen und Schüler.

Da könnten einem die Polizeibehörden diverser Kommunen ja fast schon Leid tun, die nicht durch ein Softwareprogramm in Echtzeit potenzielle Verfehlungen der Beobachteten »berechnen« können, sondern das Bildmaterial der zunehmenden Anzahl mobiler Überwachungskameras noch selbst auswerten müssen. Durch die einfache Platzierung dieser mobilen Anlagen bleibt nur allzu oft die ernsthafte Abwägung zwischen Nutzen und Grundrechtseingriff auf der Strecke, wie z. B. in Leipzig, wo trotz offensichtlicher Nutzlosigkeit der Videoüberwachung eines krawallgefährdeten Platzes dessen weitere Überwachung sogar durch öffentlich vorgetragene Lügen durchgeboxt wurde. Auch in Bielefeld wurde es bei der Rechtfertigung der Videoüberwachung im Ravensberger Park mit der Wahrheit nicht so genau genommen. Von großem Erfolg und sinkender Kriminalität berichtete das Ministerium. Das Gegenteil war jedoch der Fall, wie der FoeBuD e.V. für die Jahre 2000 und 2001 errechnete. Die Straftaten im Park sind nach Installation der Kameras 2000 sogar von 6 auf 9 gestiegen. Was nicht ins Bild passte, sollte offenbar passend gemacht werden. Bei derartiger öffentlicher Überwachungswut wundert es fast schon nicht mehr, wenn Private für sich in Anspruch nehmen, was öffentliche Stellen ihnen auf vielfältige Weise vormachen und vorbeten.

»Wozu gesetzliche Hinweisvorschriften beachten, wenn die staatlich organisierte Überwachung doch auch ohne Kenntnis der Überwachten zu-

nehmend im Geheimen arbeitet?« muss sich der Bahnhofsbuchhändler Stilke gedacht haben, als er heimlich Video-Spione in die Decke seiner Hamburger Bahnhofsfiliale einbaute, um die Belegschaft »im Blick zu haben« – ein eindeutig rechtswidriger Vorgang. Und da Angriff bekanntlich die beste Verteidigung ist, sollte der Kollege, der die Kamera zufällig entdeckt hatte, wegen Sachbeschädigung (der Kamera) fristlos entlassen werden.

Videoüberwachung gehört inzwischen so zu unserem Alltag, dass es keine moralischen Hemmschwellen mehr zu geben scheint. Den meisten »Videoten« fällt kaum noch ein, dass es juristische Grenzen geben könnte, die man nicht überschreiten darf.

Wem Unrecht widerfährt oder wer das auch nur befürchtet, ist anscheinend häufig bereit, das Recht in die eigene Hand zu nehmen und Selbstjustiz zu üben. Nicht selten schießen die Protagonisten dabei weit übers Ziel hinaus und verlieren jedes Maß – insbesondere das Persönlichkeitsrecht vieler Betroffener – aus den Augen.

In diese Kategorie fällt auch die heimliche Videoüberwachung und anschließende Internet-Veröffentlichung von Kundenfotos aus Läden des Macintosh-Großhändlers GRAVIS. Der hatte anscheinend Polizei und Staatsanwaltschaft gar nicht erst mit Arbeit behelligen wollen und heimlich aufgenommene Videoaufnahmen von Kunden im Internet veröffentlicht – mit der Bitte um Mithilfe bei der Identifizierung. Angeblich handelte es sich um Mitglieder einer Hehlerbande, die systematisch Einbrüche in GRAVIS-Geschäfte verübte. Als Preis bei diesem »Pranger-Spiel« winkte ein iPod...

Seit einigen Jahren kursieren FoeBuD-Aufkleber »Diese Toilette wird aus hygienischen Gründen videoüberwacht«. Nicht wenige haben daraufhin beim Besuch des Stillen Örtchens verschreckt die Zimmerdecke abgesucht. Aber keine Idee ist so absurd, als dass sie nicht noch von der Realität übertroffen werden könnte: In der »Wellness-Oase Mediterana« in Bergisch Gladbach wird diese Schwelle deutlich überschritten.

Nachdem man den nicht geringen Eintritt bezahlt hat, empfangen einen außer orientalischen Formen, luxuriösen Saunen und angenehmer Musik auch Videokameras an den Decken der Sammelumkleiden. Weder findet sich jedoch die gesetzlich vorgeschriebene Kennzeichnung der Überwachung, noch lässt sich in Erfahrung bringen, wer diese Aufnahmen nackter Leute betrachtet, aufzeichnet oder vielleicht auch mal wieder löscht. Ob es einen Datenschutzbeauftragten gibt, bleibt ebenfalls das Geheimnis des Betreibers.

Obwohl schon diese ernüchternde Sammlung erschreckender Beispiele zeigt, dass wir auf dem besten Wege zu flächendeckender Videoüberwachung sind, könnte man die Aufzählung noch stundenlang fortsetzen. Wir haben deshalb entschieden, in diesem Jahr im Bereich Technik keinen einzelnen Preisträger zu küren. Denn das würde die jeweils anderen Video-Überwacher im Glauben wiegen, sie seien noch mal davon gekommen.

Nein, wir sagen: Herzlichen Glückwunsch euch allen, Ihr befindet euch in schlechter Gesellschaft.

Die Gewinner der Fußballweltmeisterschaft stehen bereits fest: RFID-Chips

Kategorie Verbraucherschutz

Franz Beckenbauer, WM-Organisationskomitee

Laudatorin: Rena Tangens, FoeBuD

Der Big Brother Award 2005 in der Kategorie »Verbraucherschutz« geht an das FIFA Fußball-Weltmeisterschaft 2006 Organisationskomitee Deutschland im DFB, vertreten durch Franz Beckenbauer für die inquisitorischen Fragebögen zur Bestellung von WM-Tickets, für die geplante Weitergabe der Adressen an die FIFA und deren Sponsoren und für die Nutzung von RFID-Schnüffelchips in den WM-Eintrittskarten und damit den Versuch, eine Kontroll- und Überwachungstechnik salonfähig zu machen zum Nutzen des WM-Sponsors und RFID-Herstellers Philips.

Eigentlich war es recht vorhersehbar, dass das WM-Komitee einen BigBrotherAward bekommt. Schon 2003 stand die mit einem Schnüffelchip verwanzte Eintrittskarte der Fußballweltmeisterschaft 2006 auf der Kandidatenliste. Die BigBrotherAwards-Jury hat sich dann aber damals doch für Metros Testsupermarkt »Future Store« entschieden, wo die Funkchips schon im Kundenbereich zum Einsatz kamen. Dieser BigBrotherAward für Metro hatte weltweite Wirkungen: Die RFID-Industrie steht seitdem in der Kritik.

Im Jahr 2004 stand das WM-Komitee wieder auf der BBA-Kandidatenliste – mittlerweile waren der Jury auch weitere Details bekannt – aber wir wollten nicht langweilen und schon wieder ein RFID-Thema in den Mittelpunkt stellen. »2006 ist ja noch weit weg«, dachten wir, »da können wir ja noch ein Jahr später was tun«.

Nach der Preisverleihung vor einem Jahr stellten wir plötzlich fest, dass das WM-Überwachungsszenario viel näher war, als wir glaubten. Das Bündnis Aktiver Fußballfans, kurz »BAFF« (das sind die, die den schönen Satz »Sitzen ist für den Arsch« geprägt haben), machte uns darauf aufmerksam, dass der Eintrittskartenverkauf in bald drei Monaten – also im Februar 2005 – beginnen würde. Aus mangelnder Fußballbegeisterung hätten wir den sich anbahnenden Datenschutzgau fast verpasst ...

Zu den Fakten: Jede und jeder, die oder der ein »Ticket« haben wollte, muss dies beantragen. Und zum Antrag gehören Daten. Name. Adresse. Kinderkrankheiten... Nein, Kinderkrankheiten nicht. Aber: Geburtsdatum, Telefon, Nationalität und wessen Fan ich bin. Bitte? In Deutschland? 60 Jahre nach Kriegsende, 60 Jahre nachdem ganze Völkergruppen aus deutschen KZs ermordet worden sind, fragt ein deutsches Unternehmen auf einem Fragebogen nach Nationalität und für welche Nationalität mein Herz schlägt? Ich bin Grieche und finde die Türken toll? Ich habe einen amerikanischen Pass und mein Herz schlägt für die saudiarabische Nationalmannschaft?

Und wozu wird beispielsweise das Geburtsdatum abgefragt? Für die Kartenbestellung ist es überflüssig – für die Werbebranche dagegen von großem Wert.

Wer braucht diese Daten – wer bekommt sie und was passiert damit? Nun, sie gehen auf jeden Fall an die FIFA, den Weltfußballverband, und von dort an deren Sponsoren, als da wären Coca Cola, MasterCard, Gillette, Philips, die Airline der Vereinigten Arabischen Emirate, die Telekom, McDonalds und und und.

Der Soziologe Richard Sennett sagt sinngemäß: »Der moderne Kapitalismus ist in seiner Grundtendenz antidemokratisch. Er begünstigt das, was ich »eine weiche Spielart des Faschismus« genannt habe. In der neuen Politik ist das Diktat auf dem Vormarsch – sie führt zu willkürlichen und autoritären Entscheidungen und ihr ist es völlig gleichgültig, was die Mehrheit der Menschen denkt.«

Aber es geht ja auch gar nicht um Menschen. »Es geht um Sicherheit«, sagt das WM-Organisationskomitee. Und deshalb sollen alle Karteninteressenten auch noch die Personalausweis- oder Reisepassnummer angeben. Aber: Die Erhebung und Verarbeitung dieser Nummer ist nach dem Personalausweisgesetz gar nicht statthaft, denn die Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer hat der Gesetzgeber verboten. Doch das störte das WM-OK des DFB wenig.

Und das WM-OK fühlt sich beim Datenmissbrauch offensichtlich sicher. Denn Innenminister Otto Schily höchstpersönlich sitzt mit im Organisationskomitee der Fußball-WM und deckte die Abgabe der Ausweisnummer, ja vermutlich forderte er sie sogar. Die Personalausweis-Nummer wird gespeichert und kann in einer Datenbank mit der Nummer auf dem RFID-Chip verknüpft werden, der in die Eintrittskarten integriert ist.

Sowohl Otto Schily als auch der DFB haben bereits von der Journalistenvereinigung »Netzwerk Recherche« den Negativpreis »Die verschlossene Auster« dafür erhalten, dass sie bei kritischen Fragen Journalisten keine Auskünfte geben. Auch als der FoeBuD gerade noch rechtzeitig vor der Ticketvergabe die Öffentlichkeit aufrüttelte, und auch viele Journalisten deswegen anfragten, herrschte – wie auch schon im Vorfeld – seitens des OK und des Innenministeriums tiefes Schweigen. Keine Interviews. Kein Kommentar.

Auch auf eine Abmahnung des Verbraucherschutzverbandes vzbv wegen schwerwiegender Mängel in den Fragebögen reagierte der DFB erst, als die Verbraucherschützer mit einer einstweiligen Verfügung drohten, nach der der Ticketverkauf hätte eingestellt werden müssen.

Inzwischen hat der DFB einem lauen Kompromiss zugestimmt. Zwar muss auf den Formularen nun eindeutig der werblichen Nutzung der abgegebenen Daten zugestimmt werden, aber die illegale Eingabe der Personalausweisnummer wird nach wie vor verlangt. Die illegale Abfrage unnötiger Daten ist ebenfalls nicht vom Tisch, oder dass Karteninteressenten die Ausweis-Num-

mern von Freunden oder Familienmitgliedern eintragen müssen, wenn sie mehrere Karten bestellen.

Deutliche Kritik gab es auch von den Datenschützern vom Unabhängigen Landesdatenschutzzentrum Schleswig-Holstein. Sie griffen die Kritik des FoeBuD auf und veröffentlichten eine kritische rechtliche Bewertung. Dr. Thilo Weichert fasst zusammen:

»Die Fußball-Weltmeisterschaft wird zu einem Überwachungsgroßprojekt missbraucht, mit dem Fußball-Fans vollständig kontrollierbar gemacht werden sollen. Mit diesem Mehr an Überwachung wird aber kaum mehr Sicherheit erreicht. (...) Zugleich wird mit dem Ticket-Verfahren die RFID-Technik, der Einsatz von kleinen Funkchips, in der Gesellschaft hoffähig gemacht. RFID sind in der Logistik sinnvoll, dieser Einsatz am Menschen ist aber alles andere als datenschutzfreundlich. Auf dem Bestellformular werden zudem mehr Daten als notwendig abgefordert. (...) Da keine Alternative angeboten wird, stehen die Fußball-Fans vor der Alternative, entweder ihre Daten preiszugeben, oder auf die Teilnahme an WM-Spielen zu verzichten. Für den DFB steht offensichtlich nicht der Genuss am Fußball im Vordergrund, sondern die Vermarktung der Fans als Ware.«

Es ist ein verhängnisvoller Trend, dass zunehmend Leistungen davon abhängig gemacht werden, dass Bürger einem Unternehmen als gläserner Kunde gegenübertreten müssen. Dass Eintrittskarten verpflichtend personalisiert werden, ist eine Anmaßung eines immer autoritärer werdenden Systems.

Die gebetsmühlenartig vorgetragenen »Sicherheitsaspekte«, die wir uns immer wieder als Vorwand für dieses Gesetz und jene Maßnahme anhören müssen, sind eine Farce. Wenn Fußballspiele tatsächlich so ein Sicherheitsrisiko sein sollten, dass es nur noch möglich ist, sie in totalitären Staaten abzuhalten, dann müssen Fußballbegeisterte eben in totalitäre Staaten ausweichen. Wir wollen keinen Staat, in dem über die ständige Drohung mit einer diffusen Terrorismusgefahr die Preisgabe von Bürgerrechten und angepasstes Wohlverhalten der Bürgerinnen und Bürger erzwungen wird.

Das Erfassen der Daten im Bestellformular bringt keine Sicherheit. Der RFID-Chip, im WM-Ticket, der per Funk ausgelesen werden kann, ermöglicht das Tracking von Fußballfans, also das Verfolgen und Erstellen von Bewegungsprofilen – aber er bringt keine Sicherheit (er erhöht vermutlich nur den Schwarzmarktpreis). Das wissen die Drahtzieher im WM OK offensichtlich auch.

Originalton aus dem Interview eines Journalisten mit einem der ranghöchsten FIFA-IT-Spezialisten: »Why do you need RFID?« – »Because Philips is our sponsor.« – »Are there any technical advantages with these chips?« – »Philips is our sponsor. Please ask their representive.«

Bei der Fußball-WM wird versucht, über die WM-Tickets, die jeder Fan haben will, RFID-Technologie in Deutschland zu etablieren – denn die RFID-Lesegeräte in den Stadien werden wohl kaum zum Ende der WM wieder abgebaut. So wird – mit Millionen von Fußballfans als Testobjekten – eine potentielle Überwachungs- und Kontrollstruktur salonfähig gemacht.

Und Sie, Herr Beckenbauer, halten auch dafür Ihr Gesicht in jede Kamera.

Übrigens, die Quote stimmt auch bei uns. Rein zahlenmäßig kamen Sie bei den Vorschlägen, wer einen BigBrotherAward bekommen soll, auf den zweiten Platz. Doch das ist kein Grund zur Freude, denn jede Nominierung ist eine Rote Karte – Ihnen zugedacht von den deutschen Fußballfans.

Herzlichen Glückwunsch zum BigBrotherAward, lieber DFB, liebes WM-Organisationskomitee, lieber Franz Beckenbauer.

Kategorie Kommunikation
Erhard Rex, Generalstaatsanwaltschaft Schleswig-Holstein

Laudator: Alvar C.H. Freude, Fitug

Der BigBrotherAward 2005 in der Kategorie »Kommunikation« geht an Erhard Rex, den Generalstaatsanwalt Schleswig-Holsteins, Leiter der Staatsanwaltschaften Kiel und Lübeck für die großflächige Suche nach Zeugen mittels Handy-Ortung ohne fundierte Begründung und für die Verweigerung, die dazugehörigen Unterlagen den Datenschützern des Landes Schleswig-Holstein zur Einsicht zur Verfügung zu stellen.

Als im Juni 2005 ein Restpostenmarkt in Bad Segeberg durch Brandstiftung in Flammen aufgeht, beantragt die Staatsanwaltschaft, dass die Polizei eine so genannte Funkzellenabfrage durchführen darf. Die Mobilfunkanbieter T-Mobile, Vodafone, E-Plus und O2 werden daher aufgefordert, jeden ihrer Kunden zu ermitteln, der in der Nacht der Brandstiftung zur Tatzeit in der Nähe des Tatortes telefoniert hat. 700 Handy-Besitzer werden daraufhin von der Polizei angeschrieben. Sie sollen in einem Fragebogen angeben, wo sie in der fraglichen Nacht waren, wer bei ihnen war und ob ihnen etwas aufgefallen sei. Gegenüber der Presse gibt die Polizei zu verstehen: Wer nicht antwortet, macht sich verdächtig.

Der Fragebogen ist umfangreich – wer beispielsweise in einem Fahrzeug saß, soll Kennzeichen, Marke, Typ und Farbe angeben. Seines eigenen Fahrzeuges – werden hier wirklich nur Zeugen gesucht? Unter den Adressaten dieses Fragebogens ist auch ein Journalist, der über das Feuer berichtet und am Tatort telefoniert hatte. Presseberichte lösen schließlich eine Behandlung des Themas im Innen- und Rechtsausschuss des schleswig-holsteinischen Landtags aus. Dabei stellt sich heraus, dass diese Funkzellenabfrage eine ganz besondere Premiere darstellt: zum ersten Mal sollen keine Verdächtigen oder gar Täter ermittelt werden, sondern Zeugen. Die jedoch werden gleich als mögliche Verdächtige behandelt.

Ein Mord in Oedendorf, südöstlich von Hamburg, im Juli 2005, führt ebenfalls zu einer Handyortung. Rund 3000 Personen werden auf Anordnung der Staatsanwaltschaft ermittelt, aber der öffentliche Druck ist groß, und die Aktion muss gestoppt werden. Bis dahin wurden jedoch bereits 150 Personen telefonisch befragt. Wie viele von ihnen werden sich – durch unbedachte Äußerungen oder Missverständnisse – verdächtig gemacht haben? Schließlich liegt der Tatort in der Nähe einer Landstraße und einer Autobahn. Viele Handybenutzer, die hier unterwegs waren, geraten ins Visier der Ermittler.

Was mit den ermittelten Daten und den Gesprächsprotokollen geschehen ist, ist unbekannt. Denn als im September Mitarbeiter des Unabhängigen

Landeszentrums für Datenschutz die Datenverarbeitung überprüfen wollen, verbietet die Staatsanwaltschaft der Polizei die Herausgabe der Akten.

Die Jury des BigBrotherAward ist der Ansicht, dass in beiden Fällen das berechtigte Interesse des Staates zur Strafverfolgung in nicht hinnehmbarer Weise die Grundrechte der Betroffenen verletzt hat. Mobilfunk-Unternehmen wurden ohne konkreten Tatverdacht gezwungen, die Datenschutzvereinbarungen mit ihren Kunden zu brechen. Unzählige Unschuldige wurden zu Verdächtigen. Die Beweislast wurde umgekehrt – potenzielle Zeugen mussten beweisen, dass sie keine Täter sind.

Herzlichen Glückwunsch, Erhard Rex, Generalstaatsanwalt in Schleswig-Holstein.

Kategorie Regional
Grundschule Ennigloh, Volksbank Oeynhausen Herford, Sparkasse Herford

Laudator: padeluun, FoeBuD

Den Regionalpreis der BigBrotherAwards 2005 teilen sich die Grundschule Ennigloh, die Volksbank Herford und die Sparkasse Herford für die Weitergabe und Nutzung von Adressdaten von Schulanfängern.

»Was Hänschen nicht lernt, lernt Hans nimmermehr« – nach diesem Motto versuchen insbesondere Banken schon seit Jahren mit Schülerkonten und Konfirmationsgeschenken, Kinder so früh wie möglich an sich zu binden. Inzwischen sind schon die Schulanfänger im Visier der Banken: Zum Schulbeginn wird den Kindern ein Startkonto angeboten. Damit die Kinder rechtzeitig zur Einschulung von diesem Angebot auch erfahren, schreiben die beiden konkurrierenden Unternehmen Volksbank und Sparkasse, beide in Herford ansässig, die Kinder an und schicken Werbung fürs Startkonto ins Haus.

Da fragt sich die geneigte Zuhörer- oder Leserschaft doch gleich: »Moment mal, woher wissen die denn, wer eingeschult wird?«

Wir haben die Banken angerufen. Die Volksbank weiß natürlich, so sagt sie selbst, dass sie alles richtig gemacht haben. Auf dem Infoabend für die Eltern, so erklärt uns der nicht allzu freundliche Herr am Telefon der Volksbank, ist eine Liste herumgegangen, auf der die Eltern bekundet haben, dass sie solcherlei Werbung für ihre Kinder ausdrücklich begrüßen. Nun, die Eltern, die uns diesen Vorfall gemeldet haben, wissen nichts von einer Liste oder gar einer Einwilligung. Ob man uns diese Liste mal zufaxen könne? Aber nein, auf gar keinen Fall dröhnt es am Telefon, es sei ja schließlich nicht auszuschließen, dass die BigBrotherAwards solche Unterlagen dann an die Konkurrenz weiter geben würden. Aha.

Außerdem: so etwas hat die Konkurrenz überhaupt nicht nötig. Denn auch die weiß sich die Namen und Adressen der Kinder zu beschaffen. Und immerhin: Anders als bei der Volksbank werden wir am Telefon nicht angelogen. »Die jahrelangen guten Beziehungen zu den Schulen führen dazu, dass die Sparkasse die Namen der Kinder von den Schulen bekommt«, sagt uns eine freundliche junge Frau am Telefon. Dann guckt die Bank nach, ob man die Adressen der Eltern dazu habe, und schon ist die Datei mit der Werbeaussendung fertig.

Die meisten Schulen denken nicht daran, dass die Daten der ihnen anvertrauten Schülerinnen und Schüler Begehrlichkeiten bei allerlei – ich sag jetzt mal – Gesindel weckt. Deswegen haben wir uns entschieden (sozusagen aus pädagogischen Gründen), den Preis an erster Stelle nicht den Banken, sondern der Grundschule in Bünde zuzuerkennen. Es soll eine Mahnung für alle Schulen bundesweit sein, dass aus den Rektoraten, Sekretariaten und seitens der Kollegien keine Daten an die Adressverwerter herausgehen. Einer Instrumentalisierung der Schulen durch Wirtschaftsunternehmen sollten wir nach wie vor gemeinsam entgegenwirken.

Und so was passiert auch nicht nur an Grundschulen und bei den ABC-Schützen. An mehreren Gymnasien – wurde uns berichtet – wurden und werden Schülerinnen und Schülern Bücher aus der Duden-Reihe versprochen. Duden, Meyer, Brockhaus – ach, das scheinen renommierte Namen zu sein. Da denkt niemand etwas Böses. Wer ist wohl seriöser als der Dudenverlag?

Diese Buchgeschenke, dünne Bändchen namens »Schülerhilfe«, werden aber an eine Bedingung geknüpft: Die Schülerinnen und Schüler müssen Ihre Anschrift angeben und diese Liste muss dem »selbstlosen Geschenkemacher« von der Schule zugeschickt werden.

Und dann haben wir mal nachrecherchiert: Die Firma, über die diese Schweinerei läuft, heißt inmediaONE GmbH. Sie sitzt in Gütersloh und gehört natürlich zum Bertelsmann-Konzern. Der wiederum ist einer der ganz großen Player des Adresshandels. inmediaONE beauftragt die Firma WKV GmbH bei Trier mit der Komplettabwicklung. Die Selbstbeschreibung der Firma WKV liest sich so:

»Wir betreiben aktive Neukundenakquise und erweitern damit Ihre Kundenbasis. Wir generieren [...] qualifizierte Adressen für große Unternehmen im deutschsprachigen Raum. Unsere jährliche Kapazität liegt bei einer Summe von ca. 1 Million Netto-Interessentenadressen. [...] Dies gelingt uns beispielsweise durch die Datenerfassung bei Gewinnspielen, Preisrätseln und« – hört, hört – »Gratisaktionen«.

Eine Lehrerin, die ihre Vertrauensstellung nicht als Erfüllungsgehilfin zur Akquise von Neukunden missbrauchen lassen wollte, hat es ausprobiert: Sie hat die Anschriften Ihrer Schülerinnen und Schüler nicht angegeben, sondern einen Klassensatz angefordert – und dann gab's eben auch keine Bücher. Das macht klar: Es handelt sich nicht um »Geschenke«.

Hier erwarte ich auch von der Schulaufsicht, die noch vor kurzem – im Widerspruch zur Datenschutzbeauftragten des Landes NRW – »keinen Verstoß gegen das Datenschutzgesetz« sah, dass sie alle Schulen informiert und diesem Treiben Einhalt gebietet.

In den vergangenen Jahren haben wir immer wieder den Datenhandel in seinen verschiedensten Facetten mit einem BigBrotherAward versehen. Meist hat es die Nutznießer und Firmen getroffen. In diesem Jahr sitzt aus pädagogischen Gründen die Grundschule Ennigloh bei Bünde wegen ihrer Gedanken- oder Skrupellosigkeit in der ersten Reihe. Mit zur Nachschulung müssen in der zweiten Reihe die Volksbank und die Sparkasse Herford. In der dritten Reihe bekommt die Schulaufsicht hiermit einen blauen Brief.

Herzlichen Glückwunsch, Euch allen.

Big Brother Awards in Österreich

Am Vorabend des Nationalfeiertags, drei Tage früher als in Deutschland, wurden im Wiener Rabenhof Theater von den Vereinen Quintessenz und VIBE!AT die österreichischen Big Brother Awards verliehen. Die Nominierungsliste mit 27 Institutionen und Personen war bereits am 17. Oktober der Öffentlichkeit bekannt gegeben worden.

Business und Finanzen

In der Kategorie Business und Finanzen wurde die Gebäudereinigungsfirma Assa ausgezeichnet. Auf ihrer Webseite verkündet die Assa: »Das Reinigungspersonal, das nahezu ausschließlich aus den östlichen Nachbarräumen stammt und tendenziell zu den potentiell zu überwachenden Religions- und Glaubensgruppen zählt, wird von Assa einem besonders strengen und selektiven Auswahlverfahren unterzogen«. Dazu habe die Assa den ehemaligen Chef der österreichischen Antiterroreinheit Cobra engagiert. Die Mitarbeiter müssen sich bei Arbeitsbeginn und -ende mit einem Fingerscan legitimieren, in Zukunft sollen auch DNA-Proben von ihnen genommen werden.

Politik

Gesundheitsministerin Maria Rauch-Kallat wurde für die Schaffung des gläsernen Patienten samt Alkoholikerdatenbank ein Big Brother Award verliehen. Mit dem »Gesundheitstelematikgesetz« wolle sie die Grundlage für einen umfassenden Datenaustausch sensibler Patientendaten schaffen, die zentral gespeichert werden sollen. Ärzten, Krankenhäusern, Privatversicherungen und auch Amts- und Betriebsärzten solle ein unkontrollierter Zugriff auf sämtliche Gesundheitsdaten ermöglicht werden. Diese umfassen auch Lebensgewohnheiten, Hobbys, Sexualpraktiken, psychiatrische Diagnosen, Ernährung und Diäten oder das Erbgut. Regelungen über die Rechte der Patienten oder welche Stellen unter welchen Voraussetzungen berechtigt sind, Daten abzufragen, gibt es im Gesetz nicht.

Mit der geplanten »Vorsorgeuntersuchung Neu« werden die Meldepflichten an die Sozialversicherungen erweitert. Ärzte müssen Details über die Untersuchung personenbezogen und computerverwertbar an die Versicherungen weiterleiten. Wer bei der Vorsorgeuntersuchung nicht angibt, keinen oder nur selten Alkohol zu trinken, soll einen umfangreichen Fragebogen zu seinen Trinkgewohnheiten ausfüllen. Dessen Auswertung ergibt eine »Alkoholikerkennziffer«, die zu übermitteln ist.

Behörden und Verwaltung

Die Zahl der abgehörten Telefone stieg in Österreich in den letzten zwei Jahren um 68 %, bei der »Rufdatenerfassung« gab es einen Zuwachs um 438 %. Verantwortlich dafür seien die österreichischen Richter, die Überwachungsanträge der Polizei ohne Prüfung unterschrieben. Das Vertrauen in unabhängige und unparteiische Richter und Richterinnen als Garanten für die Rechte der Bevölkerung und als Instanz, welche die Rechte der Sicherheitsbehörden und der Bevölkerung sorgsam gegeneinander abwägt, werde nun massiv erschüttert, und dem Grundrecht auf Privatsphäre immer weniger Beachtung geschenkt. Dafür verdienten die Richter den Big Brother Award.

Kommunikation

Wer am Online-Strategie-Spiel World of Warcraft der Blizzard Entertainment teilnehmen will, muss der Installation von Spyware zustimmen. Am Ende der Nutzungsbestimmungen ist festgelegt, dass der Spieler erdulden muss, dass das Programm die auf dem Rechner laufenden Programme analysiert, »bestimmte« Informationen vom Rechner an den Hersteller überträgt, ausdrücklich eingeschlossen Identifikationsnummern von Festplatten und CPU, IP-Adressen und Betriebssysteme. »Warden liest alle Überschriften der momentan offenen Fenster aus, registriert jedes Programm im Hintergrund. Ganz offensichtlich öffnet Warden jedes beim Scan vorgefundene Programm. Der bekannte Technik-Autor Greg Hoglund schrieb dazu: ›I watched warden open my email program, and even my PGP key manager. Again, I feel this is a fairly severe violation of privacy, but what can you do?‹«

Lebenslanges Ärgernis

Für die lebenslängliche Begleitung aller Staatsbürger wurde dem österreichischen Melderegister der Big Brother Award in der Kategorie »Lebenslanges Ärgernis« verliehen. Der Staat verdient Millionen an Online-Abfragen, die zu einem großen Teil ohne ausreichende Begründung erfolgen.

Volkswahl

In der Kategorie Volkswahl siegten die Wiener Linien für die Videoaufzeichnung in Stationen, U-Bahnzügen und Straßenbahnen. Die Fahrer können die Bilder nicht sehen, diese werden 48 Stunden gespeichert und dann gelöscht. Bei Vandalismusakten oder Gewalthandlungen sollen die Aufnahmen ausgewertet werden. Der Diebstahl einer Geldbörse rechtfertige aber noch nicht den Aufwand einer Auswertung, verlauteten die Wiener Linien.

Defensor Libertatis

Zum zweiten Mal wurde auch ein Positiv-Preis, der Defensor Libertatis vergeben. Ausgezeichnet wurde das Europäische Parlament für sein Engagement und den Mut der Parlamentarier, in wichtigen Fragen auch den Konflikt mit dem Ministerrat und der Kommission zu riskieren. Hervorzuheben sei der Widerstand gegen den Entwurf zur Patentierbarkeit von Software und die Richtlinie zur Weitergabe von Flugdaten an die USA.

Big Brother Awards in der Schweiz

Am Samstag, den 29. Oktober wurden im Zürcher Kulturzentrum Rote Fabrik die Gewinner der Schweizer Big Brother Awards bekannt gegeben. Die Organisatoren, das Archiv Schnüffelstaat Schweiz (ASS), die Swiss Internet User Group (SIUG) sowie das Kulturzentrum Rote Fabrik vergaben die Betonpokale in vier Kategorien. Außerdem war der Winkelried-Award an eine Person oder Institution zu vergeben, die sich in lobenswerter Weise gegen zunehmende Überwachung und Kontrolle zur Wehr setzte.

Staats-Award

Die Gemeinde Emmen stellte zum 1. Februar 2005 den 31-jährigen ehemaligen Polizeibeamten Christoph Odermatt als «Sozialinspektor» ein, um ihre 1100 Sozialhilfeempfänger zu überwachen. In den ersten fünf Monaten wurden mittels Nachforschungen, »Umfeldabklärungen» und Hausbesuchen 28 Verdachtsfälle untersucht. Dabei konnten sieben Missbrauchsfälle aufgedeckt werden. Die eingesparte Summe reichte allerdings nicht, die Kosten für seine Tätigkeit zu decken.

Business-Award

Ein Schweizer Bürger überwies online für eine Kuba-Reise von seinem Postscheckkonto bei der PostFinance in Zürich 1528 US-Dollar auf das Konto eines kubanischen Reisebüros bei der UBS in Zürich. Sein Konto wurde mit dem entsprechenden Betrag in Schweizer Franken belastet. Einen Monat später erfuhr er von der PostFinance, dass seine Überweisung wegen des bestehenden US-Embargos gegen Kuba in den USA blockiert worden und sein Geld sich nun auf einem amerikanischen Sperrkonto befinden würde. Er könne versuchen, beim U.S. Department of the Treasury eine Rückforderung geltend zu machen. Auf Nachfrage wurde er aufgeklärt, dass die PostFinance US-Dollar-Transaktionen immer über die Deutsche Bank Trust Company Americas mit Sitz in den USA abwickeln würde. Er gab sich damit nicht zufrieden und forderte von der PostFinance sein Geld zurück. Erst zwei Monate später, nachdem er auch den Eidgenössischen Datenschutzbeauftragten eingeschaltet hatte, wurde ihm der Betrag wieder gutgeschrieben.

Arbeitsplatz-Award

Bundesanwalt Valentin Roschacher lies kurz vor Büroschluss die Papierkörbe von 100 Angestellten der Bundesanwaltschaft in Bern durchsuchen. Es habe sich bloß um eine »Routinekontrolle« gehandelt: Man habe prüfen wollen, ob die Mitarbeitenden die »operationellen Papiere« vorschriftsgemäß vom gewöhnlichen Abfall getrennt hätten. Der Leiter des Rechtsdienstes der BA räumte dann in einer Mail an die Angestellten ein, dass es »für die Papierkorbaktion keine hinreichende Rechtsgrundlage« gebe.

Lebenswerk-Award

Jürg Scherrer, Polizeidirektor von Biel-Bienne und Präsident der Freiheitspartei FPS versuchte über mehrere Jahre, die Stadt Biel durch Videokameras sicherer zu machen. Allerdings waren seine Bemühungen vergebens, denn mangels rechtlicher Grundlage musste er immer wieder den Rückzug antreten. Der Gemeinderat versagte die Zustimmung zu einem Videoreglement. Daraufhin lancierte er eine Volksinitiative zur Schaffung einer gesetzlichen Grundlage. Ein Rechtsgutachten zeigte dann aber, dass nach bernischem Gemeindegesetz die Regelung von Videokameras im öffentlichen Raum gar nicht in der Kompetenz der Gemeinden liegt. Als Trostpreis erhält der 58jährige Jürg Scherrer nun den »Big Brother Award 2005« in der Kategorie »Lebenswerk«.

Winkelried-Award

Aufgrund einer vom schweizerischen Parlament beschlossenen Revision des Telefonüberwachungsgesetzes (BüPF) mussten sich bis zum 31. Oktober 2004 alle BesitzerInnen von Prepaid-Handys bei den Telefongesellschaften identifizieren und registrieren lassen. Dazu werden allerdings nicht alle ausländischen Ausweispapiere anerkannt. Zur Registrierung muss zwingend ein gültiger Pass oder ein gültiges Reisedokument vorgelegt werden, was die meisten der Asylsuchenden oder Kriegsflüchtlinge aber nicht besitzen. Gerade für diese Menschen ist aber der jederzeit mögliche Kontakt per Telefon enorm wichtig für Kontakte zu Familien, Freunden, AnwältInnen, vor allem aber, damit sie selbst erreichbar sind.

Ein »normales« Handy-Abonnement kann nur bei Vorlage eines gültigen Passes erworben werden und muss meist auf längere Dauer abgeschlossen werden.

Die Registrierungspflicht hinderte die Bürger mit Pass allerdings nicht daran, falsche Adressen anzugeben, was die Identifizierungspflicht letztlich ad absurdum führte. Auch ist es nicht verboten, Prepaid-Handys weiterzugeben.

Die Menschenrechtsorganisation »augenauf« rief daraufhin zu einer breiten Registrier-Aktion in Zürich und Bern auf. Zahlreiche Schweizerinnen und Schweizer mit gültigem Pass haben daraufhin völlig legal auf ihre Namen tausende von Prepaid-Handy-Nummern von Asylsuchenden oder Sans-Papiers registrieren lassen.

Mit dieser Aktion hat »augenauf« eine Gesetzeslücke sinnvoll genutzt, und aufgezeigt, dass die flächendeckende Registrierung von Prepaid-Handys unnötig hohe Kosten verursacht und letztlich ins Leere läuft.

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund
Vietnamesen-Identifizierung mit Hilfe deutschen Drucks

Auf rechtlich äußerst zweifelhafte Weise leisten deutsche Behörden der vietnamesischen Regierung Amtshilfe bei der Identifizierung von Flüchtlingen. Mehrmals im Jahr reisen auf Kosten der deutschen Steuerzahler Delegationen des vietnamesischen Innenministeriums durch Deutschland und vernehmen in hiesigen Polizeidienststellen vietnamesische Flüchtlinge, um deren Identität festzustellen und so den Rücktransport zu ermöglichen. Verweigern die Flüchtlinge – in der Regel abgelehnte Asylsuchende – die Befragung, helfen die deutschen Behörden nach. So wurde ein Vietnamese mit fester Arbeit und Wohnsitz, der nach Angaben seiner Anwältin regelmäßig in vietnamesischen Exilzeitschriften publiziert, Anfang Oktober 2005 in Friedberg/Hessen verhaftet und zur Befragung offensichtlich widerrechtlich nach München gebracht. Das Landgericht Gießen hob den Haftbefehl auf; nach Ansicht der Richter hatte es einen Haftgrund zu keinem Zeitpunkt gegeben (Der Spiegel 43/2005, 22).

Bund
Testsieger bei Biometrie-Studie: Fingerabdruck

Beim bislang größten staatlichen Praxistest verschiedener biometrischer Verfahren – durchgeführt vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundeskriminalamt (BKA) unter dem Namen BIOP II – war ein System Sieger, das Fingerabdrücke scannt. Mehr als 2000 Mitarbeitende am Frankfurter Flughafen testeten vier Monate lang vier verschiedene Systeme: Gesichtserkennung, Iriserkennung und zweimal Fingerabdruckidentifizierung. Die biometrischen Informationen der Testpersonen waren in einer Datenbank gespeichert; das Prüfsystem sollte den Zugang nur freigeben, wenn die Daten mit den tatsächlichen Merkmalen übereinstimmten. Die geringsten Fehlerraten hatte dabei das System der hamburger Firma Dermalog, das beide Zeigefinger scannt. Auch das zweitplatzierte System nutzt Fingerabdrücke. Auf dem dritten Platz landete ein Verfahren zur Gesichtserkennung. Am schlechtesten funktionierte bei diesem Praxistest die Iriserkennung. Letztere wird von Datenschützern favorisiert, weil sie die freiwillige Mitarbeit des Überprüften voraussetzt. Dies kommentiert der schleswig-holsteinische Datenschutzbeauftragte Thilo Weichert: »Die Ergebnisse der Studie passen erstaunlicherweise genau auf das, was politisch geplant ist.« Das Bundesinnenministerium sieht sich denn auch durch die Studie in seinen Planungen bestätigt, bei der Einführung von biometrischen Ausweisen mit Fingerabdrücken und elektronischer Gesichtserkennung zu arbeiten.

Der Chaos Computer Club (CCC) warf den Behörden vor, sie hätten jene Ergebnisse zurückgehalten, die zeigen, wie die Sicherheitssysteme geknackt werden könnten. Zudem seien die Parameter im Verlauf der Studie verändert worden. Die viel zu hohen False Rejection Rates (FRR) machten sämtliche Systeme nicht benutzbar. BSI-Sprecher Michael Dickopf sagte dazu, die Daten zur Überwindungssicherheit seien nur von »eingeschränkter statistischer Relevanz« gewesen. Die veränderten Parameter hätten der Anpassung an verschiedene Standorte gedient. Verbesserungsbedarf sehen allerdings auch die Autoren der BIOP-II-Studie – nicht nur mit Blick auf die Technik, sondern auch bzgl. der Benutzerfreundlichkeit. Nach dem Fazit der Studie könnten aber biometrische Verfahren Passkontrollen »wirksam unterstützen« In einer früheren Version der Studie war diese Einschätzung noch vorsichtiger ausgefallen. Damals hieß es, vor dem Einsatz »sollten eine sorgfältige Definition des konkreten Szenarios sowie eine Anpassung der Systeme auf die konkreten Anforderungen und Umfeldbedingungen erfolgen« (Der Spiegel 36/2005, 19; Böcking, SZ 14.09.2005, 11; PE CCC 08.09.2005).

Bund
Kritik am biometrischen Reisepass und Ausweis

Jeder Bürger, der ab dem 01.11.2005 einen neuen Reisepass beantragt, erhält von seiner Melde- und Passbehörde ein solches Dokument mit Silizium-Chip und Antenne aus Kupferlegierung. Der Chip speichert vorläufig neben den normalen Passdaten nur das Foto der InhaberIn. Über die Antenne sollen zugelassene Lesegeräte die Daten erheben und anhand dieser die Menschen unterscheiden können. Ab März 2007 sollen die Passbehörden auch die Daten der Abdrücke von beiden Zeigefingern im Chip speichern. Danach sind vergleichbare Personalausweise geplant – auch auf europäischer einheitlicher Basis. Deutschland plant die elektronischen Personalausweise bereits für 2007. Mit der schnellen Einführung des Biometriepasses will Deutschland den Vorgaben der USA genügen: Nur BürgerInnen von Staaten, die bis Oktober 2006 begonnen haben, solche High-Tech-Dokumente einzuführen, dürfen weiterhin ohne Visum in die USA einreisen.

Ziel der Automation und Biometrisierung der Ausweisdokumente ist auch die Verbesserung der Ausländerüberwachung. Die EU will in den nächsten Jahren rund um die Schengen-Staaten einen biometrischen Schutzwall ziehen. Wer in einer Auslandsvertretung ein Visum beantragt, soll dort seine Fingerabdrücke erfassen lassen. Alle Daten sollen in zwei zentra-

len Rechnern in Straßburg und Salzbuch gespeichert werden. Versuche mit Fingerabdrücken in der deutschen Botschaft in Nigeria brachten – so der frühere Bundesinnenminister Otto Schily (SPD) – »bemerkenswerte Erfolge«. Alle, die ein langfristiges Visum für die Bundesrepublik beantragten, mussten dort bis März 2005 ihre Fingerabdrücke hinterlassen. Beim Abgleich mit deutschen Dateien, v.a. dem Automatisierten Fingerabdruck-Identifikationssystem (AFIS) beim Bundeskriminalamt (BKA), seien 40% als abgeschobene Kriminelle oder Identitätsbetrüger aufgeflogen. Der Aufbau des 97 Mio. Euro teuren Kontrollsystems soll im Mai 2006 beginnen. Nach den Plänen würde dieses Visa-Informationssystem die größte Fingerabdruckdatenbank der Welt werden. Das Know-how für die Installation derartiger großer Datenbanken besteht derzeit weltweit bei fünf Anbietern, u.a. bei der hamburger Firma Dermalog. Dermalog hat einen Prototyp des Systems schon aufgebaut mit einem Zentralrechner als Kernstück mit 1,6 Terabyte Speicherplatz, was für die Fingerabdrücke von einer Millionen Menschen reicht. Beim Bedarf nach mehr Kapazität werden einfach zusätzliche Festplatten angehängt. Die Kosten des Systems sollen 1 Mio. Euro pro 1 Mio. gespeicherte Datensätze betragen. Die Dauer eines Fingerabdruckabgleiches soll bei 10 Sekunden liegen.

Die Fehlerraten bei sämtlichen biometrischen Verfahren sind durchgängig noch sehr hoch. Bei den Fingerabdrücken liegt dies oft daran, dass die Papillarlinien wegen zu starker Abnutzung nicht automatisch gelesen werden können. Beim Gesichtsscan sind wechselnde Lichtverhältnisse, Vollbärte und Brillen hinderlich. Durch zusätzliche Sicherheitsmaßnahmen sollen die Fälschungs- und Täuschungsrisiken (z.B. Fotos beim Gesichtsscan, Latexfingerkuppen) reduziert werden. Neue Fingerscanner messen schon Puls sowie den elektrischen Widerstand der Haut, was das Fälschen erschwert. Das Fraunhofer Institut Graphische Datenverarbeitung in Darmstadt arbeitet daran, das Gesicht nicht zwei-, sondern dreidimensional zu erfassen. Fälscher müssten künftig sehr gute Masken tragen.

Sinn und Zweck der elektronischen Biometrie werden von Datenschützern und Bürgerrechtlern in Frage gestellt. Unstreitig und von Schily zugestanden ist, dass Deutschland jetzt schon in puncto Fälschungen »den sichersten Reisepass der Welt« hat. Der Chip im Pappdeckel sei »kein Allheilmittel, aber ein wichtiger Baustein im Kampf gegen den internationalen Terrorismus«. Die Apparate, die die biometrischen Daten an den Grenzen auslesen können, wird es überall erst in einige Jahren geben. Erst in 10 Jahren sollen umfassend Kameras eingeführt werden, die einen automatisierten Gesichtsabgleich bei den Reisenden vornehmen können. Bisher waren offiziell von der Bundesregierung Dateien, in denen die Körpermerkmale aller BundesbügerInnen gespeichert werden, nicht geplant. Nach Auffassung der Humanistischen Union (HU), des Chaos Computer Clubs (CCC), des Forums InformatikerInnen Frieden und gesellschaftliche Verantwortung, der JungdemokratInnen/Junge Linke und des Netzwerks Neue Medien wird hier ein Sicherheitsplacebo mit inakzeptablen bürgerrechtlichen Nebenwirkungen zwangsverabreicht.

Für den parlamentarischen Geschäftsführer der Bundestagsfraktion Bündnis 90/Die Grünen, Volker Beck, ist der so genannte »ePass« ein Musterbeispiel dafür, wie EU-Regelungen Rechte der nationalen Parlamente aushebeln können. Unter dem Eindruck der Anschläge in Madrid hatten sich die Justiz- und Innenminister im Dezember 2004 – nach massivem Einfordern von Schily – für die zwangsweise EU-weit einheitliche Einführung des neuen Passes entschieden. Die digitalen Bilder müssen danach innerhalb von 18 Monaten eingeführt sein, also bis August 2006. Beck: »Keiner konnte uns bisher belegen, was das bringen soll.« Der Bundesbeauftragte für den Datenschutz, Peter Schaar, warnt vor den Folgen der neuen Technik: »Keine Technik ist hundertprozentig sicher.« Er fürchtet um die Sicherheit der Daten, wenn z.B. andere Staaten die Informationen bei der Grenzkontrolle auslesen. Wer garantiert, dass etwa Pakistan oder China diese Daten nicht speichern? In das gleiche Horn stößt Dr. Christoph Bruch, Mitglied des Bundesvorstands der HU: »Ohne erkennbaren Sicherheitsgewinn baut die Bundesregierung eine Überwachungsinfrastruktur mit hohem Missbrauchspotenzial auf. Das entspricht nicht unserem Demokratieverständnis«. Die biometrischen Verfahren und die eingesetzten Funkchips böten mannigfaltige Möglichkeiten zur Überwachung von Menschen. Es sei kein neues Phänomen, dass einmal installierte Technologien zur Identifizierung und Überwachung die Begehrlichkeiten von Geheimdiensten, Ermittlungsbehörden, aber auch kommerziellen Unternehmen wecken.

Hinter dem politischen Interesse an der neuen Technik steckt unzweifelhaft vor allem ein ökonomisches Kalkül. Sandra Schulz, vom Branchenverband Bitkom weist darauf hin, der ePass trage dazu bei, »dass deutsche Sicherheitstechnologie auch ein Exporterfolg wird«. Sowohl bei der Herstellung von Pässen und Chips wie auch im Bereich der Biometrie liegen deutsche Firmen an der Weltspitze. Dazu gehören Unternehmen wie die Dresdner Gesichtserkennungsfirma Cognitec oder die ehemalige Bochumer Firma ZN Vision, die 2004 vom US-Hersteller Visage aufgekauft wurde und bereits etliche US-Bundesstaaten mit Gesichtserkennungssystemen für Führerscheine ausgestattet hat. Die Fingerabdruckfirma Dermalog hat schon mehr als 20 Großprojekte im Ausland realisiert.

Nach einer Studie des Marktforschungsunternehmens Soreon Research wird der Umsatz auf dem deutschen Biometriemarkt von 12 Mio. Euro im Jahr 2004 auf 144 Mio. in 2007 steigen. Weltweit sollen 2006 rund 2,1 Mrd. Dollar umgesetzt werden. Kunden sind in der Regel Regierungen, manchmal auch internationale Organisationen wie die Weltbank. Beispiel Jemen: Dort erhalten Beamten ihr Salär nur noch, wenn sie ihre Finger scannen lassen. Denn viele Staatsdiener kassieren für zwei oder drei Jobs gleichzeitig, ohne dass der Arbeitgeber hiervon wüsste. Die jemenitische Regierung hofft, mit dem Millionen-Dollar-Projekt bis zu 60.000 Doppelbeamte auffliegen zu lassen (Meyer/Stark, Der Spiegel 41/2005, 54 ff.; Gemeinsame PE HU/CCC/FIfF/JuDos/JL, NNM v. 04.10.2005).

Bund
Beim Reisepassfoto ist Lächeln verboten

Vom 01.11.2005 an werden in Deutschland als zweitem EU-Mitgliedstaat – nach Belgien – neue elektronische Reisepässe ausgegeben. Neben den üblichen Daten enthalten diese ein Lichtbild, das auch in einem digital lesbaren Chip gespeichert ist. Für diese Passfotos gelten künftig strenge Regeln: Sie werden frontal aufgenommen; auffällige Kopfbedeckungen, spiegelnde Brillen und verschattete Stirnen sind ebenso untersagt wie Profilbilder, schläfrig halb geschlossene Augen und alles, was

über den Hauch eines Lächelns hinausgeht. Als Konzession für unsere islamischen Mitbürgerinnen sind stramm sitzende Kopftücher als passtauglich anerkannt. Nähere Auskünfte über die neuen Pässe erteilen das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn sowie die Bundesdruckerei, die auf einer »Mustertafel« Hinweise für das richtige Foto gibt.

Mit der digitalen Speicherung ist künftig die biometrische Erfassung geplant, d.h. das Vermessen des Gesichts durch automatisierte Sicherheitssysteme. Ab März 2007 werden zusätzlich zwei Fingerabdrücke digital erfasst. Diese Merkmale können bei der Grenzkontrolle maschinell mit dem Passinhaber verglichen werden. Ziel ist es, gefälschte und gestohlene Reisedokumente leichter zu erkennen. Alte Pässe bleiben weiterhin gültig, vorerst auch für Reisen in die USA. Die neuen Pässe bleiben auch gültig, wenn der Chip – aus welchem Grund auch immer – funktionsuntüchtig werden sollte. Statt bisher 23 Euro wird der neue Pass 59 Euro kosten (SZ 16.09.2005, 6; Ramelsberger SZ 05.10.2005, 1, 6; zu Großbritannien s.u. S. 29).

Bund
Statistiker fordern neue Volkszählung

Der Präsident des Statistischen Bundesamtes, Johann Hahlen, hält eine aktuelle Zählung der Bevölkerung für dringend nötig. Die Veränderungen seit der letzten Volkszählung 1987 im Westen und einer Erhebung 1983 in der damaligen DDR seien so gravierend, »dass wir in Deutschland wieder einen Zensus brauchen«. Die auf einer Fortschreibung der vorliegenden Daten beruhende Bevölkerungsstatistik werde im Laufe der Jahre immer unschärfer. Danach zählt die Bevölkerung in Deutschland derzeit 82,5 Mio. Durch die Wiedervereinigung, den zunächst starken Zuzug von Spätaussiedlern, die Aufnahme von Bürgerkriegsflüchtlingen und weitere Bevölkerungsbewegungen hätten sich die Daten erheblich verändert. Nach Auffassung der Statistiker sollte sich die Bundesrepublik an der für die Jahre 2010/2011 geplanten EU-weiten Zensusrunde beteiligen.

Spätestens zum Jahr 2007 solle ein Gesetz für den Aufbau eines Gebäude-Adressregisters verabschiedet werden. Im Unterschied zu 1987, als es erheblichen Widerstand gegen die Volkszählung gab, möchte Hahlen einen »registergestützten Zensus« durchführen. Dabei sollen die Melderegister bei den Kommunen und die Register der Bundesagentur für Arbeit genutzt und durch Stichproben und Gebäudezählungen ergänzt werden. Zugleich solle der v.a. von der Wirtschaft beklagte Aufwand für die amtliche Statistik verringert werden (SZ 12.10.2005, 6).

Bund
Durchsuchung bei »Cicero« bedroht Pressefreiheit

Am 12.09.2005 wurde die Redaktion des Potsdamer Monatsblatts »Cicero« durchsucht. Die Ermittler der Staatsanwaltschaft stellten knapp acht Stunden lang die Räume des Cicero-Mitarbeiters Bruno Schirra sowie dessen Privatwohnung auf den Kopf und nahmen 15 Kisten voller Unterlagen mit, darunter Material über die Leuna-Affäre und andere Recherchefrüchte aus rund 10 Jahren Arbeit, die mit dem Anlass der Ermittlungen nichts zu tun hatten. Anlass der Durchsuchung war ein 125 Seiten starker Auswertungsbericht des Bundeskriminalamtes (BKA) zum Fall des weltweit verfolgten jordanischen Qaida-Terroristen Abu Mussad al-Sarkawi. Schirra veröffentlichte Textteile im Cicero, nicht ohne sich vorher gewissenhaft beim BKA telefonisch von der Echtheit des Dokumentes vergewissert zu haben. Der Cicero-Artikel erschien im April; es dauerte also einige Monate, bis man sich veranlasst sah, den Journalisten auf's Korn zu nehmen. Der Bericht löste die heftige Reaktionen wohl nicht zuletzt auch aus, weil in dem Bericht Erkenntnisse der CIA und anderer amerikanischer Dienste verarbeitet worden sind. Bei den internen Ermittlungen war herausgekommen, dass allein beim BKA 269 Personen zu dem Papier Zugang hatten. Die nachträgliche Überprüfung von Telefonverbindungsdaten von ca. 20 BKA-Ermittlern auf Journalistenkontakte über einen Zeitraum von mehr als 12 Monaten war ohne Erfolg geblieben. Weil der Täter des »Geheimnisverrates« (§ 353b Strafgesetzbuch – StGB) nicht zu finden war, wurde der Redakteur, der das Papier in die Hände bekam, belangt, wegen der Teilnahme an einer Straftat, die eigentlich nur von Beamten begangen werden kann. Schirra ist überzeugt, dass er vor der Durchsuchung seit längerem observiert worden ist. »Ebenso ist mir klar gesagt worden, dass meine Telefonate abgehört werden«, sagte er mit Hinweis auf Quellen, »die in der Vergangenheit sehr zuverlässig waren«.

Zwar haben Journalisten bzgl. ihrer Quellen nach der Strafprozessordnung (§ 53 StPO) ein Zeugnisverweigerungsrecht, das auch zu einem Beschlagnahmeverbot (§ 97 Abs. 5 StPO) führt. Doch soll dies nicht gelten, wenn dem Journalisten der Vorwurf der Gehilfenschaft zur Tat gemacht wird. Selbst gegen den offenbar völlig ahnungslosen Chefredakteur von Cicero, Wolfram Weimer, wurde ein Ermittlungsverfahren eingeleitet. Die Ermittler versuchten, an Schirras Handy-Verbindungsdaten heranzukommen, doch waren die Daten von der Telekom schon gelöscht. Selbst der stellv. Leiter des BKA, Bernhard Falk, vermutete, dass die Durchsuchung in Schirras Büro keine weiteren Aufschlüsse über den Täter des »Geheimnisverrates« bringen würde, was die Staatsanwaltschaft aber nicht an der Durchsuchungsaktion hinderte. Ende September erläuterte Innenminister Otto Schily beim Jahrestreffen der Zeitungsverleger in Berlin vor mehreren hundert Journalisten und Medienvertretern: »Ich werde mich dafür einsetzen, dass wir die Diskretion im Staat da, wo sie notwendig ist, auch durchsetzen«.

Die Ermittlungen gegen Cicero stießen auf breite Kritik. Dieter Wiefelspütz, innenpolitischer Sprecher der SPD-Bundestagsfraktion, meinte: »Schilys Auftritt war unverhältnismäßig. Der sollte nicht die große Keule schwingen, sondern lieber dafür sorgen, dass es in seinem Zuständigkeitsbereich keine Lecks gibt.« Der frühere Kabinettskollege Schilys und nunmehr Vorstand des WAZ-Verlages in Essen, Bodo Hombach, ergänzt: »Es wird versucht, die Wächterrolle der Medien schleichend umzudefinieren.« Kritische Kollegen würden zunehmend »als Skandalisierer kritisiert«. Das Ziel sei offenbar, »Parteiinteressen mit dem Gemeinwohl gleichzusetzen und Medien als sensationsheischende Störer zu brandmarken«. Die Vorsitzende des Kultur- und Medienausschusses des Bundestages, Monika Griefahn (SPD) meinte: »Jeder Journalist, der investigativ tätig ist, hat Quellen, die er niemals preisgeben wird. Das ist eine Grundvoraussetzung dafür, dass Informanten überhaupt bereit sind, Dinge aufzudecken. Der Informanten-

schutz ist für unsere Demokratie von immenser Bedeutung.« Die Grünen-Chefin Claudia Roth warf Otto Schily einen Angriff auf die Demokratie vor.

Noch-Bundeskanzler Gerhard Schröder stand dagegen Schily bei: Er habe grundsätzlich Vertrauen in die Arbeit von Schily. Und Schily kritisierte seine Kritiker: »Herr Wiefelspütz ist nicht die Instanz, das zu beurteilen. ... Frau Griefahn sollte sich bei mir entschuldigen für ihr törichtes Gerede. ... Der Vorwurf von Frau Roth ist an Albernheit nicht zu übertreffen.«

Die grüne Innenpolitikerin Silke Stokar drohte wegen der Einschränkung der Pressefreiheit mit einem Untersuchungsausschuss. Ähnlich äußerte sich Linkspartei-Vize Petra Pau. Mehr als eine Sondersitzung des Innenausschusses sollte es dann aber doch nicht geben. So meinte der CDU/CSU-Fraktionsvize Wolfgang Bosbach, die Durchsuchungen seien »mehr als fragwürdig. Als Verfassungsminister muss Schily die Verfassung verteidigen – darin steht die Pressefreiheit festgeschrieben. Sie wird von Schily nicht gewährt.« Aber weil der Sachverhalt klar auf der Hand läge: »Einen Untersuchungsausschuss kann ich mir schlecht vorstellen.« Und auch der parlamentarische Geschäftsführer der Grünen, Volker Beck, ruderte zurück: Ein Untersuchungsausschuss sei »die schärfste Waffe des Parlaments«.

Die Beschlagnahme der 15 Umzugskisten voller Unterlagen bei dem Journalisten Schirra brachte zwar nicht den Informanten aus dem BKA zu Tage, wohl aber ein zweites Ermittlungsverfahren, das die Berliner Justiz einleitete. Die Unterlagen betreffen die Ermittlungen des Untersuchungsausschusses rund um die Privatisierung der ostdeutschen Mineralölindustrie, die so genannte Leuna-Affäre. In den Schirra-Beständen fanden sich zudem Papiere, die nie in den Ausschuss eingeführt wurden: geheime Akten des Bundessicherheitsrats, Dossiers über Aktivitäten des einstigen Kanzleramtsministers Friedrich Bohl sowie Dokumente des Bundesnachrichtendienstes über den Kaufmann Dieter Holzer mit dem Stempel »Verschlusssache – amtlich geheim gehalten«. Schily rechtfertigte auch diese Ermittlungen, die erst durch die Zufallsfunde ausgelöst worden sind: »Wenn die Staatsanwaltschaft Hinweise auf einen Mord findet, sagt sie ja auch nicht: Das müssen wir liegen lassen.«

Volker Beck von Bündnis 90/Die Grünen kündigte nach diesen Ausweitungen an: »Sollten die Cicero-Ermittlungen nicht eingestellt werden«, so würde seine Fraktion aktiv, um die gesetzlichen Hürden für die Beschlagnahme journalistischen Materials zu erhöhen. Die Grünen schlugen vor, dass für Durchsuchungen und Beschlagnahmen bei Journalisten nicht mehr ein einfacher Anfangsverdacht genügt. Vielmehr solle ein dringender Tatverdacht der Teilnahme einer Straftat erforderlich sein. Die Maßnahmen sollten immer unzulässig sein, in denen sich der Teilnahmeverdacht auf eine Straftat richtet, die lediglich in der Weitergabe von Informationen an Journalisten bestehen soll. Die Verwertung von Zufallsfunden sollte ausgeschlossen werden. Die Idee wird von der FDP unterstützt. Auch SPD-Innenpolitiker Wiefelspütz forderte eine »Debatte über den Einzelfall hinaus«.

Gemäß den Angaben des Deutschen Journalistenverbandes fanden von 1987 bis 2000 mehr als 150 Durchsuchungen von Zeitungs- und Funkhäusern sowie Privatwohnungen von Journalisten mit Beschlagnahmen von Recherchematerial statt. In keinem einzigen Fall sei es aber zu einer Verurteilung des verdächtigten Journalisten gekommen. Aber das erklärte Ziel wurde mitunter erreicht, wenn die Informanten entdeckt wurden (Darnstädt/Neubacher/Rosenbach/Nelles, Der Spiegel 40/2005, 36 ff.; Stark/Wassermann/Winter, Der Spiegel 38/2005, 178 ff.; Der Spiegel 41/2995, 40 ff.; Neubacher/Stark, Der Spiegel 42/2005, 50; Kieler Nachrichten 08.10.2005, 4; SZ 08./09.10.2005, 7; Ramelsberger SZ 06.10.2005, 7; Prantl SZ 28.09.2005, 4; SZ 27.09.2005, 17; SZ 10.10.2005, 6; Hufelschulte/Thalmann, Focus38/2005, 42 f.; Neuber, www.heise.de 15.09.2005; PE BT-Fraktion Bündnis 90/Die Grünen Nr. 973 v. 12.10.2005).

Bund
2004 weniger große Lauschangriffe

Aus einem dem Bundestag zugeleiteten Jahresbericht der alten Bundesregierung ergibt sich, dass die Zahl der akustischen Wohnraum-Überwachungen von 37 im Jahr 2003 auf 11 im Jahr 2004 gesunken ist. In 6 der 11 Verfahren seien relevante Ergebnisse erzielt worden. In 4 Fällen hätten die Ermittlungen einen Bezug zu Straftaten der organisierten Kriminalität gehabt. Die akustische Wohnraum-Überwachung – vulgo großer Lauschangriff – ist seit 1998 erlaubt. Nach Ansicht der alten und neuen Bundesjustizministerin Brigitte Zypries belegen die Zahlen, dass das Urteil des Bundesverfassungsgerichts vom 3. März 2004 »die Praxis veranlasst hat, die akustische Wohnraumüberwachung noch zurückhaltender als bisher einzusetzen.« Auf die Einschränkungen des Bundesverfassungsgerichts, insbesondere zum Zweck der Schutzes des Kernbereichs privater Lebensgestaltung, reagierte die rot-grüne Koalition mit einem Gesetz, das seit dem 01.07.2005 in Kraft ist. »Die Bundesregierung hat den Strafverfolgungsbehörden damit klare Vorgaben an die Hand gegeben, die auch in Zukunft den zielgerichteten Einsatz dieses wichtigen Ermittlungsinstruments gewährleisten.« Zypries wies darauf hin, dass – anders als in den Vorjahren – nicht überwiegend Tötungs- und schwere Betäubungsmitteldelikte zu Abhöraktionen geführt hätten. Statt dessen sei der Lauschangriff 2004 auch bei Bestechungs- und Schleusungsdelikten eingesetzt worden. Dies zeige, dass es richtig gewesen sei, den Anwendungsbereich nicht zu stark zu beschränken. Das Grundgesetz verpflichtet die Bundesregierung, jährlich einen Bericht über die großen Lauschangriffe vorzulegen (Roßmann, SZ 25.08.2005, 6).

Bund
Finanzministerium ermittelt undichte Stelle

Bei der Ermittlung undichter Stellen im Bundesfinanzministerium kurz vor der Bundestagswahl 2005 ist die Leitung des Hauses angegriffen worden. In der Endphase des Wahlkampfes sind Artikel in den Medien erschienen, die den Eindruck erweckten, dass – so ein Schreiben an die MitarbeiterInnen – »ein riesiges Kürzungspaket in Auftrag gegeben worden sei«. In dem Fall seien interne Dokumente gezielt nach außen gegeben worden, was einen Verstoß gegen die Amtsverschwiegenheit darstelle. Es wurden verwaltungsinterne Ermittlungen eingeleitet. Daraufhin wurden in der Union und in der FDP der Verdacht geäußert, Computer, Telefone, Faxgeräte und Büros von MinisteriumsmitarbeiterInnen seien ohne deren Kenntnis durchforstet worden. In einer Antwort auf eine Anfrage des FDP-Haushaltspolitikers Jürgen Koppelin

teilte der parlamentarische Staatssekretär Karl Diller mit, die Mitarbeiter des IT-Referates seien mit administrativen Rechten ausgestattet, so dass sie theoretisch »ohne Wissen der Anwender auf deren Computer zugreifen« könnten. Dies sei aber praktisch nicht geschehen. Wohl sei aber der Mailverkehr »mit Einverständnis der betroffenen Mitarbeiter« nachvollzogen worden, womit aber »nicht Mitarbeiter überprüft, sondern Abläufe sachlich nachvollzogen« worden seien (Schäfer, SZ 08./09.10.2005, 5).

Bund

Schwarz-rote Koalition will Datenschutz auf Prüfstand stellen

Union und SPD haben ihre Leitlinien zur Innenpolitik im Rahmen der Koalitionsvereinbarung in einem achtseitigen Papier festgelegt. Danach ist unter dem Titel »Deutschland – ein sicheres und freies Land« die Bekämpfung des Terrorismus weiterhin »eine sehr wesentliche Aufgabe aller deutschen Sicherheitsbehörden«. Der Bürger habe einen »Anspruch, vor Kriminalität geschützt zu werden«. Dem müssten andere verfassungsrechtliche Sicherungen untergeordnet werden. So gelte es zu überprüfen, »inwieweit rechtliche Regelungen etwa des Datenschutzes einer effektiven Bekämpfung des Terrorismus und der Kriminalität entgegen stehen«, und wie die an sich »bewährte Sicherheitsinfrastruktur« weiterentwickelt werden müsse.

Die Koalitionspartner wollen »auf der Basis der Vorarbeiten der Innenministerkonferenz schnellstmöglich eine Antiterrordatei schaffen« und den Informationsaustausch zwischen Polizei und Nachrichtendiensten bei der Bekämpfung des islamistischen Terrorismus verbessern. Die Einrichtung des Gemeinsamen Terrorismusabwehrzentrums in Berlins sei dabei nur ein erster, wenn auch wichtiger Schritt gewesen. So soll das Bundeskriminalamt (BKA) endlich die von der dortigen Führung lange geforderte »Präventivbefugnis« zur Abwehr von Gefahren des internationalen Terrorismus erhalten und damit stärker mit Geheimdienstmethoden agieren dürfen. Schwarz-Rot kündigte an, die Ausrüstung von Ausweisdokumenten mit biometrischen Daten fortzusetzen: »Wir wollen biometrische Verfahren verstärkt einsetzen.« Pass- und Personalausweisgesetz sollen entsprechend novelliert werden. Auf EU-Ebene soll schnell ein Visainformationssystem aufgebaut werden, das Schengener Informationssystem soll ausgebaut werden (www.heise.de 07.11.2005; vgl. auch die Presseerklärung der ILMR auf S. 32).

Bund

SMS-Fahndung endgültig gescheitert

Die Fahndung per SMS ist offenbar endgültig gescheitert. Im Februar 2004 hatte Otto Schily den Startschuss zur bundesweiten Fahndung per SMS gegeben. Die Polizei sollte Fahndungsmeldungen per SMS auf die Handys vorzugsweise von Taxifahrern, Bus- und Straßenbahnfahrern oder Mitarbeitern der städtischen Ordnungsämter senden. Die Empfänger mussten sich dazu vorher freiwillig registrieren lassen.

Viele Polizeibehörden hatten erhebliche Zweifel an der Effizienz dieser Fahndungsmaßnahme und verzichteten daher auf eine Einführung. Tests in Sachsen-Anhalt und Niedersachsen wurden bereits vor Monaten eingestellt, nachdem die Resonanz ausblieb und kein Gesuchter durch Hinweise aufgrund der versandten Kurznachrichten gefunden oder gar gefangen werden konnte. Nach den Pilotversuchen in Magdeburg und Lüneburg beendete nun auch die Polizei in Bochum als letzte Behörde ihre SMS-Fahndung. Laut nordrhein-westfälischem Innenministerium werde eine landesweite Einführung nicht mehr erwogen (AFP, yahoo 30.09.2005).

Bund

Kronzeugenregelung kommt zurück

Die große Koalition von SPD und CDU/CSU will – trotz des Widerstandes von juristischen Berufsverbänden – die Kronzeugenregelung wieder einführen. Damit wird Straftätern Strafmilderung oder gar Straffreiheit versprochen, wenn diese frühere Tatgenossen belasten. 1989 war die Kronzeugenregelung als Wundermittel gegen den RAF-Terrorismus ins Strafgesetzbuch aufgenommen worden. Bis dahin hatte es eine solche Vorschrift nur im Betäubungsmittelrecht gegeben. Die Regelung wurde bis Ende 1992 befristet – eine Verlängerung sollte angesichts der vorgetragenen juristischen Bedenken nur bei erkennbaren Erfolgen in Betracht gezogen werden. Die zeitliche Befristung wurde mehrfach verlängert. Erst die rot-grüne Koalition akzeptierte – auf Drängen der Grünen – keine Verlängerung mehr, so dass die Regelung 1999 auslief. Die Länderjustizminister drängten – unterstützt vom damaligen Bundesinnenminister Otto Schily (SPD) – auf eine Wiedereinführung – u.a. mit dem Argument, so ließe sich der gewalttätige Rechtsextremismus bekämpfen. Die 2001 im Amt befindliche Bundesjustizministerin Herta Däubler-Gmelin legte 2001 einen Gesetzentwurf vor, der nunmehr wieder die Grundlage für weitere Diskussionen ist:

»Hat der Täter eine Straftat, die mit einer im Mindestmaß erhöhten zeitigen Freiheitsstrafe oder mit lebenslanger Freiheitsstrafe bedroht ist, sein Wissen über Tatsachen offenbart, deren Kenntnis geeignet ist, 1. die Begehung einer solchen Tat zu verhindern, 2. die Aufklärung eines solchen Tat, falls er daran beteiligt war, über seinen Tatbeitrag hinaus, zu fördern, oder 3. zur Ergreifung eines Täters oder Teilnehmers einer solchen Straftat zu führen, kann das Gericht auf Freiheitsstrafe nicht unter fünf Jahren erkennen.«

Die Kritiker an dieser Regelung haben Bedenken, auch wenn diese nicht zu einer kompletten Straflosigkeit, sondern nur zu einer Milderung führt. Sie befürchten u.a., dass man sich den Kronzeugenbonus durch falsche Angaben erschleichen kann, mit denen u.U. Andere zu Unrecht belastet werden. Ungeklärt ist bisher, wie ein Gericht reagieren soll, wenn sich später zeigt, dass Angaben falsch waren (Prantl, SZ 27.10.2005, 6).

Bund

Schutz für Tippgeber?

Der Skandal um verdorbenes Geflügelfleisch aus Niedersachsen, bei dem die Staatsanwaltschaft Oldenburg u.a. einen Betrieb in Lastrup bei Cloppenburg geschlossen hatte, wurde bekannt, nachdem eine Mitarbeiterin der insolventen Firma berichtet hatte, dass dort gefrorenes Fleisch unsachgemäß aufgetaut und als Frischfleisch in den Handel gebracht wird. Nun bestätigte die Gewerkschaft Nahrung-Genuss-Gast-

stätten (NGG), dass sie Anfang des Jahres 2005 von zwei Mitarbeitern über solche Praktiken in dem Betrieb informiert worden waren. Den beiden sei damals geraten worden, mit ihrem Wissen zur Polizei zu gehen. Dies hatten die aus Angst vor Kündigung aber nicht gewagt. Der NGG-Vorsitzende Franz-Josef Möllenberg forderte nun einen besseren Informantenschutz für Mitarbeitende in der Lebensmittelbranche. Es müsse gesetzlich verhindert werden, dass Arbeitgeber z.B. über die Akteneinsicht im Verfahren herausfinden können, wer ihre Praktiken verraten hat. Außerdem müssten Tippgeber vor Kündigung geschützt werden: »Die Zahl der Lebensmittel-Skandale in jüngster Zeit zeigt, dass dringend gehandelt werden muss – zumal die staatlichen Kontrollen nicht ausreichen« (Der Spiegel 45/2005, 20).

Baden-Württemberg, Bayern, Hessen, Rheinland-Pfalz, Bund

Großfahndung in Rhein-Main gegen Islamanhänger

Die Länder Baden-Württemberg, Bayern, Hessen und Rheinland-Pfalz haben sich auf verstärkte Fahndungsaktionen in der Umgebung von Moscheen und in der muslimischen Geschäftsszene verständigt. Die Polizei will damit schon frühzeitig Kleinkriminelle aufspüren, die – nach dem Muster der Anschläge von Madrid – mit der Fälschung von Ausweisen und Kreditkartenbetrug Attentate finanzierten und vorbereiteten. Der Mainzer Innenminister Karl Peter Bruch (SPD): »Wir müssen Licht ins extremistische Gestrüpp bringen.« Eine Aktion in diesem Kontext war eine Razzia am 26.09.2005 in 20 hessischen Städten, bei der mehr als 1260 Menschen kontrolliert wurden. Nach Ansicht des hessischen Innenministers Volker Bouffier muss die Polizei dahin gehen, wo gefährliche Strukturen entstehen. Aktionen dieser Art werde es in Zukunft drei- bis viermal im Jahr geben. Bruch ergänzt: »Wir wollen Bewegungsbilder von Verdächtigen erkennen, wir wollen aber auch präventiv wirken: Die Leute sollen merken, dass wir genau hinschauen.«

Der große Einsatz gegen die islamistische Szene war eigentlich schon im Juli geplant – genau einen Tag nach dem Anschlag auf die Londoner U-Bahn. Die Verantwortlichen verschoben dann sofort ihre Pläne. Die Polizei hat für diese Aktionen ein spezielles Verdachtsraster erarbeitet. So beobachten die Polizisten v.a. Personen, die mehrere Mobiltelefone benutzen. Die Beamten prüfen verstärkt Führerscheine und Ausweise auf Echtheit und achten auch auf die Jobs der Kontrollierten. Der hessische LKA-Chef Peter Raisch: »Wer etwa mit Gefahrguttransporten zu tun hat, interessiert uns ganz besonders«. Das Konzept werde »systematische Verdachtsschöpfung« bezeichnet und bundesweit eingesetzt. Bei der Aktion im Frankfurter Bahnhofsviertel wurde eine ganze Straße abgesperrt. Die Geschäftsleute hätten Verständnis für die Razzia gehabt, sagte Polizeisprecher Feist: »Die Ladenbesitzer haben ein starkes Interesse daran, dass die Gegend sauber bleibt und keine Islamisten einsickern«.

Die Muslime sind größtenteils empört, wenn Moscheen durchsucht und Muslime auf der Fahrt zum Freitagsgebet überprüft werden, dass verdeckte Ermittler auch in Moscheen arbeiten und sie immer wieder hören, die muslimischen Gemeinden lieferten keinerlei Hinweise an die Polizei. »Es ist eine Unterstellung, dass wir die Polizei nicht unterstützen«, sagt Mounir Azzaoui vom Zentralrat der Muslime in Deutschland. Muslime seien doch keine Hilfspolizisten, verwahrt sich der Vorsitzende des Islamrats in Deutschland, Ali Kizilkaya. Am 22.09.2005 kam es zu einem Treffen der Spitzen von Bundeskriminalamt, Bundesverfassungsschutz, Landeskriminalämtern und Landesverfassungsschutz mit den Vertretern der türkischen Moscheevereinigung Ditib und dem Zentralrat der Muslime. Die beiden Verbände vertreten etwa 1000 Moscheen in Deutschland (Ramelsberger SZ 30.09.2005, 6; Ramelsberger SZ 23.09.2005, 7).

Baden-Württemberg

Österreicherin zum Deutschtest geschickt

Eine Österreicherin, die sich in Deutschland einbürgern lassen wollte, ist vom Ordnungsamt Stuttgart zum Deutschtest geschickt worden. Im persönlichen Gespräch habe sich die zuständige Sachbearbeiterin zunächst nicht von den Sprachkenntnissen der 62jährigen überzeugen lassen, bestätigte das Amt einen Bericht der Stuttgarter Zeitung. Das Gespräch mit der Sachbearbeiterin sei »nicht glücklich verlaufen«. Die Österreicherin arbeitet seit neun Jahren in Stuttgart und leitet Literaturkreise – auf Deutsch (SZ 27./28.08.2005, 12).

Baden-Württemberg

Flächendeckende Kontoermittlung gegen Raubkopierer

Die Ermittlungen im Zusammenhang mit dem im Herbst 2004 aufgeflogenen Raubkopie-Portals ftp-welt.com richteten sich gegen 15.000 KundInnen dieses Anbieters, die über Monate hinweg illegal Filmhits, Musik, Software und Spiele heruntergeladen haben. Um an deren Personalien zu kommen, hatte das Landeskriminalamt Baden-Württemberg 1009 Banken angeschrieben. Mit Stand Oktober 2005 lagen 1003 Antworten vor. Sechs Anfragen wurden noch bearbeitet. Unklar ist, gegen wie viele KundInnen Ermittlungsverfahren eingeleitet werden. Hierüber entscheidet jeweils die für die Heimatanschrift zuständige Staatsanwaltschaft (Der Spiegel 40/2005, 211).

Bayern

Banken-Rasterfahndung zwecks Mordermittlung

Ein Nürnberger Ermittlungsrichter hat am 30.08.2005 dem Antrag der Staatsanwaltschaft auf Durchführung einer groß angelegten Rasterfahndung bei Banken zugestimmt. Über die Auswertung von Kontobewegungen soll vom Landeskriminalamt in München eine Serie von sieben Morde an ausländischen Kleinunternehmern aufgeklärt werden, die zwischen 2000 und 2005 in Nürnberg, München, Hamburg und Rostock begangen wurden. Opfer waren ein Grieche und sechs Türken; zuletzt wurden im Juni 2005 ein Dönerstandbesitzer und ein Betreiber eines Schlüsseldienstes getötet. Außer der Erkenntnis, dass immer die gleiche Waffe genutzt wurde, haben die Ermittler noch keine logische Verbindung zwischen den Taten. Die Staatsanwaltschaft will nun die Transaktionen an Geldautomaten sowie an Terminals in

Geschäften und Tankstellen in bestimmten Postleitzahlbezirken in der Zeit vom 08. bis 16.06.2005 abgleichen, die also zur Tatzeit im Umfeld der Tatorte stattgefunden haben. Es sei denkbar, dass der oder die Täter vor oder nach einem Mord Geld abgehoben oder getankt hat bzw. haben. Sollte etwa die mehrfache Verwendung derselben Kredit- oder EC-Karte festgestellt werden, könne dies auf die Spur der Täter führen. Es erfolgten 2000 Anfragen an verschiedene Banken, die Daten in einer vorgegebenen Form übermitteln müssen. Als Rechtsgrundlage für diese massenhafte Rasterfahndung wurde § 98a Strafprozessordnung angegeben. Die Staatsanwaltschaft hatte die Anfragen an die Banken schon zu einem Zeitpunkt verschickt, zu dem der Richter noch gar keine Entscheidung getroffen hatte. Die Kosten sollen den Banken erstattet werden (SZ 31.08.2005, 31; Aufterbeck, Handelsblatt 30.08.2005, 8:50).

Bayern

Siemens schnüffelt in Betriebsrats-Emails

Der Anwalt eines Betriebsratsvorsitzenden bei dem Weltkonzern Siemens, Jürgen Fischer, erhebt schwere Vorwürfe gegen die Unternehmensleitung: Für diese soll der werksinterne Sicherheitsdienst Computer des Betriebsrates ausspioniert und hierbei sogar verschlüsselt gespeicherte Emails gelesen haben. Seit 2003 scheint es schon Konflikte mit der Betriebsleitung zu geben. Mit der »Datenausspähung« sei jedoch die Tätigkeit der Arbeitnehmervertreter massiv untergraben worden und deren Unabhängigkeit beschädigt. Beschäftigte könnten sich nicht mehr darauf verlassen, dass vertrauliche Emails an den Betriebsrat nicht auch vom Chef gelesen würden.

2003 hatte ein damaliges Mitglied der Betriebsleitung von Siemens München, Hoffmannstraße unter Angabe seiner Privatadresse und unter Berufung auf eine anonyme Information Strafanzeige gegen den Chef des dortigen Betriebsrates mit dem Vorwurf der falschen eidesstattlichen Versicherung und der Urkundenfälschung erhoben. Protokolle von Betriebsratssitzungen, in denen im Januar 2003 die Widersprüche der Arbeitnehmervertreter gegen 366 Kündigungen behandelt wurden, seien manipuliert worden, wobei es vor allem um Termine und Formfragen ging. In der Strafanzeige wurde die »Sicherstellung« der Protokollversionen beim Betriebsrat angeregt. Daraufhin bat die zuständige Staatsanwältin die Polizei, an die Firma Siemens heranzutreten »mit der Bitte, entsprechende Einträge in ihren Computern aufzuarbeiten«. Die Polizei forderte tatsächlich Siemens auf, Daten in Bezug auf die umstrittene Betriebsratssitzung zu sichern.

Hierauf durchsuchte der Sicherheitsdienst der Firma die Dateien des Betriebsrates und beschränkte sich nicht auf die streitigen Protokolle, wie ein 19seitiger Auswertungsbericht belegt. Erst im August hatte der Rechtsanwalt des Betriebsratschefs von den Ermittlungen gegen seinen Mandanten erfahren und setzte sich gegen die »Uferlosigkeit der Schnüffelei« zur Wehr. Danach folgte die Justiz »blindlings der Begehrlichkeit der Unternehmensleitung, in der Auseinandersetzung mit der Vertretung der Arbeitnehmer diese auszuspionieren.« Dabei sei »jegliche Kommunikation zwischen den Betriebsangehörigen und ihrem Betriebsrat ausgeforscht« worden, soweit sie elektronisch gespeichert war. Erst später sei ein richterlicher Durchsuchungsbeschluss erwirkt worden: »Man hatte die selbst ernannten Ermittler bei der Siemens AG mit der Autorität von Hilfssheriffs ausgestattet und sie im Datenbestand des Betriebsrats nach Gutdünken wildern lassen.« Die Durchsicht der Dateien habe nur Staatsanwaltschaft und Polizei zugestanden, doch habe Siemens die Daten selbst geprüft und ausgewertet. Hiermit, so der Anwalt, sei »in die verfassungsrechtlich besonders geschützte Stellung des Betriebsrats eingegriffen« worden. Der Betriebsratsanwalt prüft jetzt seinerseits, ob er gegen Siemens wegen Datenausspähung Strafantrag stellen soll.

Wolfgang Müller vom Siemens-Projekt der IG Metall Bayern wies darauf hin, dass Arbeitgeber sich die Dateien von Betriebsräten nicht so einfach anschauen dürfen. Von der Unternehmensleitung kam auf Pressenachfrage nach zwei Wochen nur die knappe Antwort: »Wir geben keinen Kommentar ab.« Es handele sich um ein schwebendes Verfahren. Ein Sprecher der Staatsanwaltschaft meinte, er könne zu laufenden Ermittlungen nichts sagen. Auch der Arbeitgeberverband Gesamtmetall in Berlin wollte nicht Stellung nehmen (SZ 26.08.2005, 8; vgl. S. 33).

Bayern

Private Toilettenüberwachung vor dem Amtsgericht

Der 23jährige Marcus S. installierte – versteckt in einem Radio – in seiner Privatwohnung auf der Toilette eine Videokamera, deren aufgezeichnete Bilder er nach nebenan live übertrug und beobachten konnte. Sein Pech war, dass er mit seiner absonderlichen Peep-Show prahlte, so dass die Geschichte im Freundeskreis verbreitet wurde. Eine Bekannte erstattete Anzeige und Markus S. wurde wegen der »Verletzung des höchstpersönlichen Lebensbereichs durch Filmaufnahmen« – ein Tatbestand, der erst Sommer 2004 ins Strafgesetzbuch aufgenommen worden war – angeklagt. Als der Angeklagte am 22.08.2005 zum Verhandlungstermin nicht erschien, erließ die Amtsrichterin Haftbefehl (SZ 23.08.2003, 31).

Bayern

Sozialdaten zwecks Büchergeldbefreiung in der Schule

Der Bayerische Datenschutzbeauftragte Reinhard Vetter legte sich mit dem Landes-Kultusministerium in Sachen Büchergeld an. Vetter wehrt sich dagegen, dass Klassenlehrer die Kuverts mit dem Geld oder den Befreiungsanträgen öffnen dürfen: »Die Eltern müssen es nicht hinnehmen, dass die Lehrer ihrer Kinder Kenntnis davon erhalten, dass sie Wohngeld beziehen oder Sozialhilfeempfänger sind.« Die CSU hatte eine ursprüngliche Regelung, wonach nur Vertrauenslehrer die Kuverts öffnen dürfen, Ende September 2005 rückgängig gemacht (SZ 01.-03.10.2005, 49).

Niedersachsen

Datenschutzaufsicht über die Wirtschaft soll zum Innenministerium

Nach dem Willen der schwarz-gelben Landesregierung in Niedersachsen soll ab dem 01.01.2006 die Zuständigkeit für die Datenschutzaufsicht im Bereich der Wirtschaft vom Landesbeauftrag-

ten für den Datenschutz (LfD) zum Innenministerium wechseln. Zum Jahr 1992 war auf Grund eines Beschlusses der damaligen rot-grünen Landesregierung die Zuständigkeit von den Bezirksregierungen zum Landesbeauftragten übertragen worden. Kritiker mutmaßen, Innenminister Uwe Schünemann (CDU) verfolge mit der Entmachtung des Datenschutzbeauftragten Burckhard Nedden (SPD) rein politische Ziele. Behauptet werden dagegen vom Ministerium »Synergieeffekte« und mögliche Einsparungen. Derzeit hat der Stab des LfD 18 Mitarbeiter. Neddens Stelle und die einiger Mitarbeiter könnten – so das Ministerium – heruntergestuft werden. Im Ministerium komme eine Stelle hinzu; unterm Strich werde alles günstiger.

Der Plan findet außerhalb der Landesregierung fast nur Kritiker, die während einer Landtagsanhörung am 30.08.2005 zu Wort kamen. Der Bundesbeauftragte für den Datenschutz Peter Schaar bezweifelt, dass die Neuordnung mit der EU-Richtlinie vereinbar ist, wonach die Datenschutzaufsicht »völlig unabhängig« tätig sein muss. Schaar schlug vor, den Beauftragten der Landtagsverwaltung anzugliedern und ihm keinesfalls Aufgaben wegzunehmen. Dem stimmte für die Humanistische Union Nils Leopold zu: »Die Landesregierung setzt damit auf ein Auslaufmodell der Datenschutzaufsicht«. Die EU-Kommission hatte Anfang Juli 2005 ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, weil bislang nicht alle Aufsichtsbehörden den Vorgaben der Datenschutzrichtlinie entsprächen. Mit der Neuorganisation würden Interessenkonflikte entstehen. Die in der Privatwirtschaft vorgehaltenen Daten, z.B. von Internetprovidern, seien zunehmend für die Strafverfolgung und -verhütung oder im so genannten Kampf gegen den Terror für die Innenministerien interessant. Dies vertrage sich nicht mit einer durch die selbe Behörde durchzuführende Aufsicht über die Einhaltung des Grundrechtsschutzes in Unternehmen. Auch praktische Gründe sprächen für einen Datenschutz aus einer Hand. Mit einem Ansprechpartner werde größere Bürgernähe erreicht. Die innenpolitische Sprecherin der grünen Bundestagsfraktion Silke Stokar griff die FDP an. Diese mache als selbst ernannte Bürgerrechtspartei bei all dem klaglos mit: »Sie spielt ihre Rolle als Trauzeugin bei der Vermählung von Union und Grundrechtsabbau wie bisher weiter« (Wallbaum, HAZ 31.08.2005; PE Stokar 30.08.2005; PE Nr. 13/2005 der HU 29.08.2005; s.o. BBA S. 10f., s.u. S. 39).

Niedersachsen
Polizei sammelt DNA-Proben von CASTOR-GegnerInnen

Nach einer friedlichen Protestaktion in Form eines Volleyball-Spieles, an dem etwa 150 Menschen als SpielerInnen und ZuschauerInnen mitten im Wald an einem Bahnübergang an der CASTOR-Transportstrecke zwischen Lüneburg und Dannenberg Ende Oktober 2005 teilgenommen haben, sammelte die Polizei Zigarettenkippen von Beteiligten auf. Beamte hatten Untersuchungshandschuhe übergezogen und steckten die Kippen einzeln in Plastikbeutel. Zuvor waren die AktionsteilnehmerInnen fotografiert und wohl auch gefilmt worden. Tage später erhielten einige der Betroffenen »schriftliche Verwarnungen mit Verwarnungsgeld« wegen eines Verstoßes gegen §§ 62, 64b der Eisenbahnbau- und -betriebsordnung (EBO), weil sie nach Anordnung von Polizeibeamten den Gleisbereich nicht verlassen hätten. Schon eine Woche davor sollen Polizeibeamte nach einer angemeldeten friedlichen Anti-CASTOR-Demonstration die TeilnehmerInnen fotografiert und Zigarettenkippen aufgesammelt haben.

Bereits im Januar 2005 hatten Bundesinnenminister Otto Schily und Niedersachsens Innenminister Schünemann ihren gemeinsamen Wunsch ausgedrückt, CASTOR-GegnerInnen schon bei Ordnungswidrigkeiten per DNA-Proben und Fingerabdrücken zu erfassen. Das Vorstandsmitglied des Republikanischen Anwaltsvereins (RAV) Martin Lemke beklagte, die Menschenwürde und die Persönlichkeitsrechte würden verletzt, die einschlägigen Datenschutzbestimmungen missachtet sowie alle Betroffenen unter einen nicht gerechtfertigten Generalverdacht gestellt. Wenn die Kippen auf DNA-Spuren hin ausgewertet wurden, so sei damit eine illegale Gendatei errichtet worden. Als Hintergrund der Aktion wird die Suche nach den Urhebern eines Brandanschlages auf die »Seerauer Brücke« am 24.10.2001, von Unterspülungen der CASTOR-Strecke und eines jüngeren Brandes eines Polizei-Containers bei Woltersdorf vermutet. Keine dieser Taten ist bisher aufgeklärt worden. Die Betroffenen kündigten an, bei der Polizei die Vernichtung ihrer Daten sowie eine Unterlassungserklärung für die Zukunft zu fordern.

Die Bürgerinitiative Umweltschutz Lüchow-Dannenberg spricht von einer »grundrechtsfreien Sonderzone Gorleben«. Schon seit Wochen würden AtomkraftgegnerInnen aus dem Wendland wieder überwacht und bespitzelt. Bei Telefonaten gebe es vermehrt Fehlverbindungen und merkwürdige Echos, so ein Sprecher: »Wenn der Rechtsstaat seine Grundlagen aufgibt und sich im Interesse der Energiekonzerne und Atomindustrie zum Polizeistaat wandelt, heißt es, Widerstand zu leisten und erst recht auf die Straße, an die Schiene zu gehen« (Presseerklärung BI Lüchow-Dannenberg und RAV 27.10.2005, www.castor.de).

Hamburg
Videoüberwachung auf der Reeperbahn

Um die Gewaltkriminalität auf der Reeperbahn zu bekämpfen, will Hamburgs Innensenator Udo Nagel ein Dutzend Überwachungskameras rund um die Amüsiermeile installieren lassen. Die Kameras, die Anfang 2006 betriebsbereit sein sollen, können schwenken, zoomen und scharfe Bilder liefern. Beamte sollen in einer Polizeieinsatzzentrale die Bilder in Echtzeit auf einer Videowand mit 16 Einzelmonitoren verfolgen. Nagel möchte damit »die Reeperbahn als Visitenkarte Hamburgs sicherer machen«. Etwaige Befürchtungen, gerade Touristen könnten sich von einer derartigen Überwachung abgeschreckt fühlen, wies er zurück. Man habe so genannte »private zones« eingerichtet, in welche die Kameras keine Einsicht hätten: »Es interessiert uns nicht, wer sich in einer Wohnung auszieht.« Die Kriminalität im Stadtteil St. Pauli wird als schwerwiegend eingeschätzt. Allein im Jahr 2004 war die Zahl der Körperverletzungen um 19% gestiegen, die Zahl der Drogendelikte um 15%. Nagel: »Die Reeperbahn ist der größte Kriminalitätsschwerpunkt in Hamburg«. Von Mai 2004 bis April 2005 habe die Polizei allein auf der Reeperbahn 757 Straftaten gezählt – mehr als in allen anderen Teilen der Stadt. Der Alkohol- und Drogenkonsum auf der Meile berge die Gefahr, dass Auseinandersetzungen eskalieren.

Der Hamburgische Datenschutzbeauftragte Hartmut Lubomierski äußerte sich kritisch: »Videoüberwachung ist kein Allheilmittel. Kriminalität sollte nicht nur beobachtet, sondern auch verhindert werden.« Aus diesem Grund halte er eine zusätzlich Polizeipräsenz an lokalen Brennpunkten wie der Reeperbahn für wesentlich effektiver. Die Erfahrung zeige, dass Kameraüberwachung in der Regel nur zu einer örtlichen Verdrängung und Verlagerung von Kriminalität führe. Außerdem: »Nur der rational handelnde Täter reagiert überhaupt auf diese Form der Kontrolle. Ein Drogenhändler wird vermutlich seinen Arbeitsplatz an eine andere Stelle verlegen. Ein Selbstmordattentäter hingegen wird vor seinem Anschlag vermutlich die Finger zum Siegeszeichen in die Kamera recken.« Gerade die Terroranschläge von London hätten gezeigt, dass auch die Stadt mit der größten Kameradichte Europas nicht vor Attentaten gefeit sei. Auch Menschen im Kiez sind gegen die Überwachung, z.B. ein Kellner: »Das bringt doch auf der Reeperbahn nichts. Hier passiert am wenigsten, weil viel zu viel Betrieb ist. Die Leute werden doch in den Nebenstraßen fertig gemacht.«

Der Hamburger Senat will es nicht bei einem überwachten Straßenzug belassen. Die Innenbehörde plant bereits auch den Einsatz von Kameras an mindestens zwei weiteren Brennpunkten der Hansestadt. Ab Herbst 2006 sollen der v.a. für Drogenkriminalität und Prostitution berüchtigte Hansplatz im Stadtteil St. Georg sowie der S-Bahnhof Bergedorf im Südosten der Stadt überwacht werden (Langer, www.spiegel.de 08.09.2005).

Sachsen

Telefonüberwachung gegen Journalisten

Um Aufschlüsse über die Telefonkontakte eines Foto-Journalisten der Dresdner Morgenpost zu bekommen, versuchte die Staatsanwaltschaft Chemnitz, die Telefonzentrale des Dresdner Pressehauses anzuzapfen, in welchem neben dem Boulevardblatt auch die Sächsische Zeitung residiert. Als dies aus technischen Gründen nicht gelang, wurden die privaten und dienstlichen Telefonkontakte des Journalisten von den Fahndern registriert.

Im Hintergrund steht die Arbeit der staatsanwaltlichen Fahndungsgruppe INES zur Ermittlung von Korruptionsdelikten. Diese war ins Gerede gekommen, nachdem bei einer Durchsuchungsaktion des ehemaligen sächsischen Wirtschaftsministers Kajo Schommer (CDU) der Pressefotograf Ronny Klein noch vor den Ermittlern erschienen war und der Verdacht aufkam, Klein sei von den INES-Ermittlern informiert worden. Bei der Staatsanwaltschaft Chemnitz wurde daher ein Verfahren gegen den Dresdner Staatsanwalt Andreas Ball eröffnet, der die Ermittlungen gegen Schommer leitete. Ball hatte den ehemaligen Wirtschaftsminister verdächtigt, Gelder aus einem Vertrag mit der Abfallorganisation Grüner Punkt bekommen zu haben, ohne je eine Gegenleistung dafür zu erbringen. Mitte August 2005 wurde Ball aus »Fürsorgepflicht« gegenüber ihm selbst versetzt. Die Überprüfung der Telefonkontakte des Journalisten Klein haben gegen Ball kein Belastungsmaterial erbracht.

Kritisch wird nun vor allem die Aktion der Chemnitzer Justiz gesehen. Hubert Engeroff, Hauptgeschäftsführer des Deutschen Journalistenverbandes, meint: »Da wurde mit Kanonen auf Spatzen geschossen«. Schommers Parteifreund und sächsischer Justizminister, Geert Mackenroth, sieht zwar, dass die Pressefreiheit tangiert wurde, sie sei aber nicht verletzt. Und der Chemnitzer Oberstaatsanwalt Siegfried Rümmler sagte: »Es ist nie gewollt oder beabsichtigt gewesen, hier einen Journalisten auszubaldowern. Ein Maulwurf in einer Behörde muss gefunden werden.« Der Journalistenverband erwägt in dem konkreten Fall einen erneuten Gang zum Bundesverfassungsgericht nach Karlsruhe, wo eine Klage in einem ähnlich gelagerten Fall schon einmal zurückgewiesen worden ist (vgl. DANA 2/2003, 34 f.; Kohl, SZ 31.08.2005, 15 u. 07.09.2005, 6; Stark/Wassermann/Winter, Der Spiegel 38/2005, 181).

Ausländische Datenschutznachrichten

Welt

27. Internationale Datenschutzkonferenz zu universellem Datenschutz in Montreux

Auf der 27. Internationalen Konferenz der Datenschutzbeauftragten am 14.-16.09.2005 in Montreux/Schweiz am Genfer See wurde einstimmig eine »Montreux-Erklärung« verabschiedet, die feststellt, dass Datenschutz ein Menschenrecht sei, das als solches auch kodifiziert werden müsse. Der aktuelle geopolitische Kontext z.B. mit dem globalen Kampf gegen den Terrorismus, das Internet, die Biometrie, die Entwicklung von invasiven Technologien oder die Entstehung von Biobanken machten deutlich, so die Abschlusserklärung, dass das Recht auf Privatsphäre ein unantastbares Element einer modernen demokratischen Gesellschaft sei.

Die Montreux-Erklärung richtet ihre Forderung, global deutlich mehr für den Datenschutz zu tun, an die UNO, an den Europarat, die beim Weltgipfel der Informationsgesellschaften versammelten Regierungen sowie supranationale Organisationen wie die EU. Die IT-Branche wird aufgefordert, datenschutzfreundliche Produkte und Dienstleistungen anzubieten.

Verabschiedet wurden noch zwei weitere Erklärungen. Die eine fordert Datenschutzgarantien zur Begrenzung der Risiken von biometrischen Verfahren v.a. bei Ausweisen. Die Konferenz fordert eine strikte Trennung von biometrischen Verfahren, die öffentlichen Zwecken dienen, und solchen privaten, die auf Grund von Einwilligungen und Vertragsverhältnissen angewendet werden. Biometrische Daten in Pässen müssten auf die Identifizierung beim Grenzübertritt beschränkt werden. Auf ein Verbot von zentralen Datenbanken mit biometrischen Daten aller Bürgerinnen und Bürger konnte man sich nicht verständigen. Eine vom italienischen Datenschutzbeauftragten initiierte Resolution will die Bürger davor schützen, dass sie in ihrem Wahlverhalten

beobachtet und zum Gegenstand von politischen Profilen gemacht werden. Zunehmend würden politische Organisationen Personendaten sammeln und diese »in aggressiver Art und Weise« verwenden. Politische Werbung sei Werbung. Politische Werber müssten sich an die geltenden Regeln halten: Datensparsamkeit, Sicherstellung der Richtigkeit, Verhältnismäßigkeit und Zweckbindung. Es sei zu gewährleisten, dass die Einwilligung der Betroffenen eingeholt wird und der Auskunftsanspruch durchgesetzt werden kann. Verletzungen dieser Prinzipien sollten sanktioniert werden. Die Texte der Entschließungen sind im Internet abrufbar auf der Webseite des Eidgenössischen Datenschutzbeauftragten unter http://www.edsb.ch/d/aktuell/index.htm (Ermert, www.heise.de 16.09.2005; Ermert, c′t 21/2005, 56).

Welt

Generalversammlung von Interpol

Am 21.09.2005 fand in Berlin die Generalversammlung der Internationalen Kriminalpolizeilichen Organisation (IKPO-Interpol) statt. Zentrales Thema war die weltweite Bekämpfung des Terrorismus. Dazu meinte Interpol-Präsident Jackie Selibi aus Südafrika: »Die Polizei bekämpft den Terror besser als das Militär. Das Militär geht nach dem Motto vor: Du schießt, ich schieße. Die Polizei identifiziert den Täter, stellt seinen Aufenthalt fest und verhaftet ihn dann. So kann man Terror auch verhindern und das ist es, was getan werden muss.«

Interpol will die von der UNO verdächtigten Taliban- und Al-Qaida-Anhänger in einem eigenen weltweiten Fahndungssystem ausschreiben. Davon berichtete der frühere Chef des deutschen Bundeskriminalamtes (BKA), Ulrich Kersten, der nun Interpol-Verbindungsmann in New York ist. Dadurch erübrige sich die aufwändige Internet-Recherche nach der UN-Verdächtigenliste, auf der 328 Personen und 119 Organisationen aufgeführt sind. Nach dem Willen der UNO sollen deren Vermögen eingefroren und deren Bewegungsfreiheit eingeschränkt werden.

Der deutsche Innenminister Otto Schily sprach sich dafür aus, die Datenbestände von Interpol in Lyon/Frankreich und der Europäischen Polizeibehörde Europol in Den Haag/Holland, wo es geht, zusammenzuführen: »Wir müssen die Zusammenarbeit von Interpol und Europol noch ein wenig verbessern.« Interpol-Chef Ronald Noble und der deutsche Europol-Chef Peter Ratzel stehen darüber in Verhandlungen. Daten von gestohlenen Fahrzeugen, Kunstgegenständen oder Vermissten könnten gleich bei Interpol eingestellt werden. So könne Doppelarbeit vermieden werden.

In den Dateien von Interpol befinden sich 7,8 Millionen Datensätze über gestohlene Pässe und Millionen über entwendete Kraftfahrzeuge und Kunstgegenstände. Es gibt eine Fingerabdruckdatei und eine Datei über Kinderpornografie. Die Generalversammlung beschloss, eine weltweite Datei von Vermissten und Toten einzuführen – als direkte Konsequenz aus den Erfahrungen mit der Tsunami-Katastrophe, wo jedes Land zunächst auf eigene Faust daran arbeitete, die Toten zu identifizieren. Ein entsprechender Antrag des gastgebenden Deutschland wurde mit großer Mehrheit angenommen. Nach Mitteilung von BKA-Präsident Jörg Zierke müssten v.a. gemeinsame Formate bei der Suche nach Vermissten entwickelt werden. In Deutschland erfolge eine Spezifikation für die Suche an Hand von 800 bis 900 Einzelmerkmalen (Ramelsberger SZ 22.09.2005, 5).

International

World-Compliance bietet weltweite Warndatei an

Dirk Mohrmann ist einer von drei Geschäftsführern des im Jahr 2001 gegründeten Unternehmens World-Compliance mit Sitz in Miami/USA. Die Firma mit 50 Mitarbeitern und Partnerfirmen in acht Ländern bietet eine Datenbank als »Schutzschild gegen unerwünschte Geschäftsbeziehungen« an. Die derzeit weltweit 600.000 Datensätze enthaltende Datenbank soll Personen und Unternehmen identifizieren, die im Zusammenhang mit Geldwäsche, Korruption und Terrorismus stehen. Monatlich werden ca. 30.000 weitere »Kriminelle« hinzugespeichert. Mit dabei ist z.B. der frühere Staatssekretär Ludwig Holger Pfahls, der in Augsburg wegen Vorteilsannahme und Steuerhinterziehung vor Gericht stand. Banken und sonstige Unternehmen können ihre bestehende Kundendatei mit den verfügbaren Daten über zweifelhafte Personen abgleichen. Sie können Verdächtige auch in dringenden Fällen schnell herausfiltern. Mohrmann erhofft sich von einer neuen EU-Richtlinie gegen Geldwäsche neuen Schwung für seine Geschäftsidee. Die Richtlinie muss noch in nationales Recht umgesetzt werden. Sie verpflichtet Banken, einen risikoorientierten Ansatz nicht nur bei Krediten, sondern allgemein bei Kunden einzuführen. Die Datenbank soll dabei helfen, »riskante Kunden« zu erkennen. Zu den Abnehmern von World-Compliance gehören neben Banken Fondsanbieter und Anwaltskanzleien. Umsatz und Ergebnis des Geschäftes sind bisher nicht bekannt. Der Preis der Ware soll vom Umfang des Datenpakets abhängen; es gehe schon unterhalb von 10.000 Euro los (Einecke, SZ 23.08.2005, 22; siehe auch die äußerst instruktive Buchbesprechung zu Robert o′Harrow, No Place to Hide, und zu Daniel Solove, the digital person, bei Grötker, www.heise.de 25.09.2005).

Europa

Datenschutz für den Datenaustausch für Justiz und Polizei

Die EU-Kommission hat am 04.10.2005 einen Vorschlag vorgelegt, mit dem der Datenschutz bei der Aufklärung von Verbrechen durch Polizei und Justiz verbessert werden soll. Justizkommissar Franco Frattini begründete die Initiative damit, dass der Schutz personenbezogener Daten Hand in Hand mit der Bekämpfung von Terrorismus und organisierter Kriminalität einher gehen müsse. Der Vorschlag, dem die Mitgliedstaaten noch zustimmen müssten, soll den Datenaustausch zwischen EU-Staaten erleichtern und auch die Weitergabe von Daten an Staaten außerhalb der EU regeln. Das Papier sieht keine zeitlichen Begrenzungen vor. Im Dialog mit den Datenschutzbehörden habe sich herausgestellt, dass feste Fristen nicht praktikabel seien – so Frattini. Festgelegt ist, dass Personendaten nicht länger aufbewahrt werden, als dies für den Zweck, zu dem sie erhoben wurden, notwendig ist.

Frattini betonte, dass die Zusammenarbeit über Grenzen hinweg zum

Schutz der Bürger unerlässlich sei: »Gleichzeitig müssen sie aber auch vor dem Missbrauch ihrer Daten geschützt werden, wenn wir nicht den Terroristen in die Hände spielen wollen.« Zum Schutz der Privatsphäre sollen die Mitgliedstaaten in Zukunft daher die Sammlung personenbezogener Daten grundsätzlich verbieten. Dies gelte insbesondere für Angaben über rassische oder ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Mitgliedschaft in Gewerkschaften sowie zu Gesundheit und Sexualleben. Ausnahmen könnten nur zur Abwehr einer ernsthaften Gefahr für die öffentliche Sicherheit oder für Personen gelten. Nationale Datenschutzbehörden sollen die Einhaltung der Bestimmungen überwachen.

Der Vorschlag ergänzt die europäische Datenschutzrichtlinie von 1995. Diese regele nicht den Datenschutz beim Austausch zwischen den Mitgliedstaaten zu Zwecken der Strafverfolgung. Gemäß dem neuen Vorschlag könnten die EU-Staaten z.B. Angaben aus dem Schengen-Informationssystem zur Fahndung nutzen. Ob die Regierungen dem Rahmenbeschluss zustimmen, ist für Frattini unklar. Der Kommissar sieht aber keine Alternative: »Wir müssen das Risiko einer Ablehnung eingehen.« Strategisch scheint die Initiative auch das Ziel zu verfolgen, die starke Kritik an den europäischen Plänen zur Vorratsdatenspeicherung von Telekommunikationsdaten zu dämpfen (SZ 05.10.2005, 8; dpa 04.10.2005).

Frankreich

Elektronisch-biometrischer Pass auch in Frankreich

Neben Deutschland (s.o. S. 19ff.) führte auch Frankreich vom 01.11.2005 an Reisepässe mit Chip ein. Die ersten Exemplare wurden in Paris ausgegeben. Im Chip ist ein digitales Foto gespeichert. Derweil begann in den USA eine Testphase, bei der Diplomaten einen Pass mit biometrischen Merkmalen erhalten. Von Oktober 2006 soll die Einführung solcher Pässe notwendig sein, um in die USA visumfrei für bis zu 90 Tage einreisen zu können. Diese Möglichkeit besteht für BürgerInnen von 27 Ländern, darunter 15 EU-Staaten (SZ 26.10.2005, 10).

Großbritannien

Bahngepäck wird geröntgt

In Großbritannien sollen an Bahnhöfen Sicherheitskontrollen eingeführt werden, wie sie an Flughäfen üblich sind. Verkehrsminister Alistair Darling hat gemäß Presseberichten nach den Terroranschlägen vom 07.07.2005 in London Sicherheitsmaßnahmen entwickelt. Vorgesehen ist u.a., dass Fahrgäste durch Sicherheitsschleusen passieren müssen, während ihr Gepäck geröntgt wird. Zunächst soll an verschiedenen Bahnhöfen ausprobiert werden, wie sich die Maßnahmen auch im Berufsverkehr anwenden lassen. Ein Sprecher des Bahnverbands bemängelte, die Kontrollen seien »einfach nicht praktisch«: »Die Frage ist außerdem, wer das alles zahlt.« Sicherheit sei zwar ein großes Anliegen, die Maßnahmen dafür müssten allerdings auch durchführbar sein (SZ 31.10./01.11.2005, 7).

Großbritannien

Bei Passfotos Lächeln verboten

Das britische Innenministerium erklärte, dass die neuen biometrischen Lesegeräte beim Einscannen von Gesichtsbildern am besten funktionieren, wenn die Person auf dem Foto einen neutralen Ausdruck zeige und den Mund geschlossen halte. Daher dürfen BritInnen auf ihren Passfotos künftig nicht mehr lächeln. Die Regelungen für die neuen Pässe gelten seit dem 12.09.2005. Mit diesen Vorschriften werden die britischen Pässe an die internationalen Standards angepasst, die angeblich ein Instrument zur Bekämpfung des Terrorismus sind (SZ 13.09.2005, 9; zu Deutschland s.o. S. 20f.).

Großbritannien

Autokennzeichen mit RFID

Nach Presseberichten testet das britische Verkehrsministerium (Department for Transport – DFT) den Einsatz aktiver RFID-Tags an Autokennzeichen (e-Plates) von Polizeifahrzeugen. Der Versuch soll zeigen, ob e-Plates schwerer zu duplizieren oder zu fälschen sind als herkömmliche Autokennzeichen. RFID-basierte Identifikationssysteme für Autos kommen in verschiedenen Ländern wie Frankreich oder USA schon zur Erhebung von Maut bzw. Autobahngebühren zum Einsatz. In den USA soll ein Projekt des Verkehrsministeriums in den Startlöchern stehen, welches die Beeinflussung von Autofahrern mittels e-Plates zum Ziel haben soll. Dabei sollen z.B. Wetter- oder Unfallwarnungen übertragen und Geschwindigkeitsüberschreitungen registriert werden (Omnicard-Newsletter September 2005; www.wired.com; www.rfidnews.org; www.dft.gov.uk; www.e-plate.com).

Großbritannien

Microsoft kritisiert Biometrie-Konzept

Microsoft hat vor einem bislang nicht gekannten Ausmaß an Identitätsdiebstahl im Zusammenhang mit dem geplanten Aufbau eines landesweiten Identitätsregisters in Großbritannien gewarnt. Jerry Fishenden, National Technology Officer (NTO) bei Microsoft in Großbritannien, skizzierte das Bild eines »Honigtopfes«, der wegen seiner Fülle an sensiblen Daten zu einem äußerst attraktiven Ziel für Kriminelle werden könnte. Anfang 2005 hatte das britische Unterhaus ein Gesetz gebilligt, das im Zuge der Einführung der Ausweispflicht u.a. die Einrichtung einer zentralen Datenbank vorsieht, in der ab 2008 biometrische Merkmale aller BürgerInnen zentral gespeichert werden sollen. Dazu Fishenden: »Kein IT-Experte würde jemals empfehlen, die Identitätsmerkmale einer ganzen Nation an einem einzigen Ort aufzubewahren. Bei falscher Planung und Umsetzung kann die Einrichtung eines solchen zentralen Registers sogar zu weniger statt zu mehr Sicherheit führen. Ein wesentliches Problem dabei ist, dass Computersysteme generell keinen 100prozentigen Schutz gegen Angriffe bieten.« Unbefugte hätten z.B. auf das PNC-System (Police National Computer) und auf die Datenbestände der DVLA (Driver and Vehicle Licensing Agency) zugreifen können, obwohl diese Systeme besonders gut geschützt gewesen seien. Bei Biometrie komme erschwerend hinzu, dass man im Fall eines Missbrauchs der Daten den Betroffenen nicht einfach neue Merkmale zuteilen könne.

Lege man die von Kim Cameron postulierten Grundsätze für ein siche-

res Identitätsmanagement an, zeige sich, dass beim britischen Biometrie-Konzept derzeit noch einiges im Argen liegt. Cameron ist bei Microsoft als Chefentwickler für den Bereich Identitätsdienste tätig. Er fordert eine minimale Offenlegung persönlicher Daten sowie die volle Dateneinsicht und -kontrolle durch den Bürger. Statt persönliche Daten zentral aufzubewahren, sollen gemäß Cameron diese so verteilt werden, dass staatliche Behörden nur auf die wirklich nötigen Daten Zugriff erhalten. So berechtigt sie ist, so mag die Kritik Fishendens nicht ganz uneigennützig sein. Microsoft will selbst gerne ein großes Stück vom boomenden Geschäft mit biometrischen Identifikations- und Verifizierungslösungen abhaben (www.heise.de 19.10.2005).

Niederlande

Zentrales Bürgerdossier ab Geburt

Für alle Neugeborenen soll ab 2007 in den Niederlanden ein »Elektronisch Kinddossier« in einer zentralen Datenbank angelegt werden, gab das niederländische Gesundheitsministerium bekannt. Gespeichert werden sollen Informationen zu Gesundheit und Bildungsweg, familiäre Verhältnisse und Vorstrafen.
Damit sollen Informationsflüsse zwischen den Behörden gefördert werden; außerdem könne der Staat so Probleme von Kindern frühzeitig erkennen und gegensteuern (heise online 19.09.2005).

Schweden

Anzeigen an die Polizei über Internet

In einem Modellversuch gibt die schwedische Polizei ihren BürgerInnen nun die Möglichkeit, per Internet eine Anzeige zu erstatten. Die Polizei will damit erreichen, dass die nationale Telefonnotrufnummer tatsächlich nur noch für echte Notfälle benutzt wird. Um Streitigkeiten, kleinere Diebstähle und verloren gegangene Gegenstände zu melden, sollen die BürgerInnen künftig auf das Web-Formular ausweichen. Wer das Internet für die Anzeige benutzt, erhält nach dem Absenden sofort eine Bestätigung für die Versicherung. Die Online-Anzeige ist der zweite Versuch der schwedischen Polizei, die Menschen davon abzubringen, für Kleinkram den Notruf 112 zu wählen. Eigens für Bagatelldelikte hat Schweden vor ein halbes Jahr zuvor eine andere Telefonnummer eingeführt. Das Ergebnis war nicht ganz wie erhofft: Zwar wird der Notruf nun tatsächlich weniger oft blockiert, dafür erhöhte sich aber die Zahl der angezeigten Kleindelikte gewaltig, um 30% höher als erwartet (Der Spiegel 36/2005, 95).

USA

US-Gasteltern werden mit Sexualtäterkartei gegengecheckt

Das US-Außenministerium sah sich angesichts einer zunehmenden Zahl von sexuellen Belästigungen bis hin zu Vergewaltigungen an ausländischen AustauschschülerInnen dazu veranlasst, verschärfte Regeln für den Schüleraustausch aufzustellen. Nach den neuen Regelungen müssen alle erwachsenen Mitglieder einer Gastfamilie anhand der Sexualstraftäter-Karteien der Bundesstaaten überprüft werden. Die Austauschorganisationen werden verpflichtet, jeden Vorwurf der sexuellen Belästigung den örtlichen Behörden und dem State Department zu melden. Stanley Colvin, Koordinator des Austauschprogramms im Außenministerium: »Wenn sie die Vorwürfe nicht melden, werden wir ihnen die Zulassung entziehen«.

Außenministerin Condoleezza Rice bezeichnete die Austauschprogramme, über die jährlich ca. 28.000 SchülerInnen an amerikanische High Schools vermittelt werden, als »extrem wichtig«. Damit könne das Image der USA im Rahmen einer internationalen Kampagne verbessert werden. Koordinator Colvin räumt ein, dass die neuen Regelungen das Problem nicht beseitigen werden. Sie seien aber ein zusätzlicher Schutz. Da bisher keine Meldepflicht bestand, existieren auch keine Statistiken über das Ausmaß des sexuellen Missbrauchs von AustauschschülerInnen. Bei den meisten Organisationen kann man sich online als Gastfamilie melden. Auf vielen Websites wird mit Bildern von fröhlichen jungen Menschen geworben, in aller Unschuld auch durch eine Organisation in New Jersey: Sie zeigt ein Foto junger Mädchen mit knappen Bikinis (Klüver, SZ 19.08.2005, 10).

Australien

Schärfere Gesetze gegen Terrorismus

Mit neuen Gesetzen will die konservative australische Regierung von Premierminister John Howard Terroristen abschrecken. Behörden soll es in Zukunft leichter gemacht werden, Verdächtige zu überwachen. Diese sollen bis zu 14 Tage lang festgehalten werden können. Wer einen Koffer unbeaufsichtigt am Bahnhof stehen lässt, macht sich künftig strafbar. Strafbar wird auch, wer zu Gewalt gegen Australien aufruft. Die Einwanderung wird erschwert. Anträge sollen »aus Sicherheitsgründen« abgelehnt werden können. Howard sagte, er habe sich an den neuen Gesetzen Großbritanniens orientiert. Der Premier präsentierte die Vorschläge der Öffentlichkeit, ohne dem Parlamentsausschuss der Konservativen die Einzelheiten zur Diskussion vorgelegt zu haben. Selbst konservative Parlamentarier zeigten sich nicht nur brüskiert, sondern kritisierten die Schärfe des Gesetzes. Seit den Anschlägen vom 11. September 2001 in den USA hat Australien seine Gesetze gegen den Terrorismus kontinuierlich verschärft. Dabei ist es dort noch nie zu Anschlägen gekommen. Australien ist aber Verbündeter der USA und beteiligt sich am Krieg im Irak und in Afghanistan (SZ 09.09.2005, 8).

Südkorea

Planungen für die total automatisierte Stadt

Auf einer künstlichen Aufschüttung vor der Küste Südkoreas wächst derzeit eine Stadt heran, deren BürgerInnen allzeit von wachsamen Computerchips umgeben sein sollen. In Häusern und Straßen – so die Planungen – steckt fürsorgliche Elektronik; drahtlose Funknetze »erleichtern« das Alltagsleben. Die futuristische Kommune mit dem Namen New Songdo ist der Idee von Politikern und Stadtplanern mit viel Geld entsprungen. 25 Mrd. Dollar sind für die Modellstadt eingeplant. Die BewohnerInnen sollen dafür eines Tages nach den Verheißungen der Planungsfirma mit ein und derselben Plastikkarte ihr Haus abschließen, die Parkuhr füttern, an der Kinokasse bezahlen oder

ein öffentliches Fahrrad ausborgen. Alles wird vernetzt, der Nachbar mit Videokonferenz erreichbar und das Internet drahtlos allgegenwärtig. In Songdo werden billige Funkchips schwirren mit RFID-Technik, mit denen sich Waren aller Art markieren lassen. Lesegeräte an öffentlichen Wertstoffeimern werden danach z.B. registrieren, wer gerade vorschriftsmäßig eine leere Plastikflasche darin entsorgt – und automatisch das fällige Flaschenpfand gutschreiben. Der RFID-Funktechnik wird seit einiger Zeit das Potenzial zu einer Revolution des Warenverkehrs geweissagt. Im Westen steht dem noch datenschützerischer Argwohn entgegen. Davon wollen sich die südkoreanischen Planer aber nicht beirren lassen; sie rechnen mit einem rasant wachsenden Markt. In Songdo entsteht daher ein Forschungszentrum zur RFID-Technik, für das bereits fast 300 Mio. Dollar bereitgestellt wurden. Die Stadt, die bis 2014 fertig sein soll, ist für 65.000 EinwohnerInnen ausgelegt (Der Spiegel 42/2005, 204).

China

Yahoo verpfeift kritischen Journalisten

Das US-Internet-Portal Yahoo hat nach Angaben der Organisation Reporter ohne Grenzen (RSF – Reporteurs sans Frontiers) die chinesische Regierung mit Informationen versorgt, die zur Inhaftierung eines oppositionellen Journalisten führten. Die Hongkonger Filiale des Unternehmens habe der Staatssicherheit geholfen, den Journalisten Shi Tao zu identifizieren, der anschließend zu 10 Jahren Haft verurteilt wurde. RSF berief sich auf Gerichtsunterlagen, wonach der 37jährige wegen des »Verrats von Staatsgeheimnissen« verurteilt worden war, weil er eine interne Anordnung der Kommunistischen Partei an ein »überseeisches feindliches Element« weitergeleitet hatte. Die Anordnung hatte jedes Gedenken zum 15. Jahrestag des Tiananmen-Massakers von 1989 verboten. Das Schreiben von Shi enthielt nicht viel mehr als eine allgemeine Warnung vor der Rückkehr bestimmter Dissidenten. Allein das Wort »Dissident« dürfte in den Filterprogrammen der chinesischen Staatssicherheit hängen geblieben sein und einen der 40.000 Internet-Zensoren im Land auf die Spur gebracht haben. Der Journalist war aber in der Lage, seine Mails zu anonymisieren. Daher baten die chinesischen Staatsschützer Yahoo Hongkong um Hilfe. Yahoo ließ sich offenbar nicht lange bitten und lieferte genau die Informationen, die zur Verhaftung Shi Taos führten. Das Urteil des chinesischen Volksgerichtes vom April 2005 bezieht sich ausdrücklich auf die von Yahoo gelieferten Informationen – den persönlichen Account und die sekundengenaue Sendezeit der Email. Nach einigen kritischen Zeitungsberichten rechtfertigte die Sprecherin der amerikanischen Firma, Mary Osako, die jeweiligen Yahoo-Niederlassungen müssten im Rahmen der jeweiligen Gesetze und »Gebräuche« arbeiten. Natürlich würde die firmeneigene »privacy policy« berücksichtigt. Doch die hindert nicht die schon im Jahr 2002 von Yahoo freiwillig unterzeichnete »Verpflichtung zur Selbstdisziplin für die chinesische Internet-Industrie«. Dabei erklären sich die Firmen zur Teilnahme bei der Zensur bereit, z.B. durch Sperrung von Begriffen wie »Demokratie« oder »Menschenrechte« in Suchmaschinen. Den Internet-Firmen Google, Microsoft MSN und Yahoo wird vorgeworfen, sich aus Geschäftsinteresse dem chinesischen Druck zu beugen und sensible Informationen in Suchmaschinen und Internetseiten zu unterbinden. Die drei Portale kämpfen um einen wachsenden Markt in China, das zum zweitgrößten Internet-Nutzer weltweit nach den USA aufgerückt ist. Die Kooperation von Yahoo geht aber mit seinem Dienst als »Polizeispitzel« – so Reporter ohne Grenzen – einen Schritt weiter. Yahoo hatte sich gerade für eine Milliarde Dollar 40% der größten chinesischen E-Commerce-Firma Alibaba.com gesichert. Auch Cisco hat seine Firewalls und Router dem Zensurbedarf der Regierung angepasst (SZ 08.09.2005, 9; Klawitter, Der Spiegel 38/2005, 182).

Technik

Punktmarkierungen identifizieren Farblaser-Drucker

Der US-amerikanischen Bürgerrechtsorganisation Electronic Frontier Foundation (EFF) ist es nach eigenen Angaben gelungen, auf Ausdrucken eines Farblaserdrucker-Modells hinterlassene winzige gelbe Punkte zu entschlüsseln. Ein Forschungsteam habe herausgefunden, aus den Punkten sei Datum und Uhrzeit sowie die Seriennummer des Druckers ablesbar. Druckerhersteller würden diese Codes auf Veranlassung des US-amerikanischen Secret Service anbringen, um den Ursprung von Fälschungen ermitteln zu können.

Die EFF hatte im Juli 2005 dazu aufgerufen, Ausdrucke vom eigenen Farblaserdrucker einzuschicken, damit sie diese dokumentieren und erforschen können. Bei der Untersuchung von Ausdrucken aus Xerox-DocuColor-Druckern wurde ein Schlüssel gefunden, um die Punktmarkierungen zu interpretieren. Auf der Dokumentationsseite der EFF können Besitzer eines DocuColor-Druckers die Entschlüsselung des Codes nachvollziehen. Die Forschenden gehen davon aus, dass sich auch die Schlüssel für andere Druckermodelle finden werden und bitten weiterhin um die Einsendung von Testausdrucken. Die EFF kritisiert, mit den Absprachen zwischen Herstellern und Geheimdiensten würde das Recht auf freie Rede untergraben. Menschenrechtler könnten in Gefahr geraten, wenn sie anonyme Flugblätter drucken wollen und über das geheime Muster identifiziert werden könnten (Der Spiegel 43/2005, 96; www.heise.de 17.10.2005; vgl. http://www.eff.org/Privacy/printers/docucolor/index.php# program).

RFID-Antennen in der Folie

Professor Alfred Ebberg und seine Mitarbeiter von der Fachhochschule Westküste in Heide/Schleswig-Holstein haben eine Antenne für die RFID-Technologie entwickelt, die direkt bei der Herstellung in die Verpackung integriert werden kann. Auftraggeber hierfür ist Silicon Manufacturing Itzehoe (SMI),

deren Leiter von Marketing und Logistic, Georg Mendes, den Zweck erläutert: »Wir wollen die Wertschöpfungskette verkürzen und damit die Kosten reduzieren.« Funkchips und Antennen können so z.B. in die Aluminiumfolie von Zigaretten- oder Medikamentenschachteln integriert werden. Je nach Material und verwendetem Produkt muss die Antenne modifiziert werden. Die Forschungs- und Entwicklungsarbeiten, die der Bund mit 2,5 Mio. Euro fördert, stehen noch am Anfang. Das Projekt, an dem auch der internationale Verpackungshersteller Alcan Packaging und Philips Semiconductor beteiligt sind, läuft bis 2008. Danach sollen umgehend Produkte mit dieser Technologie auf den Markt kommen (Schmid, Eckernförder Ztg. 11.10.2005, 9).

Geburtsjahrbestimmung durch Zahnschmelzanalyse

Schwedische Biologen haben ein Verfahren entwickelt, um das Geburtsjahr von Menschen, z.B. von Verbrechensopfern, zu errechnen. Dabei wird der Gehalt des Kohlenstoff-Isotops 14C im Zahnschmelz gemessen. Dieses verbreitete sich nach Atomtests in den Jahren 1955 bis 1963 weltweit in der Atmosphäre. Der Zahnschmelz speichert es, wenn er sich im zwölften Lebensjahr bildet. Da sich 14C in der Atmosphäre langsam abbaut, lässt sich durch den Vergleich das Alter auf 1,6 Jahre genau ermitteln (Focus 38/2005, 104).

Große Sicherheitslücken bei Email-Handy Blackberry?

Blackberry ist ein bei Managern beliebter kleiner Taschencomputer, der automatisch alle eingehenden Emails anzeigt. Nach einer internen Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) scheint die Email-Maschine schwere Sicherheitslücken zu haben: »Auf Grund der unsicheren Architektur ist der Blackberry für den Einsatz in sicherheitsempfindlichen Bereichen der öffentlichen Verwaltung und spionagegefährdeten Unternehmen nicht geeignet.« Der Grund: Wenn ein Blackberry-Kunde eine neue Email erhält, werden die Daten zunächst von seinem Computer an einen von weltweit nur drei Blackberry-Rechnern weitergeleitet. Dort werden die Emails an die Mobilfunkbetreiber in den einzelnen Unternehmen verteilt, die sie schließlich auf dem Display der Endgeräte anzeigen. Das BSI beunruhigt insbesondere, dass Blackberrys gesamter europäischer Email-Verkehr »zwangsweise« über ein Rechenzentrum in der Nähe von London läuft: Nach britischem Recht könnten sich die örtlichen Sicherheitsbehörden unter sehr weit gefassten Voraussetzungen Zugang zu den Inhalten der Emails verschaffen, evtl. »zum Wohle der britischen Wirtschaft«.

Die kanadische Firma Research in Motion (RIM), die den Blackberry-Service betreibt, bestreitet derartige Gefahren vehement. In den Rechenzentren würden die Daten lediglich an die Empfänger weitergeleitet, keinesfalls aber gespeichert. Der gesamte Email-Verkehr sei verschlüsselt mit Codewörtern, die nur der jeweilige Kunde kennt. Einen »Master-Key« gebe es nicht. Sicherheitsexperten sehen dagegen schon in der Beschränkung auf weltweit nur drei Rechenzentren eine mögliche Bedrohung. Geheimdienste hätten, wenn sie die Daten der Blackberry-Nutzenden anzapfen wollten, relativ leichtes Spiel. Deutlich schwieriger würde sich das Abhören gestalten, wenn die Email-Server direkt in den Firmen stünden oder über viele Nationalen verteilt wären (Stirn, SZ 07.10.2005, 11).

Gentechnik

Rechtsmediziner für Gentest bei allen Neugeborenen

Der Direktor des Hamburger Instituts für Rechtsmedizin, Klaus Püschel, forderte zum Auftakt einer internationalen Fachtagung am 19.09.2005 in Hamburg einen verstärkten Einsatz des genetischen Fingerabdrucks: »Schon bei der Geburt sollte von jedem der genetische Code genommen und gespeichert werden« (Kieler Nachrichten 20.09.2005, 12).

Pränataldiagnostik aus dem Blut

Ein Bluttest bei der Mutter kann voraussichtlich künftig die riskante Fruchtwasseruntersuchung zur Diagnose von Gendefekten oder Chromosomenveränderungen ungeborener Kinder ersetzen. Wissenschaftler aus Hongkong, den USA und den Niederlanden berichten in dem Fachblatt »Proceedings of the National Academy of Science«, dass über die Plazenta während der Schwangerschaft kindliche Erbsubstanz in den mütterlichen Blutkreislauf gelangt. Diese war bislang von der der Mutter kaum zu unterscheiden, allenfalls bei Jungen mit dem männlichen Geschlechtschromosom.

Forschenden um Stephen Chim von der Chinesischen Universität Hongkong fiel jetzt auf, dass in einem bestimmten DNA-Bereich die mütterliche Erbsubstanz weit mehr so genannte Methylgruppen aufweist als der Fötus. Damit wurde erstmals ein universeller Marker für fötale DNA im Plasma der Mutter gefunden. Auf der Grundlage dieses Unterschieds wollen Chim und sein Team nun Tests für den klinischen Einsatz entwickeln (Der Spiegel 41/2005, 184).

Täter legen immer öfter falsche DNA-Spuren

Kriminelle hinterlassen immer öfter falsche Spuren, indem sie eingesammelte Zigarettenkippen am Tatort hinterlassen. Sie bezögen weitere Hinweise über die Spurenvermeidung aus Fernsehserien über die polizeiliche Untersuchungs- und Analysemethoden bei der Verbrechensaufklärung.

Das ergab eine Studie der Universität Leicester. Allerdings würden viele kriminaltechnische Wissenschaftler mittlerweile sehr zurückhaltend im Umgang mit den Medien (AFP, yahoo 07.09.2005)

Rechtsprechung

BVerwG

Schreibtest bei Einbürgerung unzulässig

Ausländer können auch ohne umfassende Schriftkenntnisse der deutschen Sprache eingebürgert werden. Nach einem Urteil des Bundesverwaltungsgerichts (BVerwG) vom 20.10.2005 genügt es, wenn sich ein Ausländer im familiären und geschäftlichen Umfeld sowie im Umgang mit Behörden verständlich machen kann, d.h. wenn er einen Text deutsch diktieren und auf seine Richtigkeit hin überprüfen kann. Entscheidend sei, dass er den Text als seinen eigenen anerkenne. Lesekenntnisse der deutschen Sprache seien jedoch auf jeden Fall Voraussetzung für eine Einbürgerung. In einigen Ländern, z.B. Bayern und Baden-Württemberg, wurden bisher von den Einbürgerungswilligen schriftliche Sprachtests abverlangt.

Geklagt hatten zwei türkischstämmige Ausländer, denen vom Verwaltungsgerichtshof (VGH) Mannheim wegen fehlender Deutschkenntnisse der deutsche Pass verweigert wurde. Strittig war der Passus des Staatsangehörigkeitsgesetzes, in dem »ausreichende Kenntnisse der deutschen Sprache« verlangt werden. Die Leipziger Richter gaben damit einem 42jährigen Türken Recht, der seit 27 Jahren in Stuttgart lebt und gut deutsch sprechen kann. Zwei Sprachtests hatte er jedoch im schriftlichen Teil nicht bestanden. Der zweite Kläger blieb jedoch erfolglos. Der Mann lebt seit 20 Jahren in Rheinland-Pfalz und kann gut deutsch sprechen; doch ist er Analphabet und kann die Sprache nicht lesen.

Das BVerwG widersprach damit zugleich einer Entscheidung des hessischen VGH in Kassel, der 2002 in einem ähnlichen Fall ebenfalls schriftliche Deutschkenntnisse für eine Einbürgerung verlangt hatte. Die Sprachtests zur Einbürgerung werden seit In-Kraft-Treten des Staatsangehörigkeitsgesetzes Anfang 2000 je nach Bundesland unterschiedlich gehandhabt. In Ländern, in denen die SPD an der Regierung beteiligt ist, müssen die Antragsteller i.d.R. nur einen Hör- und Sprechtest bestehen. In Bayern war bisher der so genannten Postkartentest beliebt. Die Antragsteller müssen aus einer fiktiven Urlaubssituation heraus eine kurze Nachricht nach Hause verfassen. Dies war für viele Teilnehmenden die höchste Hürde im Test, was zu erheblich höheren Durchfallquoten führte als in nördlichen Bundesländern (U.v. 20.10.2005, Az. 5 C 8.05; 5 C 17.05; Preuß, SZ 21.10.2005, 1, 5).

LG München I

Durchsuchung bei Siemens-Betriebsrat rechtswidrig

Das Landgericht (LG) München I hat die Durchsuchung von Dateien des Betriebsratsvorsitzenden eines Siemenswerkes für rechtswidrig erklärt. Wegen der Strafanzeige eines damaligen Mitglieds der Betriebsleitung der Niederlassung München-Hoffmannstraße hatte die Staatsanwaltschaft beim Amtsgericht einen Durchsuchungsbeschluss erwirkt. Die Umsetzung übernahm der Sicherheitsdienst von Siemens, der die Dateien entschlüsselte und einen umfangreichen Auswertungsbericht verfasste – als »Hilfssheriffs« der Staatsanwaltschaft, wie sich der Anwalt des Betriebsrates Jürgen Fischer erboste.

Das LG stellte Anfang November 2005 die Unverhältnismäßigkeit des Durchsuchungsbeschlusses fest, weil er sich auf eine zu große und nur vage umrissene Datenmenge bezogen habe. Zudem »durfte nicht die Auswahl und die Durchsicht der Dateien der Firma Siemens respektive dem der Firma Siemens zugehörigen Sicherheitsdienst überlassen werden.« Dies wäre Sache der Staatsanwaltschaft gewesen. Das Gericht teilte die »Auffassung des Beschwerdeführers«, dass es zu einem »eklatanten Eingriff in das Grundrecht auf informationelle Selbstbestimmung und zu einem Eingriff in die von der Verfassung geschützten Rechte als Betriebsrat gekommen sei.

Der Betriebsrat hatte zuvor mit dem Gang vor das Bundesverfassungsgericht gedroht. Zunächst hatten die Richter des LG die Beschwerde ablehnt. Der bayerische IG-Metall-Chef Werner Neugebauer: »Es ist gut, dass dieses Stück aus dem Tollhaus nun für illegal erklärt wurde.« Die Gewerkschaft überlege, wie sie künftig Betriebsräte vor einer Ausspähung schützen könne. Siemens selbst wollte sich nicht zur Sache äußern. Der Konzern sei »nicht Beteiligter des Beschwerdeverfahrens«. Dies sei ein Vorgang zwischen dem Betriebsratsanwalt und dem Amtsgericht sowie dem Landgericht (Viering SZ 05./06.11.2005, 6; s.o. S. 25).

LG Kaiserslautern

Netzbetreiber muss TKÜ-Anordnung dulden

Gemäß einem am 01.08.2005 bekannt gewordenen Beschluss des Landgerichts (LG) Kaiserslautern kann sich ein Netzbetreiber grundsätzlich nicht gegen die Anordnung einer Telefonüberwachung bei einem seiner Kunden gerichtlich zur Wehr setzen. Mit der Überwachungsanordnung werde allein in die Rechte der jeweiligen Gesprächspartner, nicht aber ohne weiteres auch in die des Netzbetreibers eingegriffen. Eine Ausnahme gelte nur, soweit der Netzbetreiber besondere technische Voraussetzungen schaffen müsste.

Das LG verwarf mit seinem Beschluss die Beschwerde einer Telefongesellschaft als unzulässig. Das Amtsgericht (AG) Kaiserslautern hatte sie angewiesen festzustellen, welcher ihrer Kunden einen bestimmten Telefonanschluss zu einem bestimmten Zeitpunkt angerufen hatte. Das Unternehmen kam dem zwar nach, legte aber zugleich wegen möglicher »Wiederholungsgefahr« Beschwerde ein, da es sich in seinem Recht der freien Berufsausübung beeinträchtigt sah. Das LG Kaiserslautern sah dagegen in dem bloßen Rückverfolgen der Telefonanrufe keine Rechtsbeeinträchtigung des Netzbetreibers (Az. 1 T 12/05; www.heise.de 02.08.2005).

Buchbesprechungen

Kongehl, Gerhard (Hrsg.)

Datenschutz-Management

wrs Verlag Planegg/München 2005 (Loseblatt mit CD), 148 Euro, ISBN 3-8092-1705-0

(tw) Mit diesem Loseblatt-Praxishandbuch ist der Begriff »Datenschutz-Management« als Titel in der Datenschutzliteratur angekommen. Gerhard Kongehl stellt mit den Ko-Autoren Sebastian Greß, Gerhard Weck, Hannes Federrath, Rüdiger Dierstein und Stefan Lerbs dar, wie in Unternehmen und Behörden Datenschutz professionell umgesetzt und gestaltet werden kann bzw. soll. Dabei erfolgt eine starke Fixierung auf den betrieblichen Datenschutzbeauftragten (bDSB), der bisher auch in fast allen Unternehmen nicht nur im Zentrum des Datenschutz-Managements steht, sondern sich dieses auf diesen beschränkt. Dass Datenschutzmanagement mehr sein kann und die Unternehmensleitung, die Organisation eines Betriebs sowie die Belegschaft voll integrieren kann mit Zielvereinbarungen, Audits, Gütesiegeln, einem datenschutzkonformen Workflow und Mediationsprozessen, das lässt sich in der Darstellung erahnen, ist aber nicht deren zentraler Ansatz. Damit erweist sich dieses Handbuch weniger als eine Handreichung für die Unternehmensleitung, sondern als Unterstützung für den betrieblichen/behördlichen Datenschutzbeauftragten (bDSB). Und hierfür ist dieses Werk sehr gut geeignet. Ideal verwendbar ist das Werk als Starthilfe für den bDSB, zur Ausbildung – autodidaktisch oder kursbegleitend – und zur Arbeitsunterstützung.

Bei Ausbildungsliteratur ist es sinnvoll, wenn wichtige Themen redundant bearbeitet werden. Dies ist hier der Fall, wenn – wie bei Ausbildungsmodulen – in unterschiedlichen Kapiteln der Arbeitsplatz des bDSB, die bDSB-Praxis, das Datenschutzrecht und die IT-Sicherheit dargestellt werden. Die Darstellung ist inhaltlich regelmäßig auf einem hohen Niveau. Nur selten finden sich inhaltliche Fehler, etwa wenn die Speicherung einer Mietminderung in einer Warndatei für zulässig erklärt wird, wenn nur der Grund der Zahlungsverweigerung bei dieser Speicherung erkennbar ist. Die systematische rechtliche Darstellung – mit vielen Beispielen – ist äußerst erfreulich; bei der IT-Sicherheit wäre weniger Allgemeines und mehr Konkretes für die Zukunft wünschenswert. Das Werk richtet sich aber – offenbar gezielt – weniger an den Experten, der zu einer konkreten Frage eine Lösung nachschlagen will, sondern zunächst – manchmal etwas wortreich – an denjenigen, der an die Aufgabe des bDSB herangeführt werden soll. Dabei verwirrt das Werk nicht durch die Darstellung von kontroversen Positionen und durch Abdruck von vielen Fundstellen, sondern gibt eine klare Linie vor. Diese ist durchgängig datenschutzfreundlich und ausgerichtet am so genannten »Ulmer Modell«. Dabei wahrt das Werk aber dennoch eine gewisse Pluralität. Die Stärke der Darstellung wird aber dann zur Schwäche, wenn kritische Fragen – z.B. von der Unternehmensleitung – gestellt werden. Dann wäre manche weiterführende Literatur oder manche Auseinandersetzung mit anderen Positionen förderlich.

Äußerst erfreulich ist, dass das Werk durchgängig einem »positiven Datenschutz« verpflichtet ist, der sich am effektiven Grundrechtsschutz orientiert und nicht am Abarbeiten bürokratischer Anforderungen. Ein nur scheinbarer Widerspruch hierzu besteht darin, dass dann doch viele Hilfen durch Schemata, Checklisten, Vordrucke, Power-Point-Folien zur Mitarbeiterschulung und Verfahrensratschläge gegeben werden; ist doch das Bewältigen eines bürokratischen Minimums die Voraussetzung, um für die inhaltliche Arbeit den Rücken frei zu haben. Hilfreich sind auch ein Datenschutzlexikon, das noch ein wenig beliebig ausgewählte Stichworte erläutert, und auf CD-ROM wichtige Arbeitshilfen. Abschließendes Votum: als Startset für den bDSB sehr zu empfehlen; ja man kann sagen, dass das Werk das nötige Grundwissen eines bDSB vermittelt. Fatal wäre es, wenn der bDSB sich bei seiner weiteren Arbeit dann aber ausschließlich hierauf verlassen würde.

Coester, Ursula/Hein, Mathias

IT-Sicherheit für den Mittelstand

Datakontext Fachverlag Frechen 2005 393 S., 29 Euro, ISBN 8-89577-346-8

(tw) Die unbeschwerten Zeiten der Technikeuphorie in der Wirtschaft sind definitiv vorbei. Es ist nicht mehr nur die Rede von Chancen, sondern auch von Risiken, insbesondere im Hinblick auf die informationstechnische Sicherheit. Als neues Marktsegment der IT-Sicherheit wurde erst in allerjüngster Zeit der Mittelstand entdeckt: Während Großunternehmen ihre eigenen IT-Sicherheitsleute haben und der Kleinunternehmer ähnlich wie der private Nutzer mangels ausreichenden Finanzen auf Standardlösungen angewiesen ist, sind die mittelständischen Unternehmen ein äußerst interessanter Abnehmerkreis: Der Zwang zur Automation bzw. zur umfassenden Netznutzung ist hier gewaltig, die Kompetenz für IT-Sicherheit dagegen zu teuer.

Insofern stößt das Buch von Coester/Hein in eine Marktlücke. Es beschreibt ausführlich die technischen Risiken. Hierbei fallen alle aktuellen Stichworte – von Abhören über Cracker, Hacker, Session Hijacking, Social Engineering, Spam, Spoofing, Phising bis hin zur Wirtschaftsspionage. Beschrieben wird auch – regelmäßig verständlich und präzise – das technische Instrumentarium von Biometrie über Intranet, RFID, VoIP bis World Wide Web, um dann auch die Sicherheitslösungen darzustellen, sei es technischer Art – von der AES-Verschlüsselung über Firewall, Intrusion Detection, Virenscan bis zur Zugriffskontrolle – oder organisatorischer Art – vom Audit über Bedrohungsanalyse, Sicherheitsrichtlinien bis zum Zertifikat. In Sachen IT-Sicherheit gibt das Buch also einen guten Überblick, der auch für den Nichtfachmann verstanden werden kann.

Und dieser Adressatenkreis ist auch das Problem des Buches: Die IT-Verantwortlichen im mittelständischen Unternehmen sollen über die drohenden rechtlichen und finanziellen Gefahren und die Erkenntnis ihrer Verantwortung zu Maßnahmen veranlasst werden, ohne dass weiter gehende Hinweise hierfür gegeben werden. Statt eines differenzierten Angebots von Selbsthilfe-Tools, Verbund-Lösungsmöglichkeiten und eingekaufter externer Hilfe setzt das Buch fast ausschließlich darauf, dass sich die mittelständischen Unternehmen nicht nur Rat, sondern vor allem dauernde Hilfe von externen Experten einholen und sich damit in deren Abhängigkeit begeben. Dass auch dies ein Sicherheitsproblem sein kann, wird nicht thematisiert. Dies mag in den meisten Fällen der richtige Weg sein, der einzige Weg ist es sicher nicht. So sensibilisiert dieses Buch und gibt erste Hinweise für Organisation und Technik im eigenen Unternehmen, doch schweigt es bei der Benennung der hilfreichen Adressen, der nützlichen Instrumente und den etwas komplexeren intelligenten Lösungen. Es gibt zwar ein sehr gut nutzbares Stichwort-Verzeichnisse – doch fehlen die weiterführenden hilfreichen Fußnoten und alle die vielen anderen Verzeichnisse, die bei Handbüchern für Problemlagen oft so äußerst nützlich sind.

Eine kritische Anmerkung muss schließlich von einem Datenschützer kommen: Datensicherheit als Bestandteil des Datenschutzes wird von den Autoren als ein wichtiges Motiv für IT-Sicherheit benannt. Doch würde man sich als Datenschützer mehr wünschen als die Angst vor der Aufsichtsbehörde, vor Ausfallschäden, Haftungsfolgen oder Bußgeldern. Dass IT-Sicherheit auch etwas mit Vertrauen der Kunden und Vertragspartner oder gar mit dem Schutz der Privatsphäre zu tun haben kann, darauf kommt man bei der Lektüre des Buches nicht unbedingt. Auch dass der betriebliche Datenschutzbeauftragte eine wichtige IT-Sicherheitsfunktion haben könnte, wird nicht angesprochen. Hier – wie aber auch in anderen Rechtsbereichen – wird die Rechtslage zwar korrekt, aber viel zu allgemein beschrieben. Der sehr journalistische und auf die Technik abstellende Text lässt oft Komplexität und Tiefe vermissen. Dies gilt auch für die Beschreibung der rechtlichen Anforderungen, über die dann wohl ein externer Anwalt im Einzelfall aufklären soll. Dieses Defizit soll aber den Verdienst dieses Buches in dem Bereich, den es abdeckt, nicht in Abrede stellen: Es dient zur Sensibilisierung, zur Vermittlung der technischen Grundlagen und im Ergebnis auch zu einem in die richtige Richtung gehenden Sicherheitsbewusstsein und den notwendigen Sicherheitsmaßnahmen.

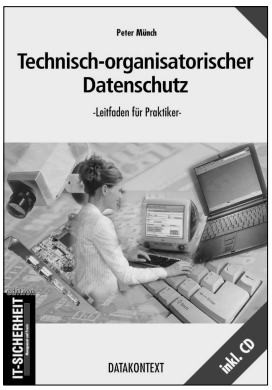
Wohlgemuth, Hans H./Gerloff, Jürgen

Datenschutzrecht – Eine Einführung mit praktischen Fällen

Luchterhand, 3. Aufl. München-Unterschleißheim 2005, 315 S., 22.80 Euro, ISBN 3-472-02652-9.

(tw) Es gibt eine Menge Literatur zum Datenschutz, es gibt aber bisher keine aktuelle, kurze, verständliche und inhaltliche präzise Einführung für interessierte Laien auf dem Markt. So durfte man auf die 3. Aufl. des Wohlgemuth hoffen, der mit seinem kleinen Büchlein zum Datenschutz im Jahr 1988 genau mit diesen Eigenschaften den Markt bereicherte. Die Hoffnung ist in großen Teilen vergebens. Die dritte Auflage, nun von Wohlgemuth/Gerloff, ist einem Anfänger nicht und einem Fortgeschrittenen nur bedingt zu empfehlen: Die Darstellung ist extrem juristisch geprägt und in langen Passagen selbst für manchen Juristen nicht zu genießen bzw. zu verstehen. Eine Leseprobe: »Datenschutzrecht als materielles Gesetz kann sich präsentieren, indem Datenschutz insgesamt die Regelungsmaterie bestimmt, wie dies beim Bundesdatenschutzgesetz oder dem Teledienstedatenschutzgesetz (TDSG) der Fall ist« (S. 8). Der systematische Aufbau des Buches folgt dem klassischen von Datenschutzkursen, aber mit verwirrenden Abwegen, etwa zum Stasi-Unterlagengesetz. Einen pädagogischen Nutzen könnten die den Kapiteln vorangestellten Fallbeispiele haben, die dann im Text erläutert und gelöst werden. Doch zeigen die Lösungen oft ein wenig vorbildliches Judiz, etwa wenn eine Wirtschaftsauskunft von einer Auskunftei für zulässig erklärt wird, mit der sich jemand auf einer Hauptversammlung gegen einen redeberechtigten Aktionär munitioniert. Manche Rechtsstreits in der Datenschutzliteratur werden zwar kontrovers dargestellt, ohne sie aber mit einer nachvollziehbaren Begründung zu entscheiden. Manche Position ist wenig durchdacht oder zumindest einfach so wie dargestellt nicht verständlich. Dies gilt z.B. für den Satz: »Die Erhebung von Daten im Geltungsbereich des § 30 wird in der Praxis nur aufgrund einer Einwilligung des Betroffenen erfolgen können« (S. 109). Andere Kapitel, z.B. das zum Arbeitnehmerdatenschutz, sind dagegen konsistent, gut verständlich geschrieben und instruktiv.

Zweifellos ist das Buch eine praktische erste Quellenlektüre. Es erfolgt eine umfangreiche Auswertung der Literatur, auf die verwiesen wird. Hier können auch manche weniger zugängliche Aufsätze, Entscheidungen oder Beiträge gefunden werden. Nützlich ist auch der Abdruck der EU-Datenschutzrichtlinie, des BDSG, des StUG sowie einiger Bundes-Sicherheitsgesetze, was insgesamt einen Raum von 150 Seiten einnimmt. Das Sachregister ist dagegen – anders als das Inhaltsverzeichnis – wenig hilfreich.



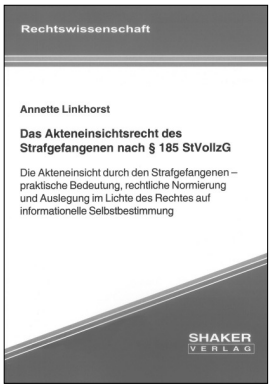
Münch, Peter

Technisch-organisatorischer Datenschutz – Leitfaden für Praktiker

Datakontext Verlag Frechen 2. Aufl. 2005, 426 S., 49 Euro, ISBN 3-89577-358-1

(tw) Es ist gerade etwas mehr als zwei Jahre her, dass die erste Auflage dieses Buches in der DANA lobend besprochen worden ist (DANA 2/2001, 31 f.). Dieses Lob kann uneingeschränkt auf die zweite Auflage erstreckt werden: Das Buch von Münch eignet sich ideal als Standard-Nachschlagewerk für den technisch interessierten Datenschützer, der nicht mit Juristerei und auch nicht mit Technikerkauderwelsch erschlagen werden will. Präzise und praxisorientiert sind die anschaulichen Abbildungen, Checklisten und praktischen Hinweisen vor allem für den betrieblichen Datenschutzbeauftragten. Ebenso hilfreich sind die aussagekräftigen Verzeichnisse über Inhalt, Stichworte, Begriffe, Abkürzungen und Literatur – nicht nur in gedruckter Form zwischen den zwei Umschlagdeckeln, sondern auch auf einer CD mit hilfreichen Checklisten, Mustern, Hinweisen, Formularen und Gesetzestexten.

Die aktuellen Probleme der Datensicherheit werden mit praktischen Beispielen erläutert sowie die Lösungen. Verschlüsselung, Signatur, Biometrie, Firewall, RFID, VPN, WLAN und vieles mehr werden verständlich und korrekt beschrieben. Sie werden zudem für den betrieblichen Datenschützer, den IT-Leiter oder auch den Unternehmensleiter handhabbar und bewertbar gemacht. Erfreulich ist der plurale Ansatz sowohl bei der Organisation wie bei der Technik: Der betriebliche Datenschutzbeauftragte kann es allein nicht richten, vielmehr sind im Rahmen eines Risikomanagements die Mitarbeiter, die Leitung, die IT-Spezialisten und die anderen Beteiligten gegenseitig aufeinander angewiesen. Bei der technischen Darstellung werden detailreich die Rahmenbedingungen benannt und keine einfachen Patentlösungen vorgegaukelt. Risiken werden nicht nur an die Wand gemalt, sondern erklärt, für die Lösungen gibt es zumindest erste Hinweise. Mehr kann das Buch aber auch nicht leisten. Für die speziellen technischen Lösungen zur Datensicherheit bedarf es des IT-Sachverstandes, für rechtliche Fragen der Kompetenz eines Juristen. Das Buch deckt die Schnittmenge zwischen beiden ab und hilft so bei Verständigungsproblemen sowie denen, die dazwischen stehen.



Linkhorst, Anette

Das Akteneinsichtsrecht des Strafgefangenen nach § 185 StVollzG

Shaker Verlag Aachen 2005, 332 S., 49.80 Euro, ISBN 3-8322-4238-4

(tw) Das Strafvollzugsrecht ist eines der letzten Gebiete, in denen die »Magna Charta« des Datenschutzes, das Auskunfts- und Akteneinsichtsrecht weder faktisch noch rechtlich umfassend verwirklicht ist. Zwar gibt es seit dem Jahr 2000 die Regelung des § 185 Strafvollzugsgesetz (StVollzG), mit der angeblich den verfassungsrechtlichen Anforderungen entsprochen werden sollte, doch bleibt schon die Regelung selbst hinter diesen Anforderungen zurück, indem sie die Akteneinsicht davon abhängig macht, dass diese »für die Wahrnehmung seiner rechtlichen Interessen« erforderlich ist. Die Realität der Akteneinsichtsgewährung ist noch katastrophaler, wie die Untersuchungen von Linkhorst in ihrer Dissertation zeigen. Bei einer leider wenig repräsentativen Untersuchung in Bremen ergab sich bei 9 Anträgen nur in zwei Fällen eine gesetzeskonforme Akteneinsicht; in einem Fall war hierzu die Intervention eines Rechtsanwaltes nötig.

Angesichts dieser »Not« konnte man gespannt sein, was Linkhorst in ihrer Arbeit zu § 185 StVollzG zusammengestellt hat, zumal es sich um die erste monografische Arbeit zu dem Thema seit Erlass der Regelung handelt. Das Ergebnis ist – nicht nur bzgl. des Umfangs des Buches – beachtlich: Die Autorin referiert ausführlich die gesamte verfügbare Rechtsprechung und hierbei auch viele nicht veröffentlichte Urteile. Sie stellt umfassend dar, wer sich in der Literatur zu diesem Thema geäußert hat. Behandelt werden ausführlich die dem § 185 verwandten Regelungen im Verwaltungsrecht, im Stasi-Unterlagengesetz, im (Umwelt-) Informationsfreiheitsrecht, im Strafprozessrecht, ja sogar im Beamtenrecht. Die Geschichte des Strafvollzugs passiert Revue, auch im Hinblick auf das Akteneinsichtsrecht. Die Relevanz der Akteneinsicht für Resozialisierung und informationelle Selbstbestimmung wird herausgearbeitet. Hierbei lässt sich die Autorin von einem grundrechtsfreundlichen Selbstverständnis leiten. Leider führt die gefangenenfreundliche Sichtweise dazu, dass die rechtsdogmatischen Probleme der Akteneinsicht oberflächlich behandelt werden. Es ist gerade im stark sicherheitsrelevanten Strafvollzug allzu leichtfertig, ohne umfangreichen Einstieg in eine Auseinandersetzung zum Ergebnis zu kommen, es könnten in Praxis keine Versagungsgründe gegen die Akteneinsicht vorgebracht werden. Damit kommt das Buch nicht befriedigend dem Versprechen auf dem Umschlag nach, Hilfen bei der »Auslegung im Lichte des Rechts auf informationelle Selbstbestimmung« zu geben. Die Grundlagen des Akteneinsichtsrecht werden fleißig und ausführlich erarbeitet. Die Hoffnung, dass diese dann gebündelt und auf einer höheren Abstraktionsebene verallgemeinert würden, bleibt aber unbegründet. So gibt es z.B. zwar viele Antworten von Rechtsprechung und Literatur, was es mit der Differenzierung zwischen Auskunft und Akteneinsicht im § 185 StVollzG auf sich hat. Aber eine eigene klare Meinung der Autorin wird nicht daraus abgeleitet. Insgesamt: Der Wert dieser Arbeit liegt darin, zum Thema eine große Fundgrube für Informationen und Material zu sein.

Drastischer Abbau des Datenschutzes geplant

Presseerklärung der DVD vom 23.09.2005

Die Deutsche Vereinigung für Datenschutz e.V. fordert in einer Presseerklärung den Bundesrat auf, Pläne zur Schwächung des betrieblichen Datenschutzes fallen zu lassen.

Nach einem Vorstoß der Länder Niedersachsen und Hessen im Bundesrat soll die Schwelle zur Bestellung eines Datenschutzbeauftragten von fünf auf zwanzig Beschäftigte erhöht werden. Entsprechend soll der Schwellenwert für die Meldepflicht geändert werden. Mit diesem Vorschlag würde der Grundrechtsschutz von Millionen von Beschäftigten und Verbrauchern durch eine geringere Kontrolldichte gefährdet. Diese Meinung vertritt die Deutsche Vereinigung für Datenschutz e. V., Bonn.

Insbesondere bei der Verarbeitung von Massendaten (Inkassobüros, Personalvermittlungen, Schreibbüros, Lettershops, kleine IT-Dienstleister, etc.) entsteht dadurch eine Schutzlücke. Darüber hinaus wird die Änderung gerade auch den Schutz besonders sensibler Daten, wie sie z.B. in Arztpraxen, Apotheken, Rechtsanwalts- und Steuerberaterkanzleien etc. anfallen, gefährden.

Nach den Erfahrungen der DVD wird der Schutz des Rechts auf informationelle Selbstbestimmung der Bürger viel zu stiefmütterlich behandelt. Hunderttausende Unternehmen und Dienstleister verzeichnen hier heute schon erhebliche Defizite.

Das deutsche Modell des Datenschutzbeauftragten als innerbetriebliche Kontrollinstanz hat sich bewährt und wird inzwischen zunehmend international kopiert (zuletzt in Frankreich).

Der Datenschutzbeauftragte nimmt dabei eine wichtige Funktion in dem vom Bundesverfassungsgericht geforderten Kontrollsystem wahr. Er erhöht die Rechtssicherheit und Vertrauenswürdigkeit in seinem Unternehmen.

Für die Festlegung der Pflicht zur Bestellung eines Datenschutzbeauftragten werden diejenigen Beschäftigten in einem Unternehmen gezählt, die regelmäßig mit personenbezogenen Daten umgehen. Es steht zu befürchten, dass durch die geforderte Anhebung des Schwellenwertes der Grundrechtsschutz für die Beschäftigten und die Verbraucher aus kurzsichtigen wirtschaftlichen Zwängen oder aufgrund mangelnden innerbetrieblichen Sachverstandes geopfert wird.

Aus den gleichen Gründen ist die angestrebte Anhebung des Schwellenwertes für das Entstehen der Meldepflicht abzulehnen. Die gleichzeitige Umsetzung beider Vorschläge bedeutet die faktische Abschaffung des Datenschutzes in weiten Teilen der Gesellschaft. Wir fordern daher den Bundesrat auf, sich in seiner Abstimmung am 23.9. gegen diese Initiative auszusprechen.

Gemeinsame Erklärung zur Vorratsdatenspeicherung

Diese Erklärung wurde im Oktober 2005 von Patrick Breyer initiiert und von der DVD sowie zahlreichen anderen Bürgerrechtsorganisationen unterschrieben.

Als Repräsentanten von Bürgern, Freiberuflern und Unternehmen in Europa und weltweit,

überzeugt, dass die Anerkennung unveräußerlicher Menschenrechte die Grundlage von Freiheit, Sicherheit und wirtschaftlichem Wohlstand darstellt,

besorgt, dass wir im Kampf gegen Terrorismus und Kriminalität diejenigen Werte aufgeben, die wir zu schützen versuchen, nämlich Freiheit und Demokratie,

der Ansicht, dass die aktuellen Pläne zur Aufzeichnung von Informationen über die Kommunikation, Bewegung und Mediennutzung jedes Bürgers die bislang größte Gefahr für unser Recht auf ein selbstbestimmtes und privates Leben darstellen könnten,

bringen wir unsere folgende Überzeugung zum Ausdruck:

1. Die systematische Erfassung oder Speicherung personenbezogener Daten über unsere Kommunikation, Bewegungen und Mediennutzung (»Vorratsdatenspeicherung«) über das für Geschäftszwecke erforderliche Maß hinaus ist inakzeptabel. Wir verlangen, dass sämtliche Vorhaben zur Einführung einer Vorratsdatenspeicherung sofort aufgegeben werden.
2. Die folgenden Überlegungen haben uns zu dieser Schlussfolgerung geführt:
   - Eine Vorratsdatenspeicherung greift exzessiv in die persönliche Privatsphäre ein. Sie beeinträchtigt freiberufliche Aktivitäten (z.B. in den Bereichen Medizin, Recht, Kirche, Journalismus) ebenso wie politische und unternehmerische Aktivitäten, die Vertraulichkeit voraussetzen.
   - Eine Vorratsdatenspeicherung verhindert Terrorismus oder Kriminalität nicht. Sie ist unnötig und kann von Kriminellen leicht umgangen werden.
   - Eine Vorratsdatenspeicherung verstößt gegen das Menschenrecht auf Privatsphäre und informationelle Selbstbestimmung.
   - Eine Vorratsdatenspeicherung ist teuer und belastet die Wirtschaft.
   - Eine Vorratsdatenspeicherung diskriminiert Nutzer von Telefon, Mobiltelefon und Internet.
3. Rechtliche Bestimmungen über den Umgang mit Kommunikationsdaten dürfen nur mit vorheriger parlamentarischer Zustimmung beschlossen werden. Zusätzliche Kosten, die Anbietern infolge sicherheitsbedingter Pflichten entstehen, müssen ihnen erstattet werden.

Große Koalition bringt Bürgerrechte weiter in Gefahr: »Koalitionspartner übernehmen kritiklos Schilys staatsautoritäres Erbe und satteln noch drauf«

Presseerklärung der Internationalen Liga für Menschenrechte vom 17.11.2005

»Unter einer Großen Koalition sind die Bürgerrechte weiter in Gefahr, einer vermeintlichen Sicherheit untergeordnet zu werden.« Zu diesem Ergebnis kommt der Präsident der »Internationalen Liga für Menschenrechte«, Dr. Rolf Gössner, in einem Gastbeitrag für die Berliner Ost-West-Zeitung FREITAG (Ausgabe vom 18.11.2005).

Unter dem Titel »Schilys staatsautoritäres Erbe« analysiert er jenen Teil der Koalitionsvereinbarung zwischen CDU/CSU und SPD, der mit »Deutschland – ein sicheres und freies Land« überschrieben und in dem auch vom »Recht auf Sicherheit« die Rede ist. Es sei nicht zu verkennen, »dass die künftige Große Koalition fraglos das staatsautoritäre Erbe Otto Schilys antritt und weiter auf Nachrüstung setzt – etwa mit einer nachträglichen Sicherungsverwahrung auch für Jugendliche und einer neuen Kronzeugenregelung«.

Die höchst umstrittene Kronzeugenregelung ist Ende 1999 aus guten Gründen ausgelaufen. Begründet wurde dies damals mit »Zweifeln an der Glaubwürdigkeit von Kronzeugen«. Der ihnen in Aussicht gestellte Strafnachlass wirke wie ein »Anreiz zu falschen Verdächtigungen und Denunziationen«. »Sollen diese Erkenntnisse nichts mehr gelten, will man erneut mit schmutzigen Deals gegen das Böse zu Felde ziehen?« fragt Liga-Präsident Gössner in seinem Gastbeitrag, in dem er seine Ablehnung solcher »Zeugen« so begründet: »Wo der Verrat um des persönlichen Vorteils willen gefordert wird, da sind falsche Bezichtigungen geradezu vorprogrammiert. Der Warencharakter solcher Aussagen liegt in der Natur der Kronzeugenschaft und der Beweiswert eines solchen Staatszeugen sinkt letztlich gegen Null, wie auch die Überzeugungskraft eines darauf gestützten Strafurteils.«

Gerade im Bereich der »Inneren Sicherheit« und in der Kriminalpolitik sei der gemeinsame Nenner der Großkoalitionäre gefährlich groß. Zwar habe die präventive Sicherungshaft für »gefährliche« Personen noch abgewendet werden können. Dennoch werde mit problematischen Vorhaben nachgerüstet: So sollen dem Bundeskriminalamt für die Terrorbekämpfung künftig präventive, auch geheimpolizeiliche Befugnisse zur Gefahrenabwehr eingeräumt werden – also schon weit im Vorfeld von möglichen Straftaten und Gefahren.

Die »Antiterror«-Gesetze sollen entfristet werden und keine weitere Evaluierung erfahren. Ebenso sollen die strengen Verfahrensregeln fallen, die bisher zu einem eher maßvollen Einsatz der neuen Eingriffsbefugnisse geführt haben. Die Trennung zwischen Polizei und Geheimdiensten wird weiter aufgeweicht, u.a. mit einer gemeinsamen »Antiterror-Datei«. Eine Entscheidung über den umstrittenen Einsatz der Bundeswehr im Innern, wie er von der CDU/CSU gefordert wird, ist lediglich vertagt worden. Verbesserung des Flüchtlings- und Abschiebeschutzes – bislang Fehlanzeige.

Nach Auffassung der Liga widerspricht es dem Charakter einer liberalen und demokratischen Gesellschaft und einem ebensolchen Rechtsstaat, wenn permanent an der staatlichen Aufrüstungsschraube gedreht wird und dabei Bürgerrechte immer stärker ausgehöhlt werden. »Die Eskalation polizeilicher, geheimdienstlicher oder gar militärischer Antiterror-Reaktionen – deren Effizienz ohnehin recht fraglich ist und die sich oft als kontraproduktiv erweisen – führt letztlich in ein anderes, ein illiberal-autoritäres System«, warnt Gössner im »Freitag«. »Die kritiklose Übernahme der Schilyschen Hinterlassenschaften und die Weiterführung seiner staatsautoritären Politik ist angesichts dieser Gefahr in höchstem Maße bedenklich.«

Kontakt:
Dr. Rolf Gössner, Telefon 0421/703354, Fax 0421/703290, rolf-goessner@ilmr.de, www.rolf-goessner.de.

Prime-Projekt veröffentlicht White Paper

»PRIME - Privacy and Identity Management for Europe« (»Datenschutz und Identitätsmanagement für Europa«) ist ein Anfang 2004 gestartetes EU-Projekt, das Lösungen erforschen und entwickeln soll, die es den Menschen ermöglichen, selbst die Kontrolle über ihre Privatsphäre im Internet zu übernehmen.

Partner des mit 16 Mio. Euro dotierten und bis Februar 2008 laufenden Projektes sind neben zahlreichen Universitäten auch Unternehmen der Privatwirtschaft sowie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein als Datenschutzbehörde.

Das Projekt hat Anfang August die erste Version seines White Paper veröffentlicht, um eine Diskussion über Datenschutz und Identitätsmanagement in Gang zu setzen. Das Dokument konzentriert sich auf wegweisende Lösungen zum Schutz der Privatsphäre gegen Risiken, die durch starke Technik entstehen. Es untersucht die Probleme der Offenlegung persönlicher Daten und der unzureichenden Kontrollmöglichkeit des Einzelnen über ihre Verwendung. Es präsentiert Vorschläge, wie die Kontrolle des Nutzers verbessert und damit auch die Akzeptanz von neuen Anwendungen erhöht werden kann.

Das Projekt lädt Anbieter wie Nutzer ein, sich eine Meinung über die vorgestellten Perspektiven und Vorschläge zu bilden und eine Rückmeldung zu geben.

(Presseerklärung vom 11.08.2005; www.prime-project.eu.org).

Für eine völlige Unabhängigkeit der niedersächsischen Datenschutzkontrolle – Bürgerrechtsorganisation legt Stellungnahme für Landtagsanhörung vor

Presseerklärung der Humanistische Union vom 29.8.2005

Der Beschluss der niedersächsischen Landesregierung, dem Datenschutzbeauftragten die Kontrolle über die Privatwirtschaft zu entziehen, verstößt nach Auffassung der Humanistischen Union (HU) gegen EU-Recht und verfassungsrechtliche Bestimmungen zum Schutz der Grundrechte der Bürgerinnen und Bürger.

So lautet das Fazit der schriftlichen Stellungnahme, die die Humanistische Union anlässlich der morgigen Anhörung im Innenausschuss des niedersächsischen Landtags vorgelegt hat.

Nach dem Willen der niedersächsischen Landesregierung soll ab 1.1.2006 das Innenministerium die Einhaltung der Datenschutzbestimmungen im nicht-öffentlichen Bereich kontrollieren. »Die Landesregierung setzt damit auf ein Auslaufmodell der Datenschutzaufsicht«, erklärt Nils Leopold, Vorstandsmitglied und HU-Datenschutzexperte. »Die EG-Datenschutzrichtlinie fordert eine völlige Unabhängigkeit der Datenschutzkontrolleure. Eine Einverleibung in das Innenministerium stellt einen klaren Verstoß dar.« Unterstützt wird diese Einschätzung durch die EU-Kommission. Sie hatte Anfang Juli ein Vertragsverletzungsverfahren gegen die Bundesrepublik eingeleitet, da bislang sämtliche Aufsichtsbehörden für den Privatbereich nicht den Vorgaben der Datenschutzrichtlinie entsprechen.

Wird die Datenschutzkontrolle über den privaten Bereich beim Innenministerium angesiedelt, befürchtet die Humanistische Union zudem Interessenkonflikte. Die in der Privatwirtschaft vorgehaltenen Daten, z.B. von Telekommunikationsdienstleistern und Internetprovidern, sind zunehmend auch für die Straftatenverfolgung und -verhütung oder im so genannten Kampf gegen den Terror für die Innenministerien interessant. Dieses Interesse verträgt sich nicht mit einer in derselben Behörde durchzuführenden Aufsicht über die Einhaltung des Grundrechtsschutzes in Unternehmen.

Auch praktische Gründe sprechen für einen Datenschutz aus einer Hand: Mit einem einzigen Ansprechpartner für alle Fragen des Datenschutzes wird größere Bürgernähe erreicht. Eine Aufteilung der Zuständigkeiten zwischen Ministerium und Datenschutzbeauftragten ist für viele Bürgerinnen und Bürger nicht nachvollziehbar.

Kontakt: Martina Kant (Bundesgeschäftsführerin), Tel. (030) 204 502-56, E-Mail: info@humanistische-union.de.

Alles auf eine Karte? FIfF-Broschüre zur elektronischen Gesundheitskarte

Dagmar Boedicker, FIfF e.V.

Ab Januar 2006 wird die elektronische Gesundheitskarte (eGK) schrittweise eingeführt, und wer sich im Internet darüber informieren möchte, findet eine Fülle an Material. So viel, dass wir vom FIfF e.V. fanden, ein kleiner Leitfaden sei nötig, um sich in der Vielfalt zu orientieren. Für diejenigen, die nicht selbst im Internet auf die Suche gehen möchten, ist das Angebot dagegen karg. Sind Sie von Ihrer Krankenversicherung schon informiert worden?

Wenn nicht, kann diese Broschüre weiterhelfen. Sie enthält kurze und übersichtliche Angaben zur eGK, ihrem Zweck und ihren Funktionen, der Sicherheit, den Beteiligten und nicht Beteiligten an der Einführung und ihren Interessen. Wir haben Fachleute gebeten, ihre Sicht auf mögliche Auswirkungen, die Situation der Patienten und die technische Infrastruktur zu erläutern.

Die Broschüre enthält ein Glossar, damit Sie das technische und gesundheitspolitische Fachchinesisch rund um die Karte besser überblicken können, und eine kommentierte Liste von Internet-Seiten, damit Sie sich leichter zurechtfinden, wenn Sie selbst weiter suchen wollen. Die Autoren:

- Peter Friemelt, Bundesarbeitsgemeinschaft der PatientInnenstellen
- Klaus-Peter Görlitzer, Zeitschrift BIOSKOP
- Peter Pharow, Fraunhofer-Institut für Integrierte Schaltungen IIS
- Dagmar Boedicker, FIfF e.V.

Die Broschüre ist zum Preis von 3,50 Euro zuzügl. Versandkosten erhältlich beim FIfF e.V., Goetheplatz 4, D-28203 Bremen oder im Buchhandel (ISBN: 3-9802468-9-2, bzw. ab Januar 2006: 978-3-9802468-9-7) oder ab Januar 2006 kostenlos von unserer Website als PDF-Datei herunterzuladen: http://www.fiff.de.